CPS&IoT'2021

2nd Summer School on Cyber-Physical Systems and Internet-of-Things

Budva, Montenegro, June 07-10, 2021

Proceedings of the 2nd Summer School on Cyber-Physical Systems and Internet-of-Things

Vol. II

Editors

Lech Jóźwiak, Chairmen of the CPS&IoT'2021
Eindhoven University of Technology, The Netherlands
and
Radovan Stojanović
University of Montenegro, Montenegro

MECOnet Montenegro in cooperation with SMART4ALL Consortium

Montenegro, June 2021

Message from Chairman,

This Summer School on Cyber-Physical Systems and Internet of Things (SS-CPS&IoT'2021) is continuation of very successful 1st School from 2019. Unfortunately, last year, 2020, we were not able to organize the School because of Covid-19 pandemic. This year we adapted to the situation and managed the event on two tracks, remotely and on site.

SS-CPS&IoT'2021 aims at serving the following main purposes:

-**advanced training** of industrial and academic researchers, developers, engineers and decision-makers; academic teachers, Ph.D. and M.Sc. students; entrepreneurs, investors, research funding agents, and policy makers; and other participants who want to learn about CPS and IoT engineering;

-**dissemination, exchange and discussion** of advanced knowledge and project results from numerous European R&D projects in CPS and IoT;

-**promotion and facilitation** of international contacts and collaboration among people working or interested in the CPS and IoT area.

The School is open to everybody, but previous knowledge or equivalent practical experience at least at the Bachelor level in engineering (e.g. system, computer, electronic, electrical, automotive, aviation, mechanical, or industrial engineering), computer science, informatics, applied physics or similar is recommended. Industry participation is encouraged. SS-CPS&IoT'2021 is not only to follow courses and learn new knowledge on Embedded Systems, CPS and IoT from top professionals, but to meet people, interact and discuss with outstanding researchers, developers, academic lecturers, advanced students, and other participants, collaborate or start collaborations, and meet many talented people who may become employees of your companies as well.

Distinguishing features of this advanced traditional Summer School are that its lectures, demonstrations, and practical hands-on sessions are given by top European and Worldwide specialists in particular CPS and IoT fields from industry and academia, delivering very fresh advanced knowledge. They are based on results from numerous currently running or recently finished European R&D projects in CPS and IoT, what gives an excellent opportunity to get acquainted with issues and challenges of CPS and IoT development; actual industrial problems, designs and case studies; and new concepts, advanced knowledge and modern design methods and tools created in the European R&D projects. This year, we had the honor to invite guest lecturer outside Europe, from Huawei, multinational company, leading global provider of information and communications technology (ICT) infrastructure and smart devices.

Part of the students and lecturers came from the H2020 project SMART4ALL, "Self-sustained customized cyber physical system experiments for capacity building among European stakeholders", so it can be said that it was a Joint School of our community with this significant project.

SS-CPS&IoT’2021 is collocated with CPSIoT’2021, 9th International Conference on Cyber-Physical Systems and Internet-of-Things and 10th Mediterranean Conference on Embedded Computing. The Summer School participants were encouraged to submit their papers to CPSIoT’2021 and MECO’2021, and thus gain additional experience of presenting work in one of the TOP conference in computing.

The CPS&IoT’2021 Summer School Program is composed of four days of lectures, demonstrations, practical hands-on sessions, and discussions, as well as free participation in MECO’2021 and CPSIoT’2021 sessions. The topics of the lectures, demonstrations, and practical hands-on sessions cover major CPS applications (focusing on modern mobile applications that require high-performance or low energy consumption, as well as, high reliability, security and safety), computing technology for modern CPS, CPS architectures, development problems and solutions, as well as, design methodologies and design tools for all CPS design phases. In line with the technological challenges caused by the Covid-19 pandemic, part of the lecture was focused on fighting this disaster by using CPSs. There were also lectures from precision agriculture, in fact, Smart Anything Everywhere.

Detailed list of the SS-CPS&IoT’2021 presentations including the names of their authors and presenters is provided in the Schedule of the School.

Venue of SS-CPS&IoT’2021 was Hotel Budva*****, Budva, Montenegro. Budva is a 3500 years old town located at the Adriatic Sea coast of Montenegro. It is a popular touristic destination, with its charming Old Town, beautiful natural environment, 35 clean sandy beaches, and proximity to many famous touristic attractions as Kotor, Boka Kotorska, Sveti Stefan, Dubrovnik, and several national parks. It is an excellent place to have a summer school in a relaxed and friendly atmosphere.

What were the brief data about this year Summer School? We had 70 lecturers and students, coming from over 20 countries around the world. We worked for four days in a 32-hour capacity, that is equivalent to an academic workload of 3 ECTS credits.

The Chairmen of the SS-CPS&IoT’2021 express their thanks to all authors and presenters, as well as, to all other people who contributed to the success of the Summer School. We are especially proud on 2nd generation of students who successfully finished School and showed an enviable level of knowledge and interest.

We are very grateful to Professor Budimur Lutovac, Publication Chair of CPSIoT’2021 and MECO’2021 helping us to compose these Proceedings, which represents only part of the results carried out by SS-CPSIoT’2021.

We hope to see you again next year, mostly on the spot, in good health and mood.

Yours,

Lech Jóźwiak Eindhoven University of Technology, The Netherlands

Radovan Stojanović University of Montenegro, Montenegro

Contents

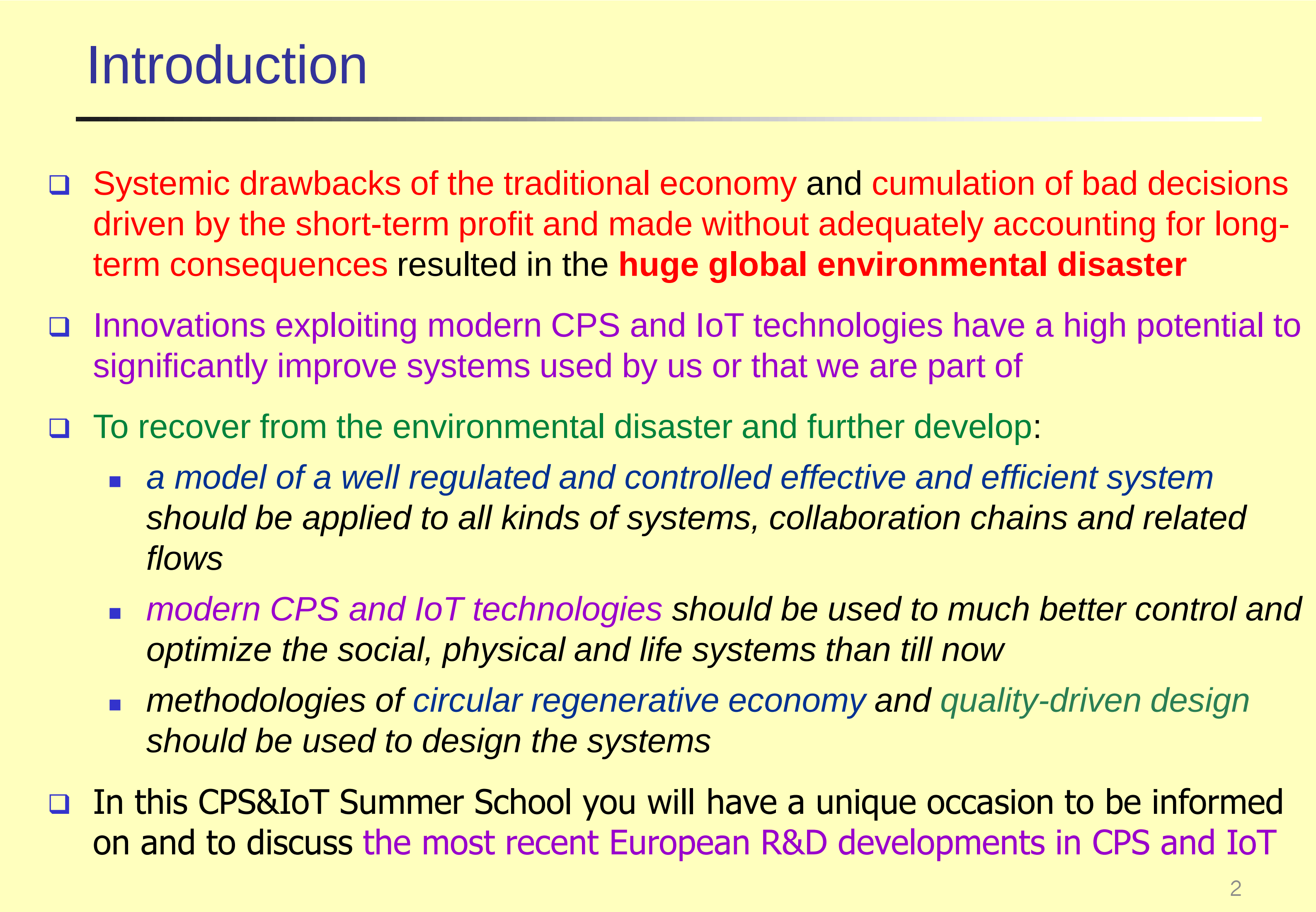
CPS&IoT
SMART4ALL

CPS&IoT'2021 Summer School

Budva, Montenegro
June 7-10, 2021

Introduction

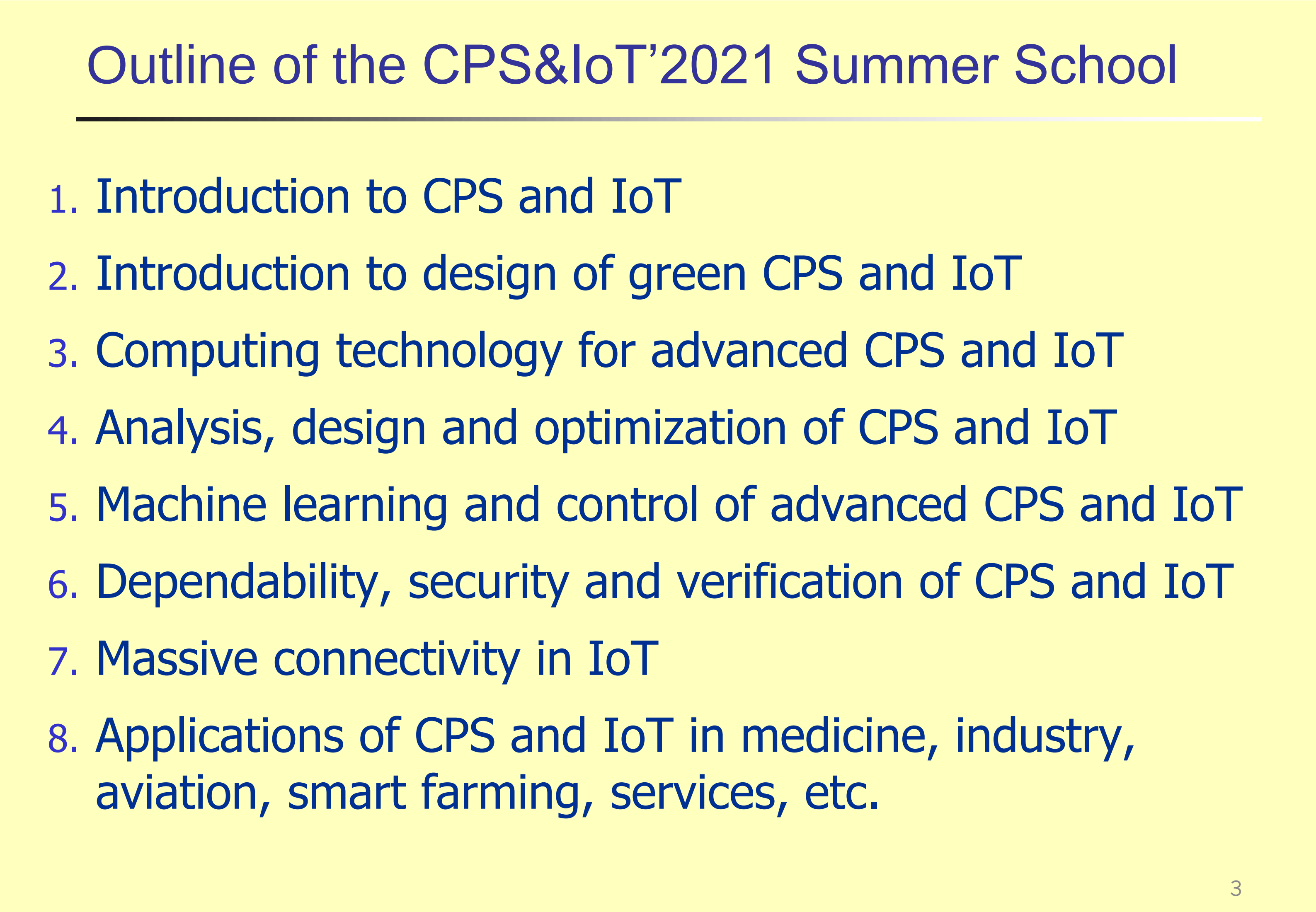
Lech Jóźwiak and Radovan Stojanović



Introduction

- Systemic drawbacks of the traditional economy and cumulation of bad decisions driven by the short-term profit and made without adequately accounting for long-term consequences resulted in the **huge global environmental disaster**
- Innovations exploiting modern CPS and IoT technologies have a high potential to significantly improve systems used by us or that we are part of
- To recover from the environmental disaster and further develop:
  - *a model of a well regulated and controlled effective and efficient system should be applied to all kinds of systems, collaboration chains and related flows*
  - *modern CPS and IoT technologies should be used to much better control and optimize the social, physical and life systems than till now*
  - *methodologies of circular regenerative economy and quality-driven design should be used to design the systems*
- In this CPS&IoT Summer School you will have a unique occasion to be informed on and to discuss the most recent European R&D developments in CPS and IoT

2



Outline of the CPS&IoT’2021 Summer School

1. Introduction to CPS and IoT
2. Introduction to design of green CPS and IoT
3. Computing technology for advanced CPS and IoT
4. Analysis, design and optimization of CPS and IoT
5. Machine learning and control of advanced CPS and IoT
6. Dependability, security and verification of CPS and IoT
7. Massive connectivity in IoT
8. Applications of CPS and IoT in medicine, industry, aviation, smart farming, services, etc.

Privacy Protection, Ethics, Robustness and Regulatory Issues in Autonomous Systems

Ioannis Pitas
Department of Informatics,
Aristotle University of Thessaloniki, Greece
Email: pitas@csd.auth.gr

Abstract – **One of the most important challenges of the present decade in Autonomous Systems (AS) and CPS is the accommodation of ethics, security and privacy issues related to embedded intelligence. Drones and Autonomous Vehicles (AV) are multipurpose AS with civilian, police and military applications, thus their prototype design includes components that may be built for dual use purposes. Second, AS suffer from different cyber-attack types, and some degree of cybersecurity is required. Moreover, as ASs misuse can be accidental or deliberate, it may lead to safety risks, to security risks of both physical and virtual assets, and potential infringements of privacy. Unfortunately, there is no specific legislation that prescribes the protective measures to misuse avoidance and vulnerability exploitation of ASs. Thankfully, there are some technical measures that should be considered in the design stage, mitigating some of these risks. On the legal perspective, privacy laws have been examined to govern ASs usage. However, these regulations still do not govern issues related to what kind of data can be collected by an AS and what ASs owners can deal with these data. As drones and AVs collect footage data, raise privacy and security concerns, related to flying boundaries, data collected in public and private spaces, stored and disseminated data. An increasing number of studies tackle on privacy and security concerns, on effective use of geofences, designated spaces, as to reinforce privacy for users and security for ASs. Data management and protection of AVs collected data is still at a "nascent stage", as there are still some unanswered issues: e.g., the distinguish between personal and non-personal data; capability of "re-identification" etc. This lecture overviews all these aspects and prescribes some technical solutions towards risk mitigation.**

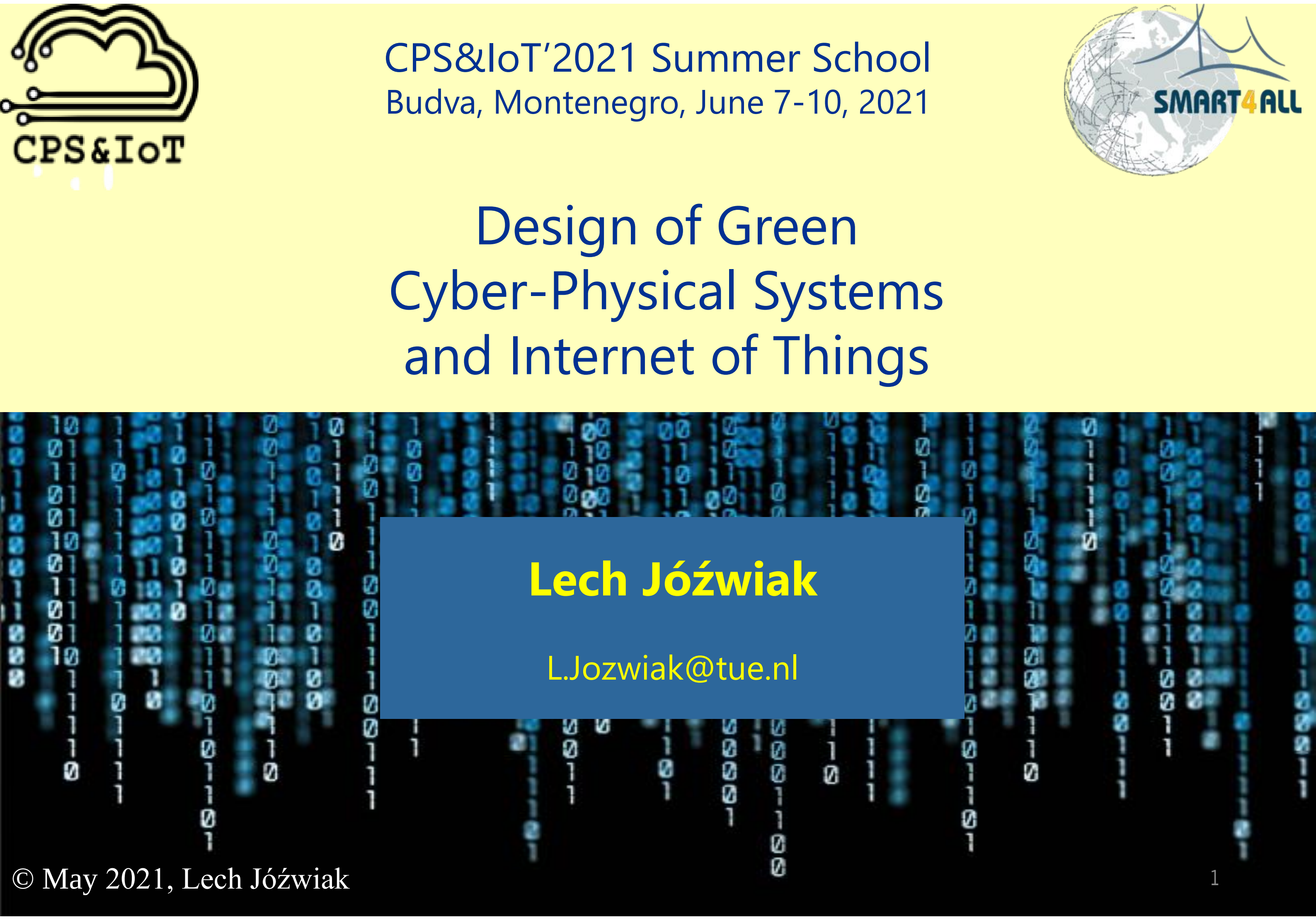
Keywords – Privacy Protection, Ethics, Robustness, Regulatory Issues, Autonomous Systems

About the author

Prof. Ioannis Pitas *(IEEE fellow, IEEE Distinguished Lecturer, EURASIP fellow) received the Diploma and PhD degree in Electrical Engineering, both from the Aristotle University of Thessaloniki (AUTH), Greece. Since 1994, he has been a Professor at the Department of Informatics of AUTH and Director of the Artificial Intelligence and Information Analysis (AIIA) lab. He served as a Visiting Professor at several Universities.*

His current interests are in the areas of computer vision, machine learning, autonomous systems, intelligent digital media, image/video processing, human-centred computing, affective computing, 3D imaging and biomedical imaging. He has published over 920 papers, contributed in 45 books in his areas of interest and edited or (co-)authored another 11 books. He has also been member of the program committee of many scientific conferences and workshops. In the past he served as Associate Editor or co-Editor of 13 international journals and General or Technical Chair of 5 international conferences. He delivered 98 keynote/invited speeches worldwide. He co-organized 33 conferences and participated in technical committees of 291 conferences. He participated in 71 R&D projects, primarily funded by the European Union and is/was principal investigator in 43 such projects. Prof. Pitas lead the big European H2020 R&D project MULTIDRONE: https://multidrone.eu/. He is AUTH principal investigator in H2020 R&D projects Aerial Core and AI4Media. He was chair and initiator of the Autonomous Systems Initiative https://ieeeasi.signalprocessingsociety.org/. He is head of the EC funded AI doctoral school of Horizon2020 EU funded R&D project AI4Media (1 of the 4 in Europe). He has 33100+ citations to his work and h-index 86+ (Google Scholar).

.

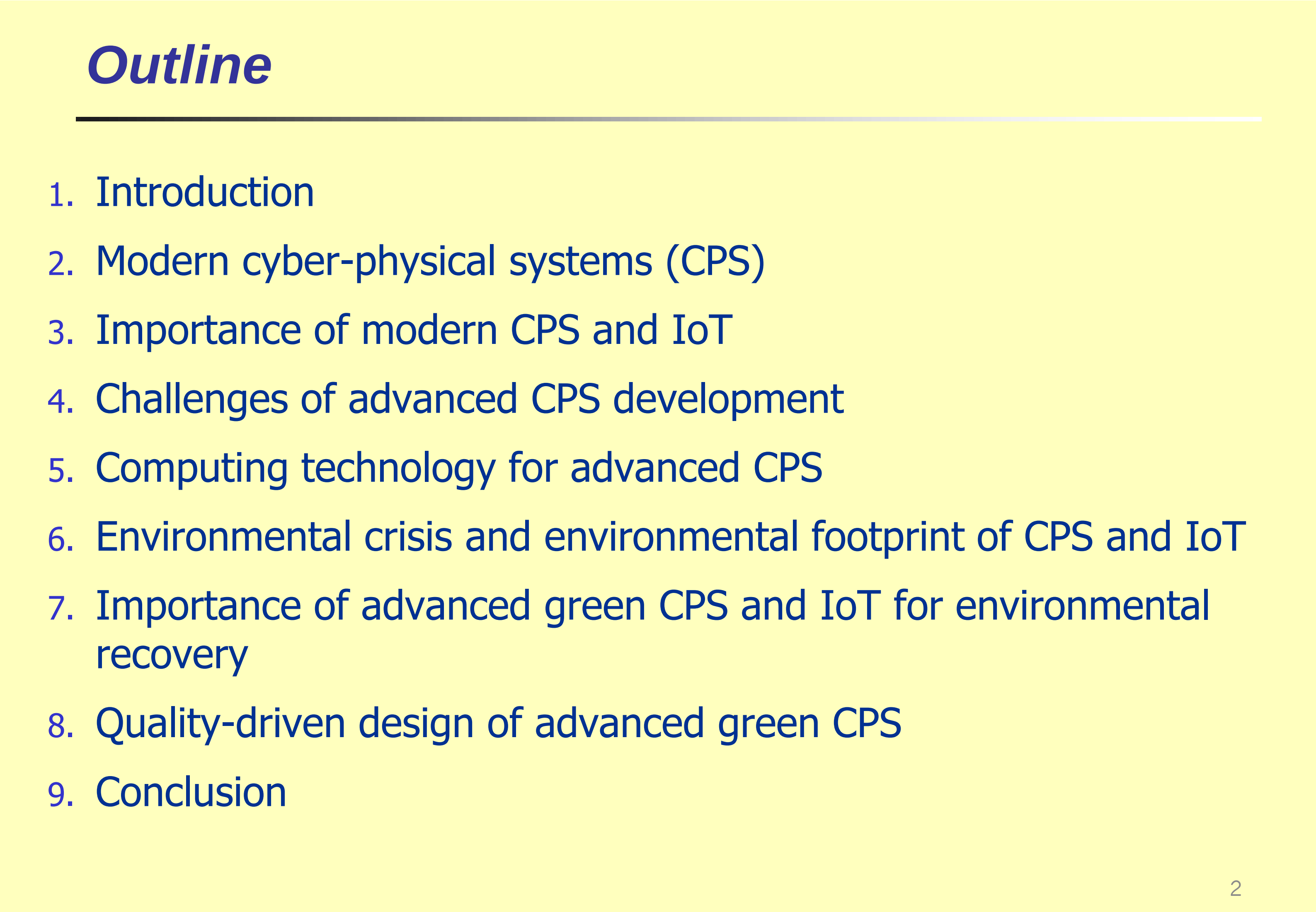


CPS&IoT'2021 Summer School
Budva, Montenegro, June 7-10, 2021

Design of Green Cyber-Physical Systems and Internet of Things

Lech Jóźwiak

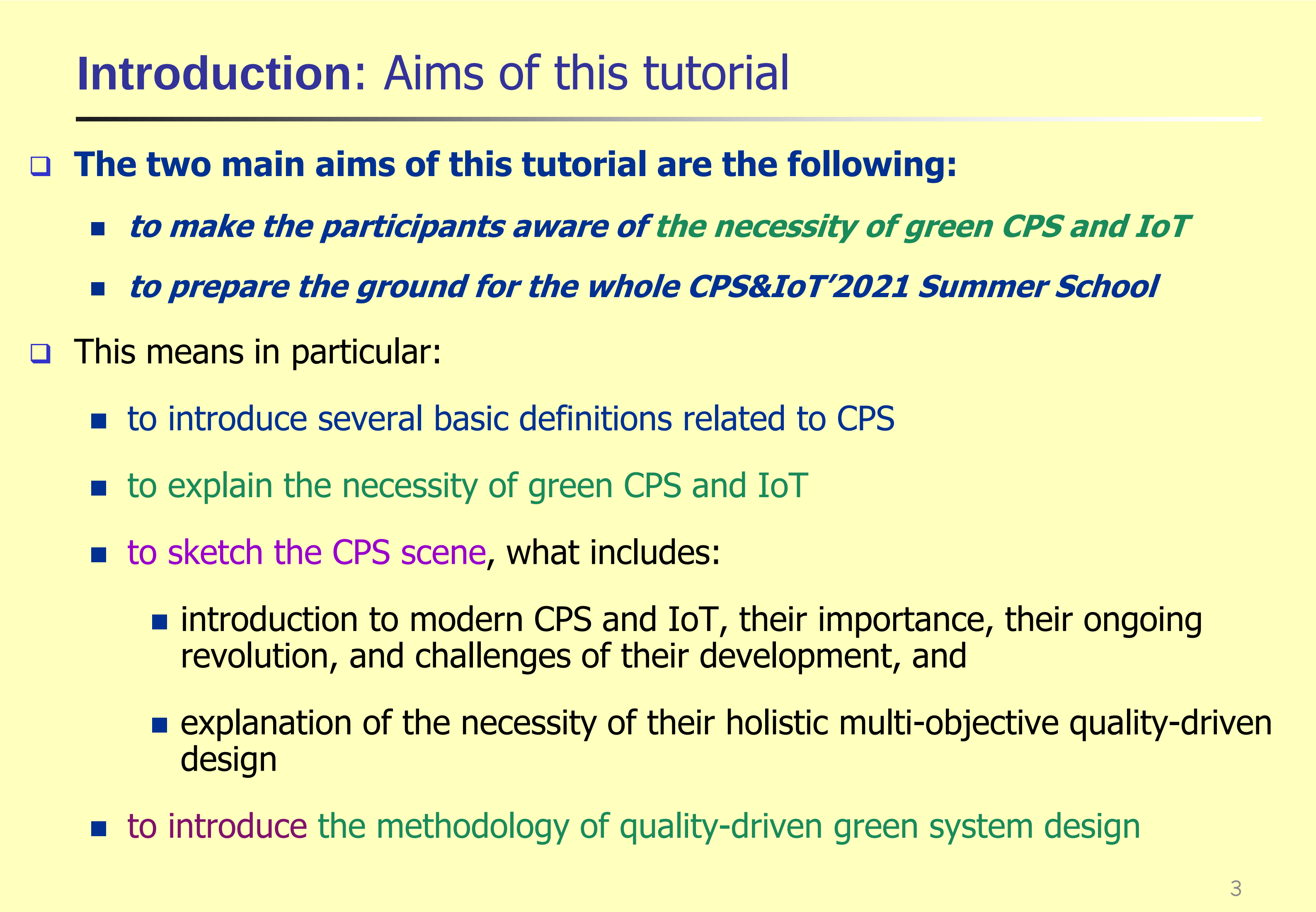
L.Jozwiak@tue.nl



Outline

1. Introduction
2. Modern cyber-physical systems (CPS)
3. Importance of modern CPS and IoT
4. Challenges of advanced CPS development
5. Computing technology for advanced CPS
6. Environmental crisis and environmental footprint of CPS and IoT
7. Importance of advanced green CPS and IoT for environmental recovery
8. Quality-driven design of advanced green CPS
9. Conclusion

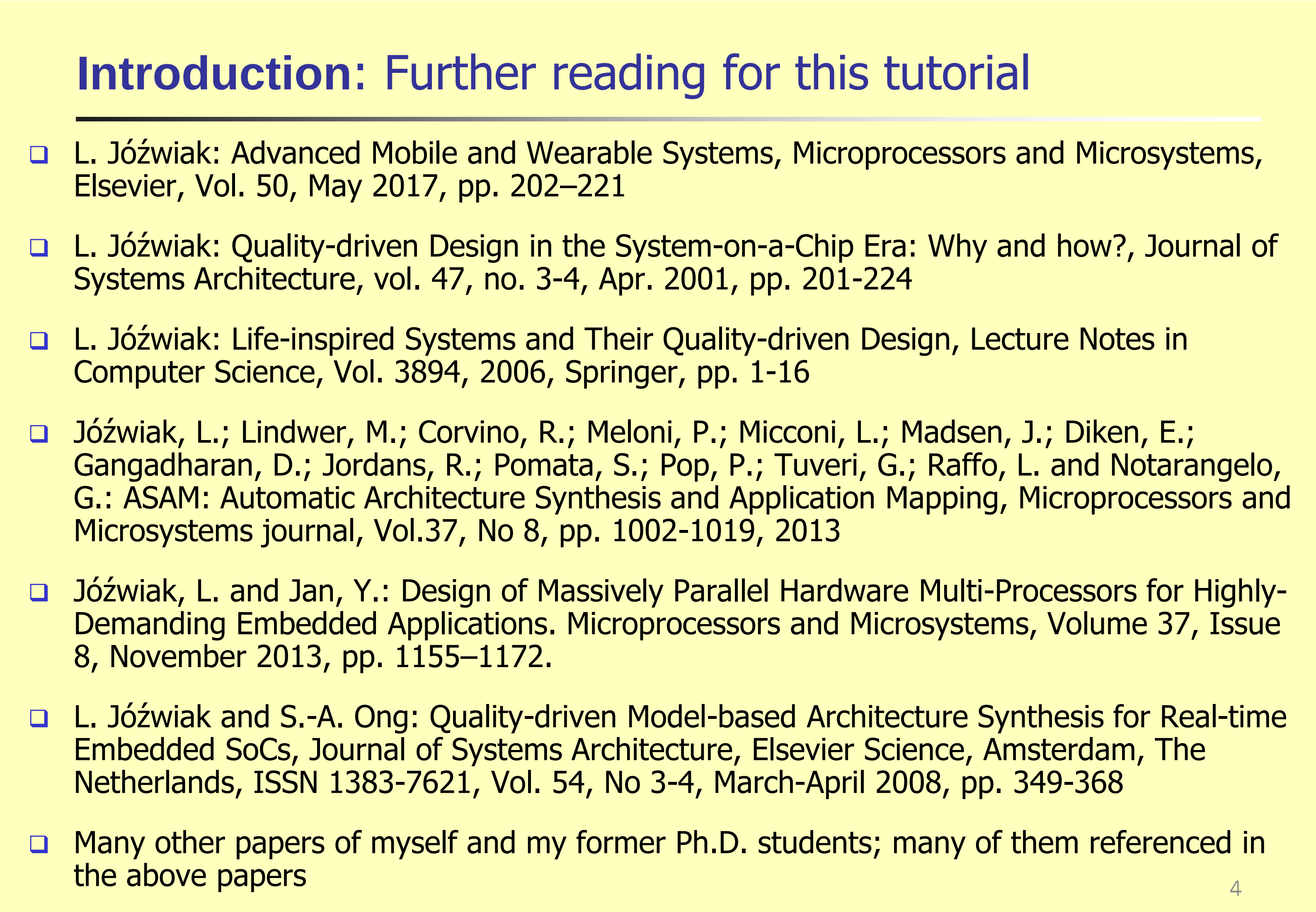
2



Introduction: Aims of this tutorial

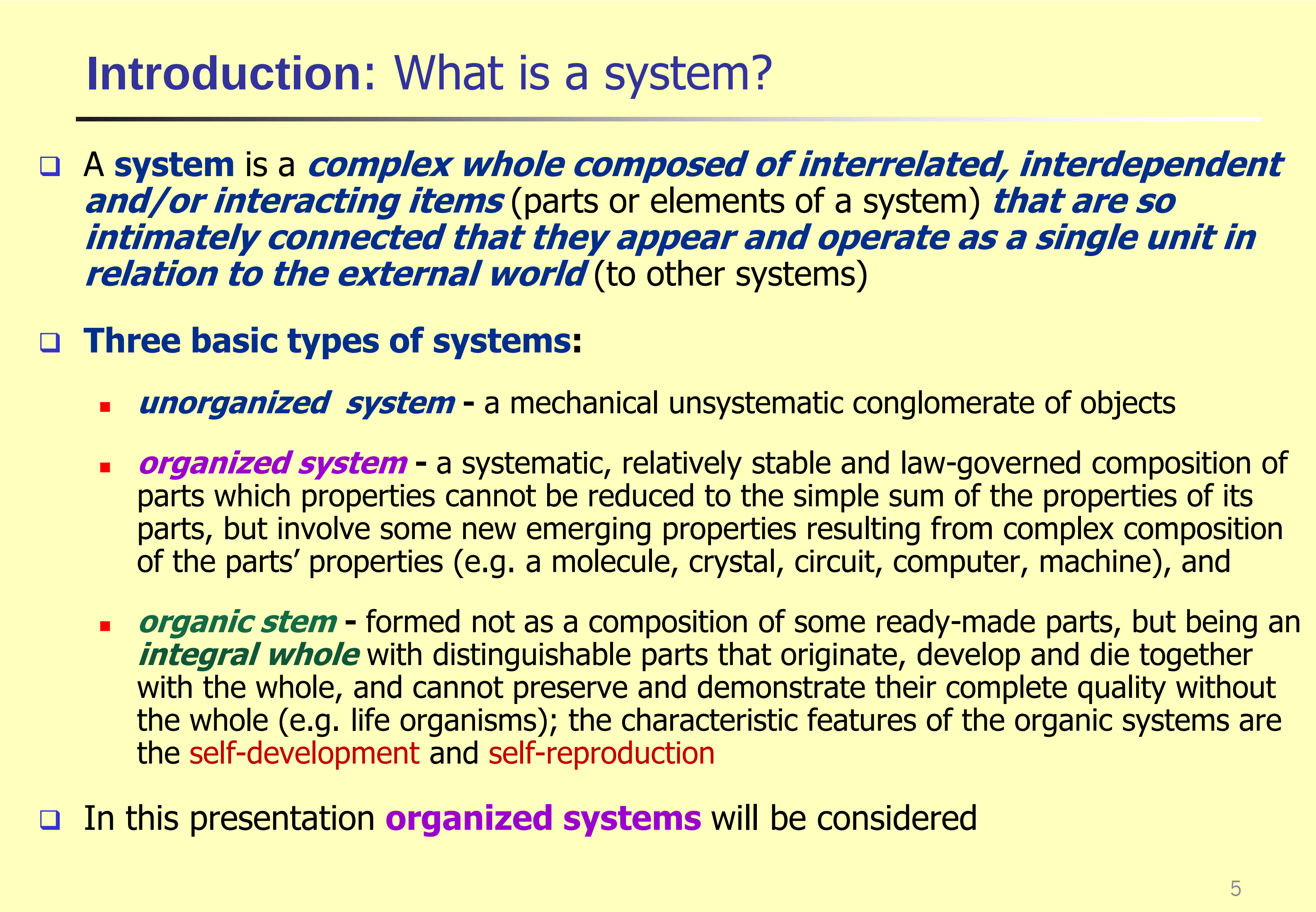
- **The two main aims of this tutorial are the following:**
  - ***to make the participants aware of the necessity of green CPS and IoT***
  - ***to prepare the ground for the whole CPS&IoT'2021 Summer School***
- This means in particular:
  - to introduce several basic definitions related to CPS
  - to explain the necessity of green CPS and IoT
  - to sketch the CPS scene, what includes:
    - introduction to modern CPS and IoT, their importance, their ongoing revolution, and challenges of their development, and
    - explanation of the necessity of their holistic multi-objective quality-driven design
  - to introduce the methodology of quality-driven green system design

3



Introduction: Further reading for this tutorial

- L. Jóźwiak: Advanced Mobile and Wearable Systems, Microprocessors and Microsystems, Elsevier, Vol. 50, May 2017, pp. 202–221
- L. Jóźwiak: Quality-driven Design in the System-on-a-Chip Era: Why and how?, Journal of Systems Architecture, vol. 47, no. 3-4, Apr. 2001, pp. 201-224
- L. Jóźwiak: Life-inspired Systems and Their Quality-driven Design, Lecture Notes in Computer Science, Vol. 3894, 2006, Springer, pp. 1-16
- Jóźwiak, L.; Lindwer, M.; Corvino, R.; Meloni, P.; Micconi, L.; Madsen, J.; Diken, E.; Gangadharan, D.; Jordans, R.; Pomata, S.; Pop, P.; Tuveri, G.; Raffo, L. and Notarangelo, G.: ASAM: Automatic Architecture Synthesis and Application Mapping, Microprocessors and Microsystems journal, Vol.37, No 8, pp. 1002-1019, 2013
- Jóźwiak, L. and Jan, Y.: Design of Massively Parallel Hardware Multi-Processors for Highly-Demanding Embedded Applications. Microprocessors and Microsystems, Volume 37, Issue 8, November 2013, pp. 1155–1172.
- L. Jóźwiak and S.-A. Ong: Quality-driven Model-based Architecture Synthesis for Real-time Embedded SoCs, Journal of Systems Architecture, Elsevier Science, Amsterdam, The Netherlands, ISSN 1383-7621, Vol. 54, No 3-4, March-April 2008, pp. 349-368
- Many other papers of myself and my former Ph.D. students; many of them referenced in the above papers



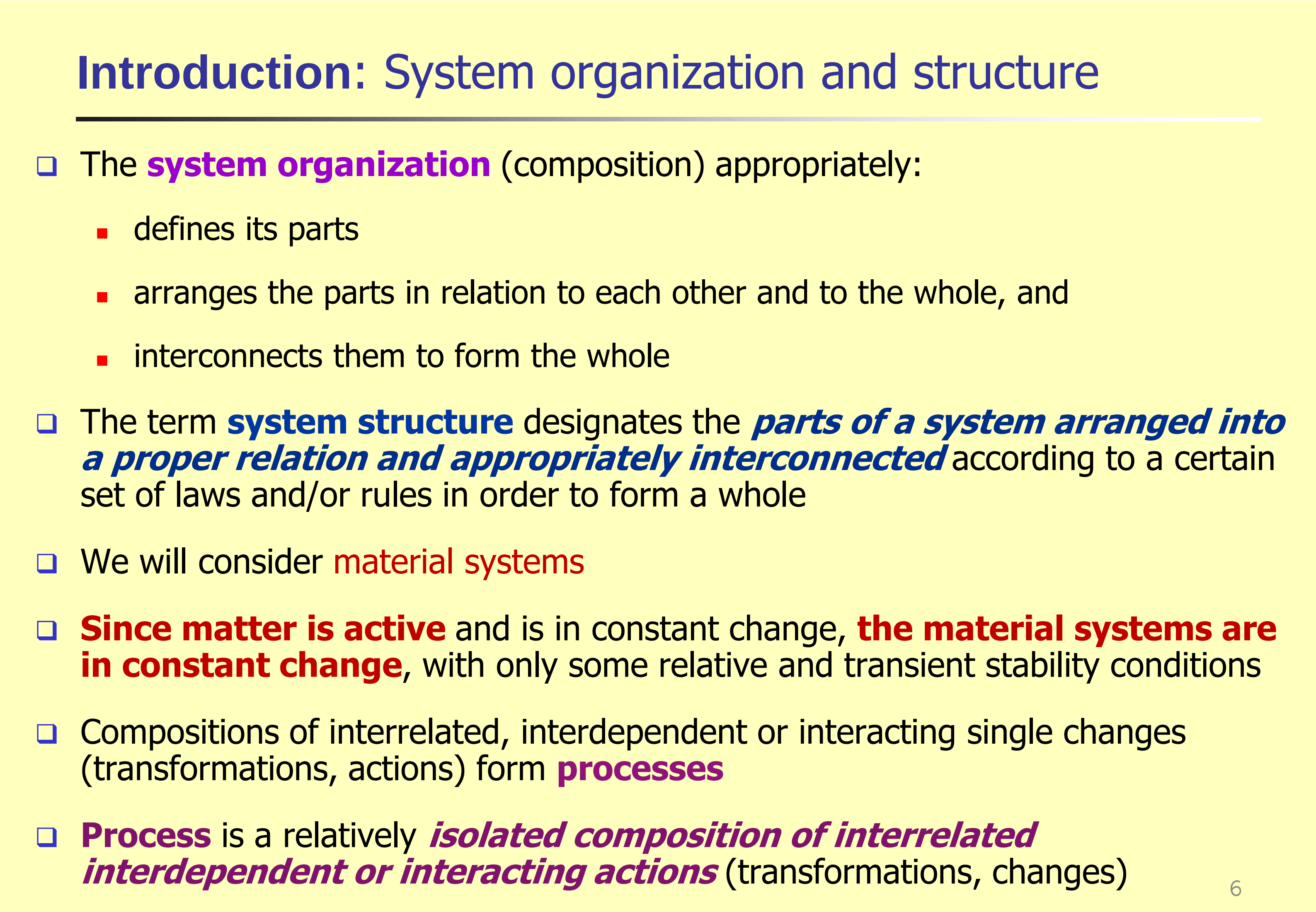
Introduction: What is a system?

- A **system** is a ***complex whole composed of interrelated, interdependent and/or interacting items*** (parts or elements of a system) ***that are so intimately connected that they appear and operate as a single unit in relation to the external world*** (to other systems)

- **Three basic types of systems:**
  - ***unorganized system*** **-** a mechanical unsystematic conglomerate of objects
  - ***organized system*** **-** a systematic, relatively stable and law-governed composition of parts which properties cannot be reduced to the simple sum of the properties of its parts, but involve some new emerging properties resulting from complex composition of the parts' properties (e.g. a molecule, crystal, circuit, computer, machine), and
  - ***organic stem*** **-** formed not as a composition of some ready-made parts, but being an ***integral whole*** with distinguishable parts that originate, develop and die together with the whole, and cannot preserve and demonstrate their complete quality without the whole (e.g. life organisms); the characteristic features of the organic systems are the self-development and self-reproduction

- In this presentation **organized systems** will be considered

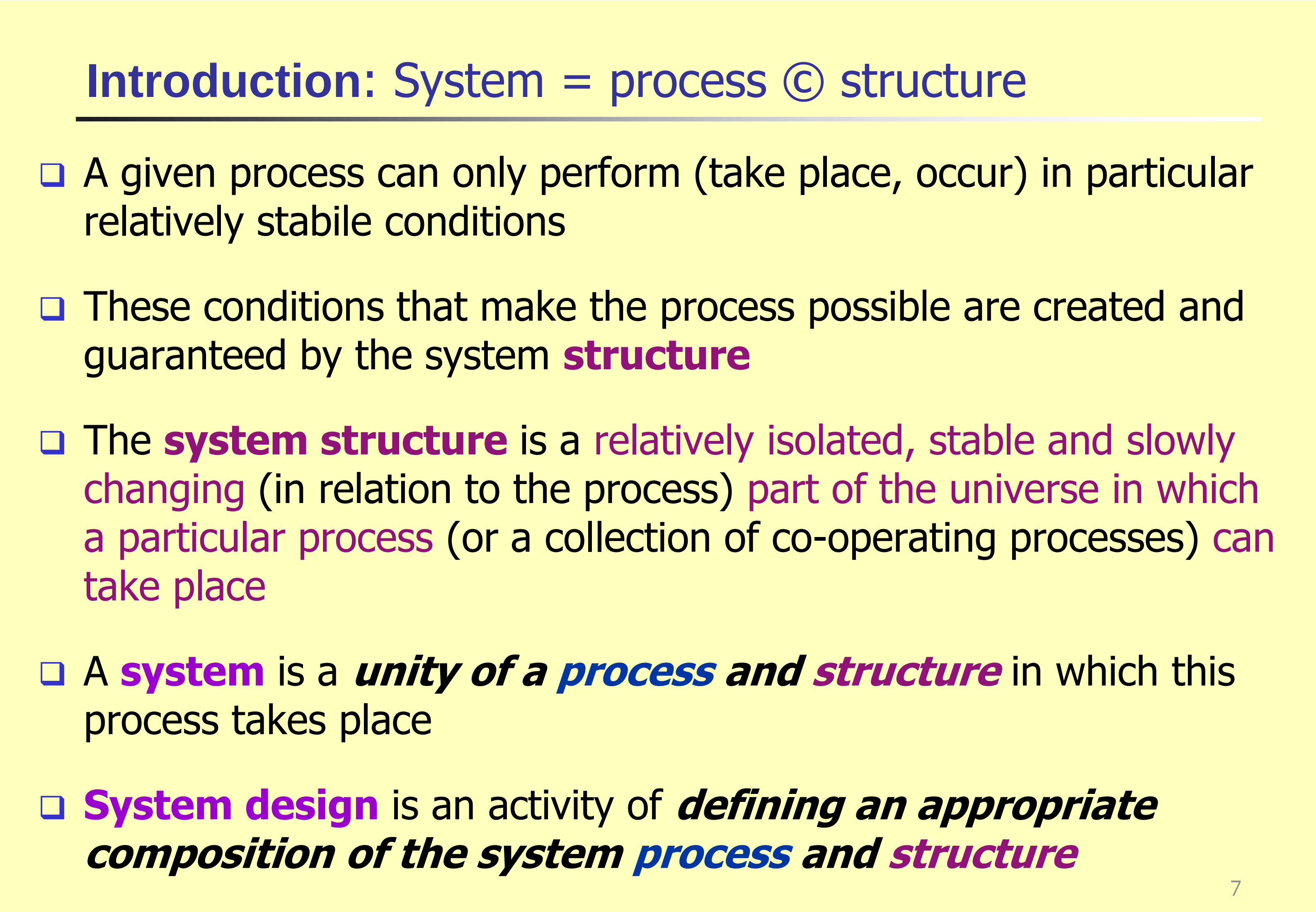
5



Introduction: System organization and structure

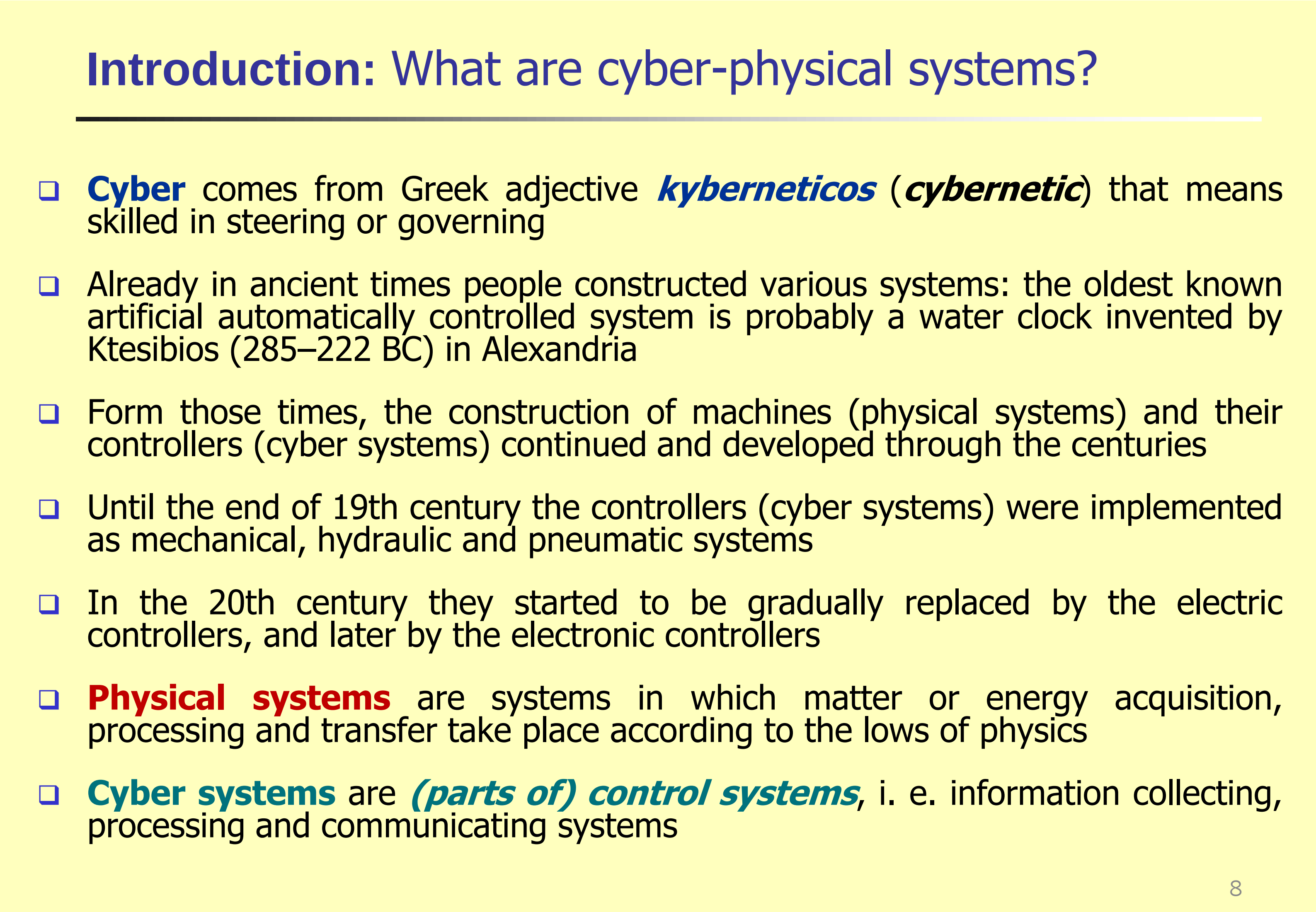
- The **system organization** (composition) appropriately:
  - defines its parts
  - arranges the parts in relation to each other and to the whole, and
  - interconnects them to form the whole
- The term **system structure** designates the ***parts of a system arranged into a proper relation and appropriately interconnected*** according to a certain set of laws and/or rules in order to form a whole
- We will consider material systems
- **Since matter is active** and is in constant change, **the material systems are in constant change**, with only some relative and transient stability conditions
- Compositions of interrelated, interdependent or interacting single changes (transformations, actions) form **processes**
- **Process** is a relatively ***isolated composition of interrelated interdependent or interacting actions*** (transformations, changes)

6



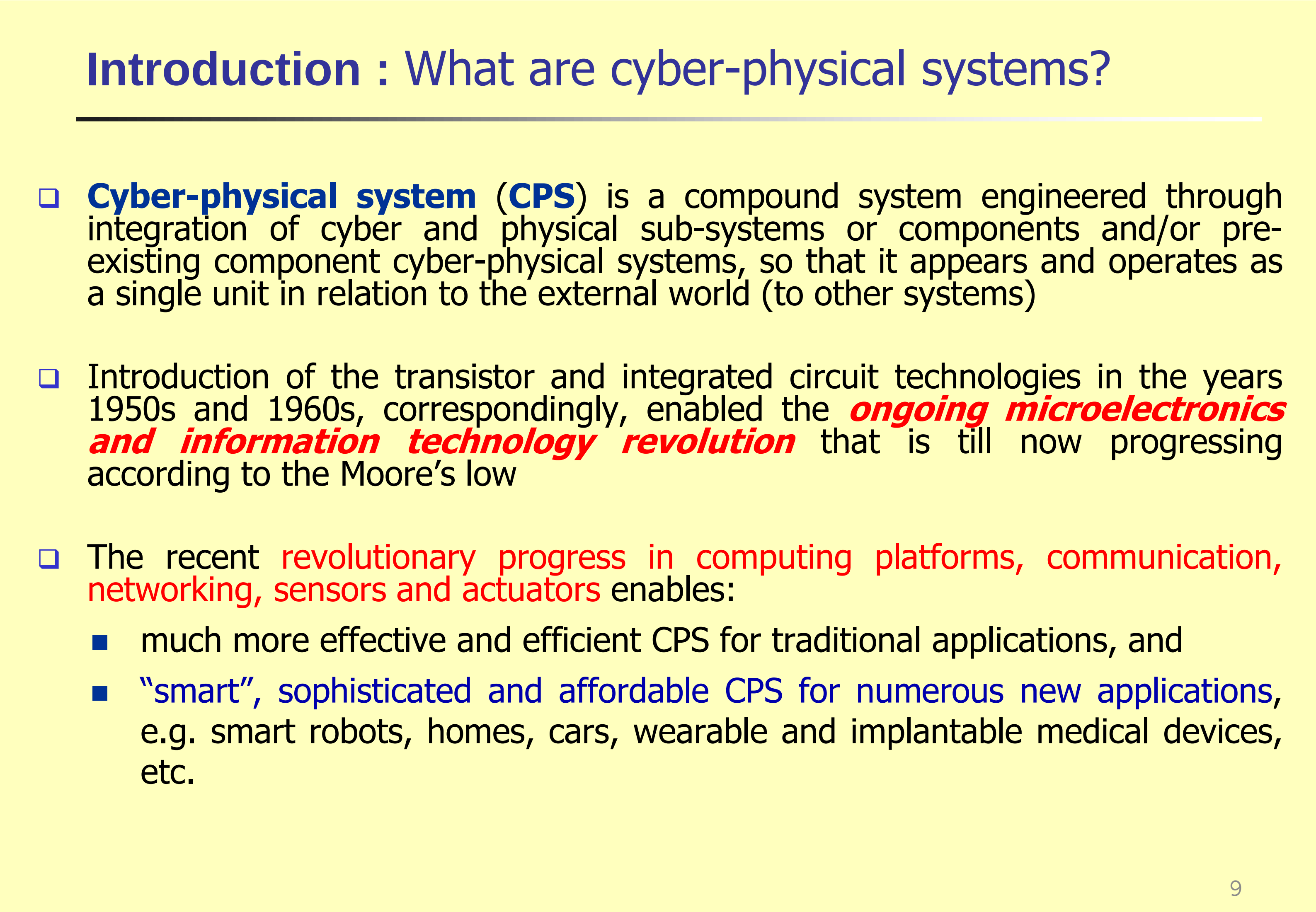
Introduction: System = process © structure

- A given process can only perform (take place, occur) in particular relatively stabile conditions
- These conditions that make the process possible are created and guaranteed by the system **structure**
- The **system structure** is a relatively isolated, stable and slowly changing (in relation to the process) part of the universe in which a particular process (or a collection of co-operating processes) can take place
- A **system** is a ***unity of a process and structure*** in which this process takes place
- **System design** is an activity of ***defining an appropriate composition of the system process and structure***



Introduction: What are cyber-physical systems?

- **Cyber** comes from Greek adjective ***kyberneticos*** (***cybernetic***) that means skilled in steering or governing
- Already in ancient times people constructed various systems: the oldest known artificial automatically controlled system is probably a water clock invented by Ktesibios (285–222 BC) in Alexandria
- Form those times, the construction of machines (physical systems) and their controllers (cyber systems) continued and developed through the centuries
- Until the end of 19th century the controllers (cyber systems) were implemented as mechanical, hydraulic and pneumatic systems
- In the 20th century they started to be gradually replaced by the electric controllers, and later by the electronic controllers
- **Physical systems** are systems in which matter or energy acquisition, processing and transfer take place according to the lows of physics
- **Cyber systems** are ***(parts of) control systems***, i. e. information collecting, processing and communicating systems

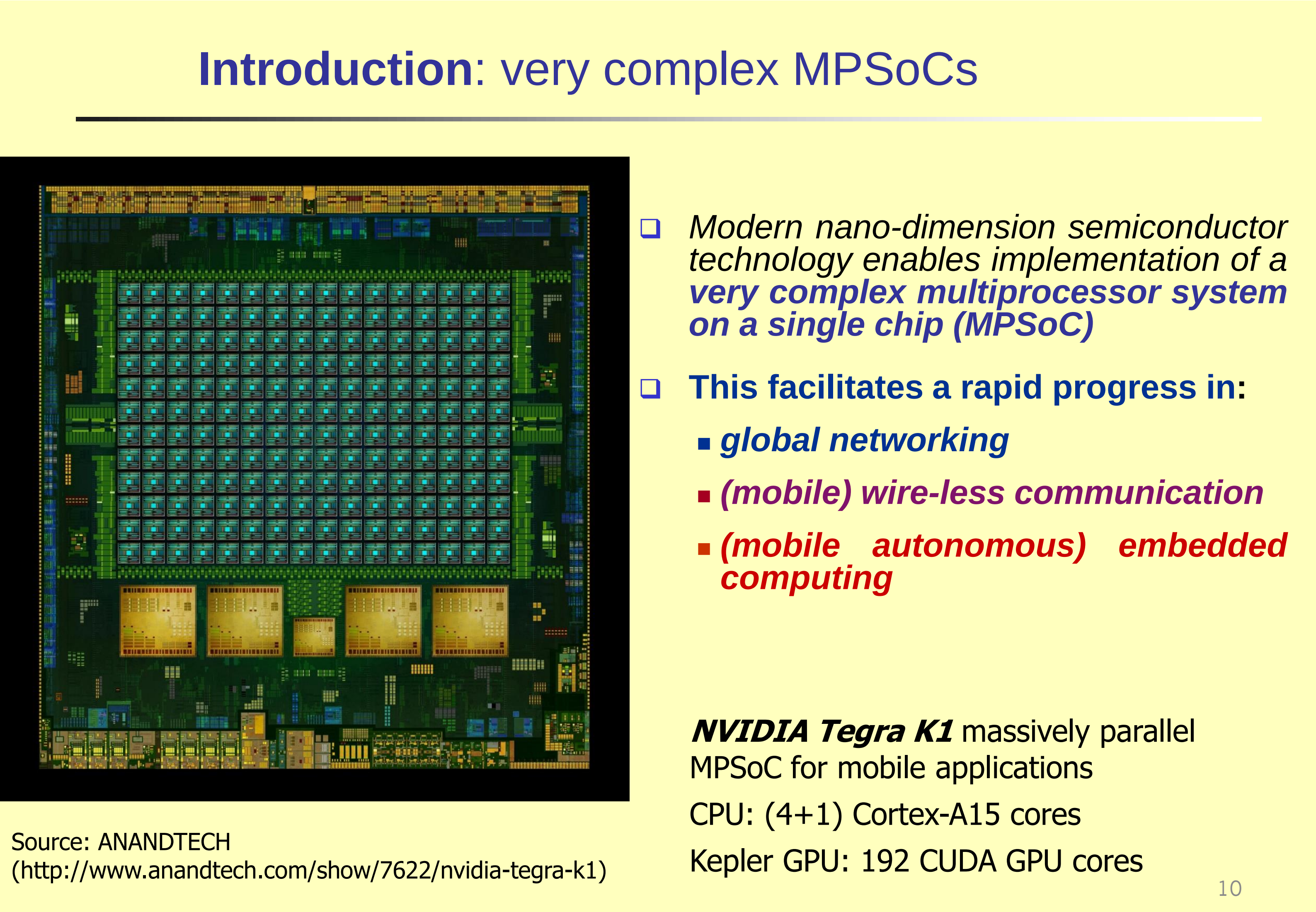


Introduction : What are cyber-physical systems?

- **Cyber-physical system** (**CPS**) is a compound system engineered through integration of cyber and physical sub-systems or components and/or pre-existing component cyber-physical systems, so that it appears and operates as a single unit in relation to the external world (to other systems)

- Introduction of the transistor and integrated circuit technologies in the years 1950s and 1960s, correspondingly, enabled the ***ongoing microelectronics and information technology revolution*** that is till now progressing according to the Moore’s low

- The recent revolutionary progress in computing platforms, communication, networking, sensors and actuators enables:
  - much more effective and efficient CPS for traditional applications, and
  - “smart”, sophisticated and affordable CPS for numerous new applications, e.g. smart robots, homes, cars, wearable and implantable medical devices, etc.



Introduction: very complex MPSoCs

- *Modern nano-dimension semiconductor technology enables implementation of a* ***very complex multiprocessor system on a single chip (MPSoC)***
- **This facilitates a rapid progress in:**
  - ***global networking***
  - ***(mobile) wire-less communication***
  - ***(mobile autonomous) embedded computing***

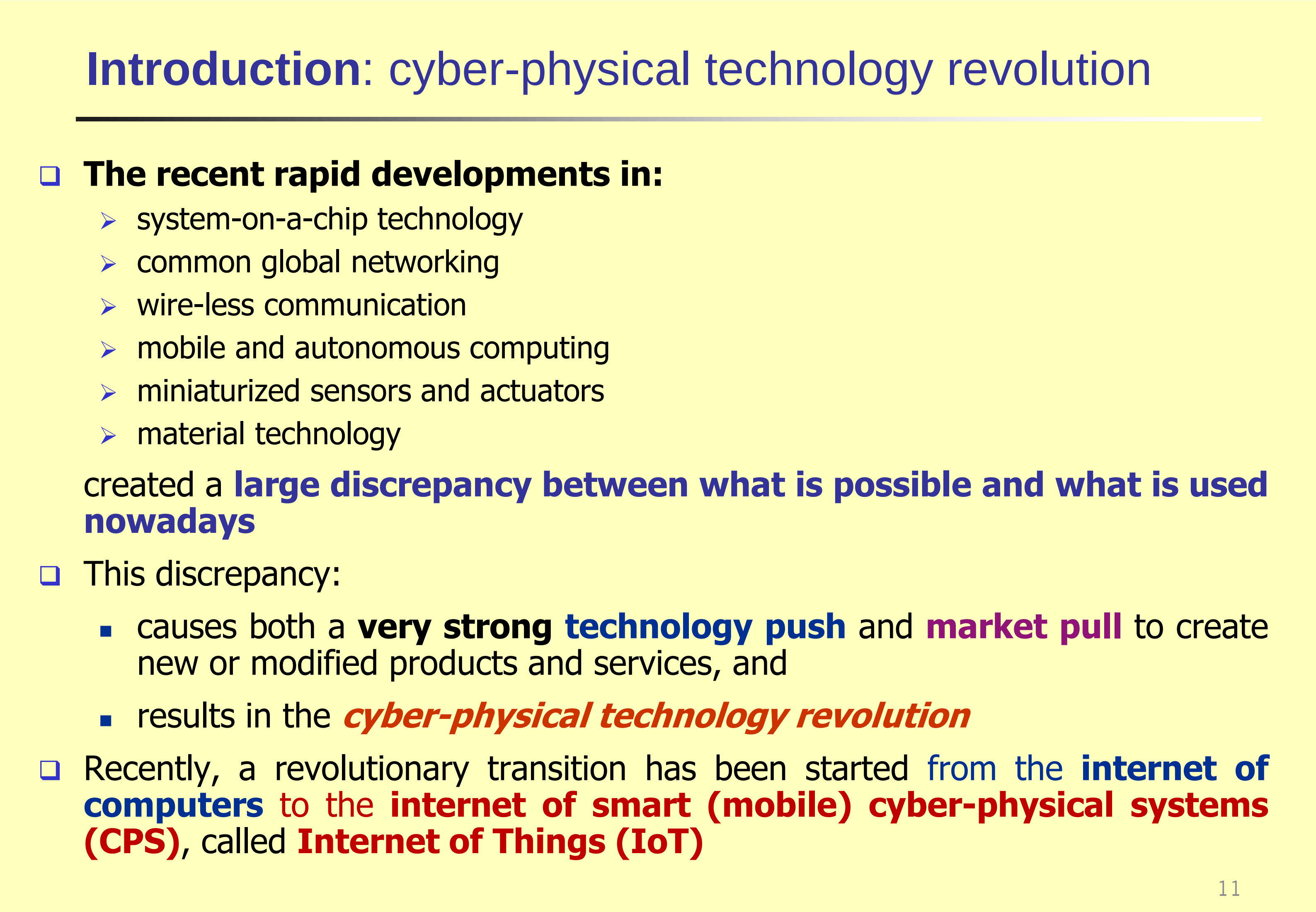
Source: ANANDTECH
(http://www.anandtech.com/show/7622/nvidia-tegra-k1)

NVIDIA Tegra K1 massively parallel MPSoC for mobile applications

CPU: (4+1) Cortex-A15 cores

Kepler GPU: 192 CUDA GPU cores

10

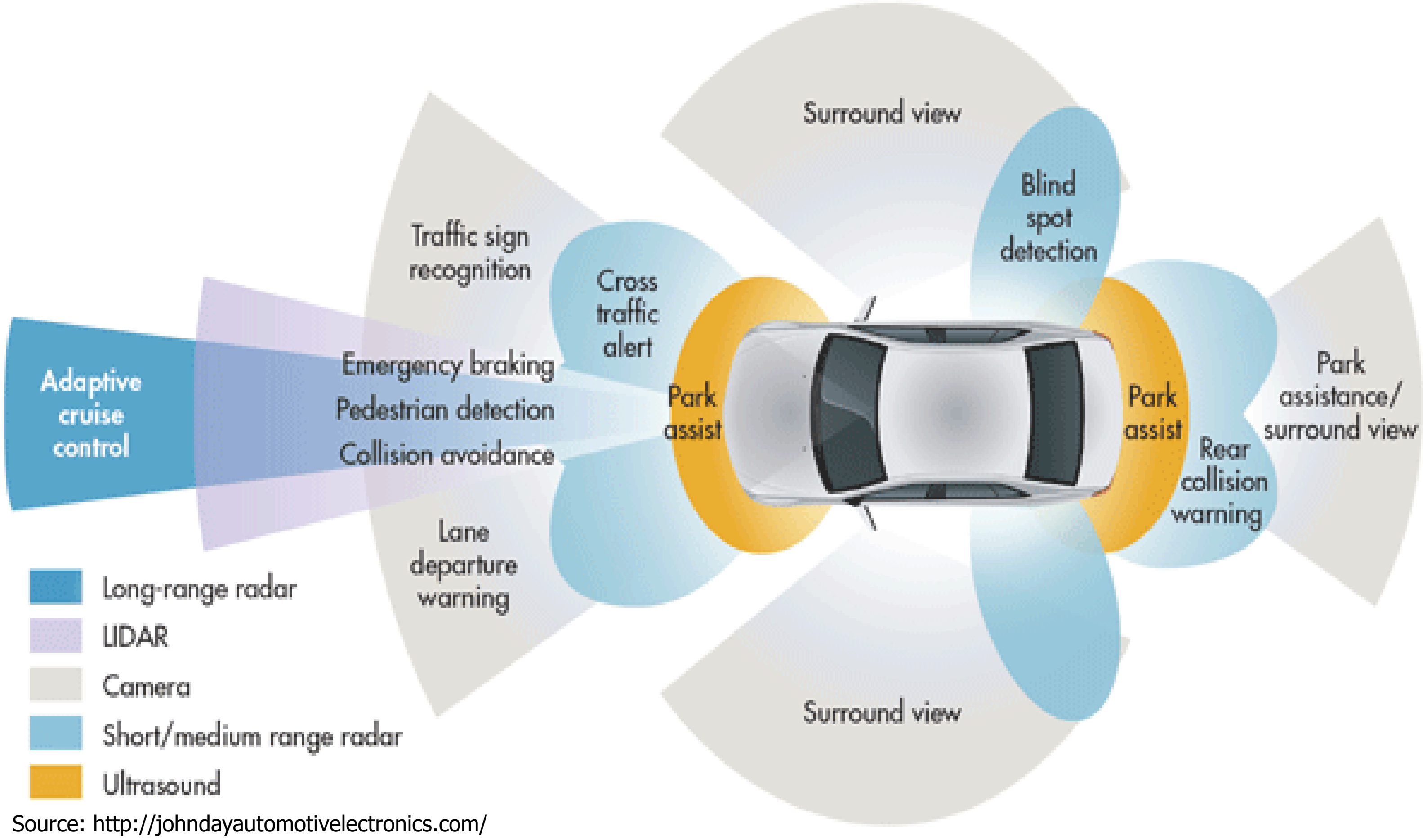


Introduction: cyber-physical technology revolution

- **The recent rapid developments in:**
  - system-on-a-chip technology
  - common global networking
  - wire-less communication
  - mobile and autonomous computing
  - miniaturized sensors and actuators
  - material technology

  created a **large discrepancy between what is possible and what is used nowadays**
- This discrepancy:
  - causes both a **very strong technology push** and **market pull** to create new or modified products and services, and
  - results in the ***cyber-physical technology revolution***
- Recently, a revolutionary transition has been started from the **internet of computers** to the **internet of smart (mobile) cyber-physical systems (CPS)**, called **Internet of Things (IoT)**

Examples of modern mobile CPS: autonomously-driving cars



Source: http://johndayautomotivelectronics.com/

Examples of modern mobile CPS: smart wearables

13

Examples of CPS: wearable virtual and augmented reality

Oculus
Gear VR
Oculus
Active Matrix Liquid Crystal Display image display
Sensor fusion
Binocular 40 degree by degree field-of-view
Integrated day and night camera
Ejection Safe to 600 knots equivalent air speed

Source: http://www.technodo.com/

Source: https://www.oculus.com

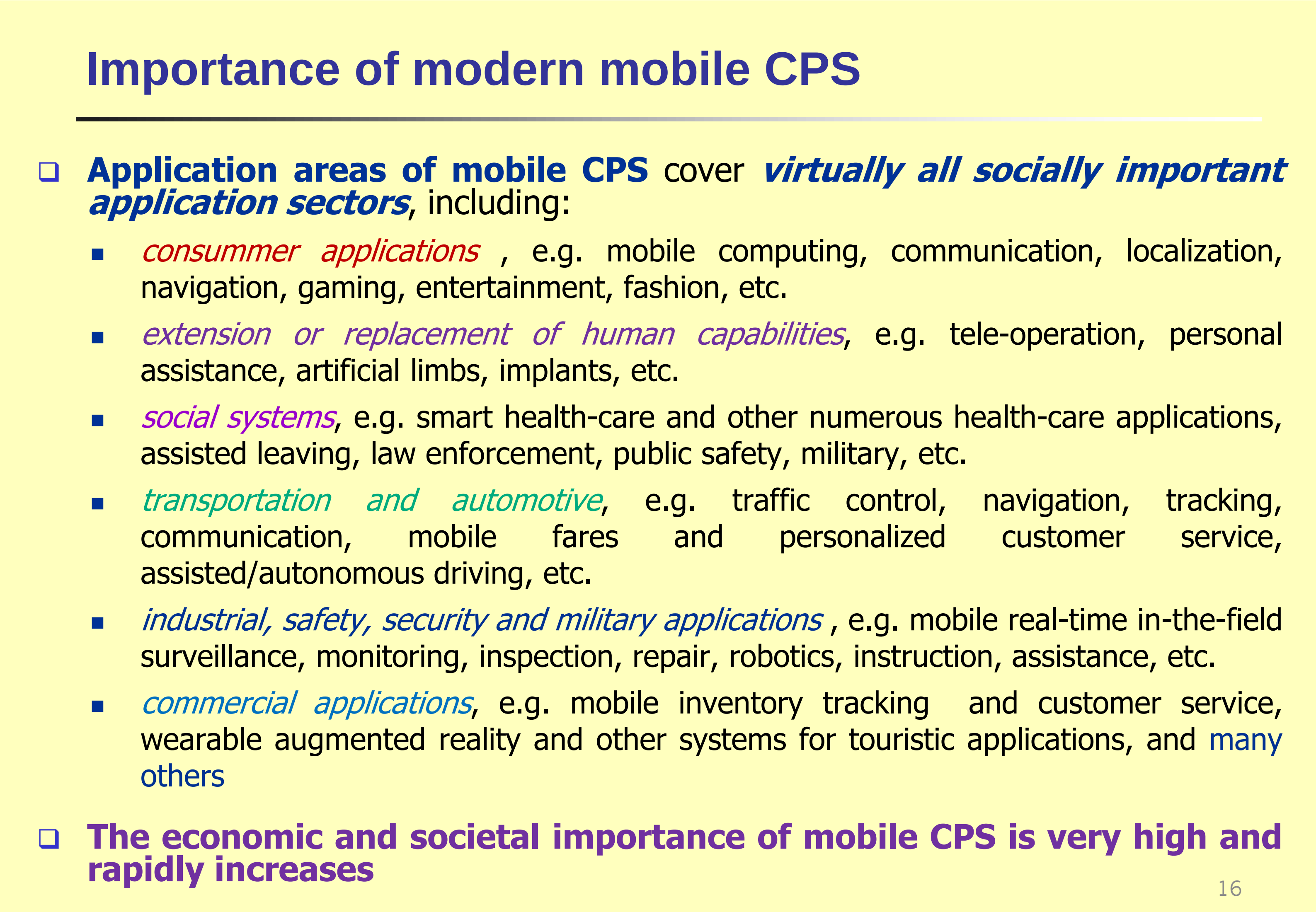
14

Examples of modern CPS: smart miniaturized implants and pill-size medical devices

modern 10 times smaller pace-makers

A new wave of the information technology revolution has arrived that creates much more coherent and fit to use CPS and connects them to form the IoT

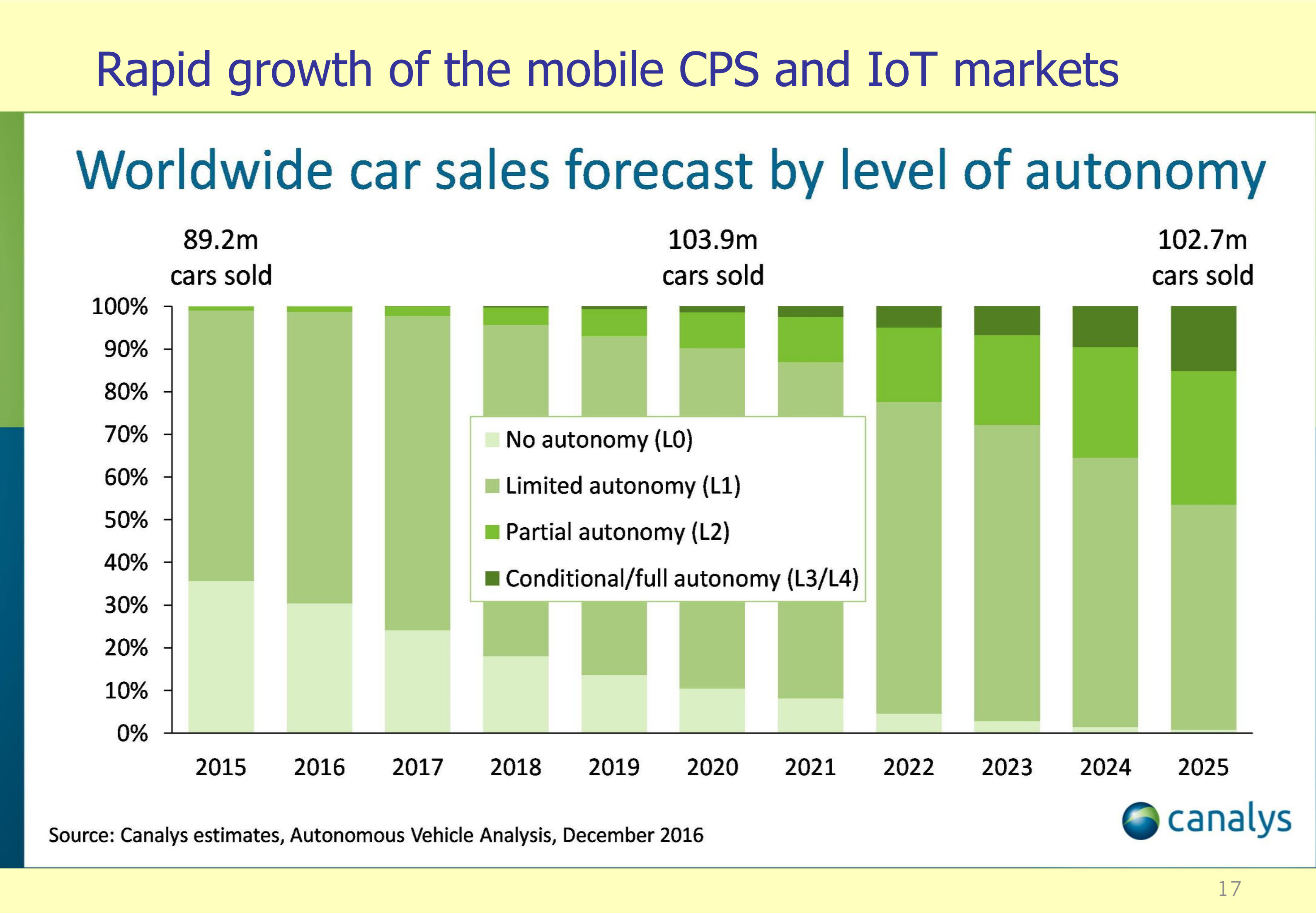
15



Importance of modern mobile CPS

- **Application areas of mobile CPS** cover ***virtually all socially important application sectors***, including:
  - *consummer applications* , e.g. mobile computing, communication, localization, navigation, gaming, entertainment, fashion, etc.
  - *extension or replacement of human capabilities*, e.g. tele-operation, personal assistance, artificial limbs, implants, etc.
  - *social systems*, e.g. smart health-care and other numerous health-care applications, assisted leaving, law enforcement, public safety, military, etc.
  - *transportation and automotive*, e.g. traffic control, navigation, tracking, communication, mobile fares and personalized customer service, assisted/autonomous driving, etc.
  - *industrial, safety, security and military applications* , e.g. mobile real-time in-the-field surveillance, monitoring, inspection, repair, robotics, instruction, assistance, etc.
  - *commercial applications*, e.g. mobile inventory tracking and customer service, wearable augmented reality and other systems for touristic applications, and many others
- **The economic and societal importance of mobile CPS is very high and rapidly increases**

16

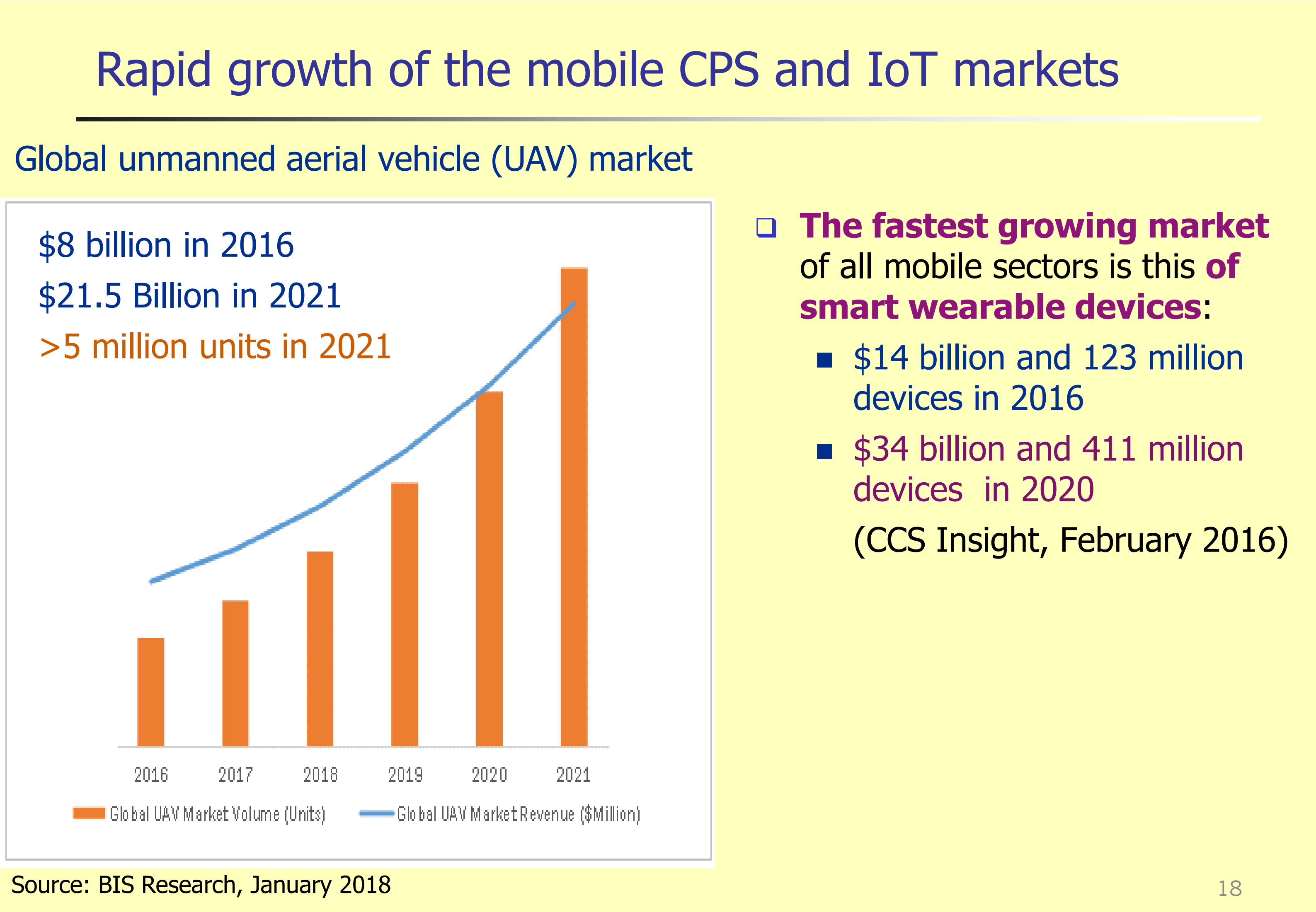


Rapid growth of the mobile CPS and IoT markets

Worldwide car sales forecast by level of autonomy

Source: Canalys estimates, Autonomous Vehicle Analysis, December 2016

17



Rapid growth of the mobile CPS and IoT markets

Global unmanned aerial vehicle (UAV) market

$8 billion in 2016

$21.5 Billion in 2021

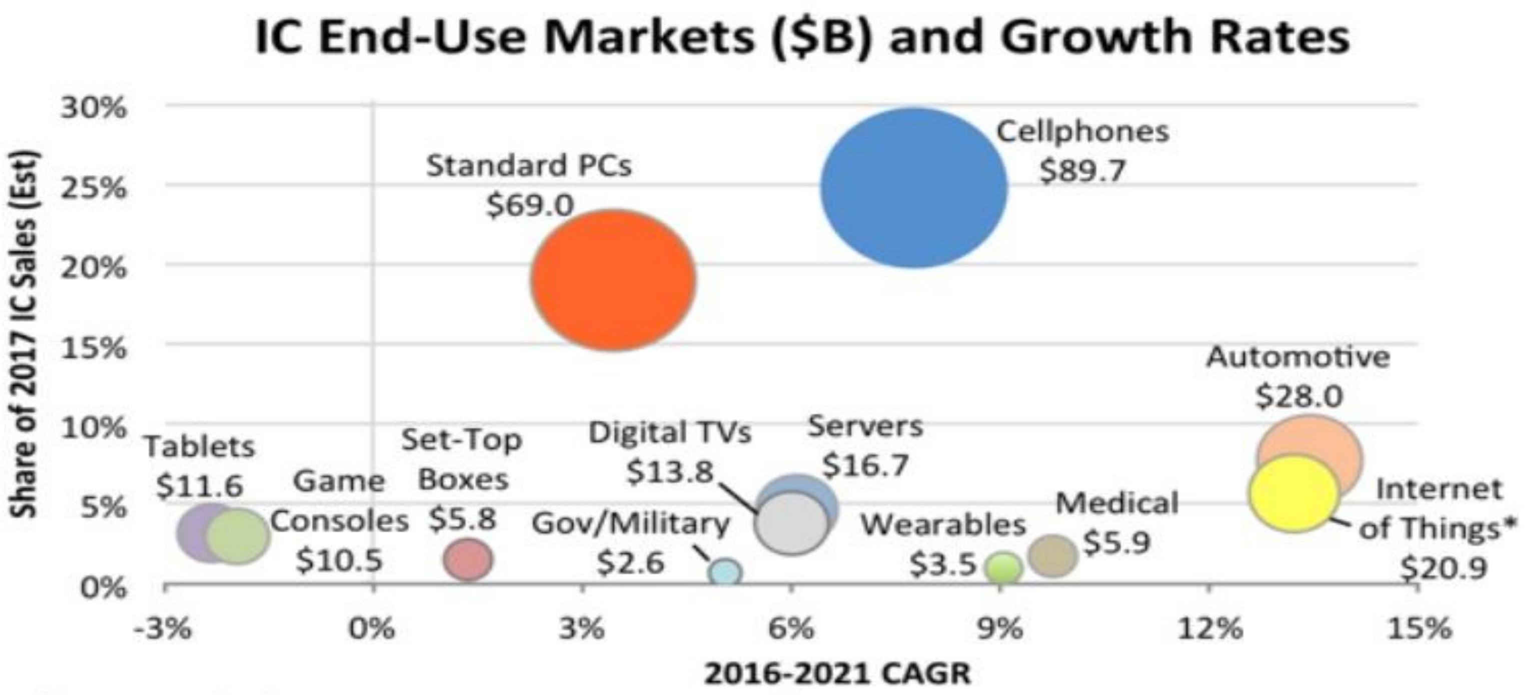
>5 million units in 2021

Source: BIS Research, January 2018

- **The fastest growing market** of all mobile sectors is this **of smart wearable devices**:
  - $14 billion and 123 million devices in 2016
  - $34 billion and 411 million devices in 2020

  (CCS Insight, February 2016)

Rapid growth of the **chip market** for mobile CPS and IoT



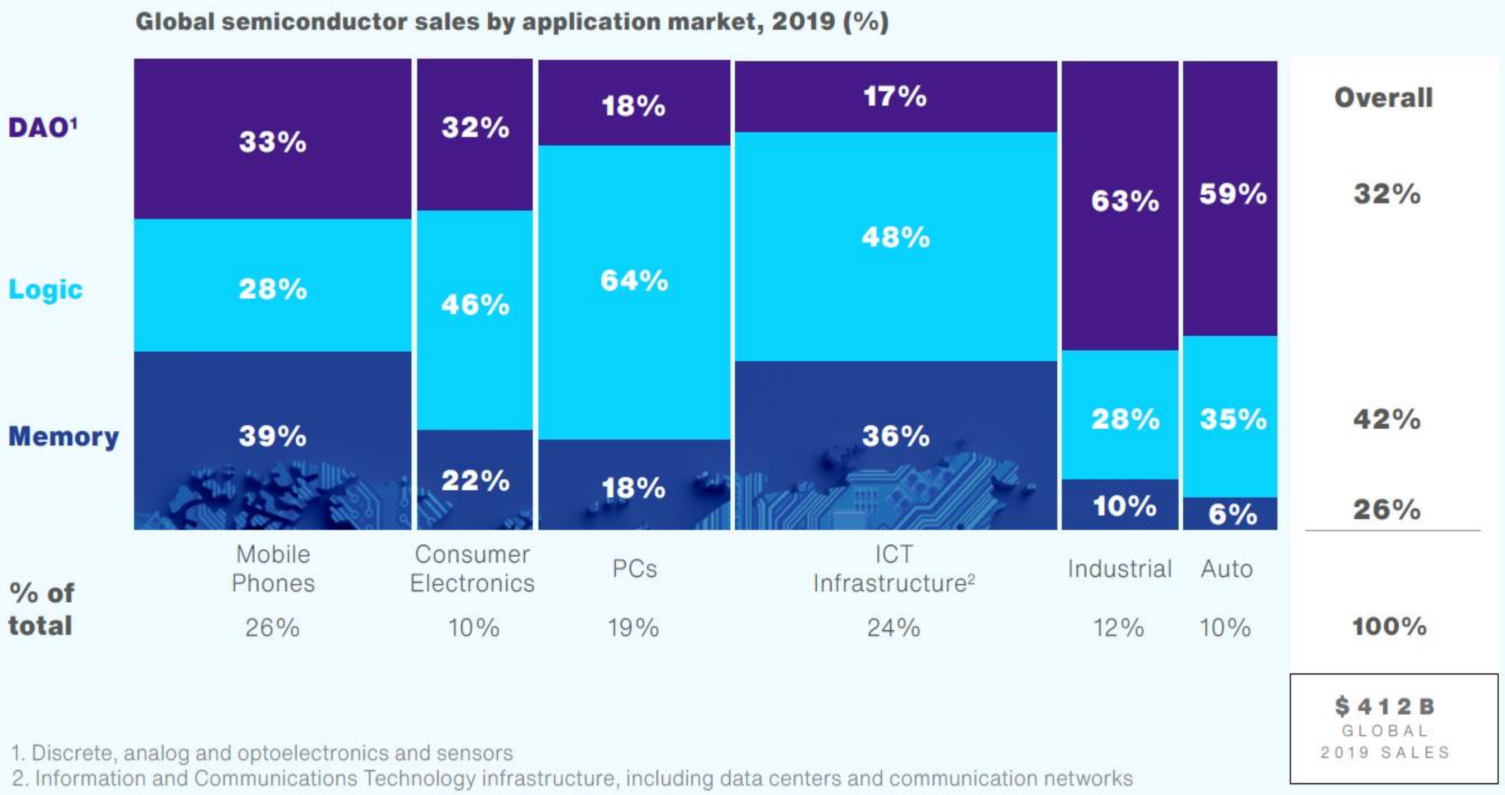
*Covers only the Internet connection portion of systems.

Source: IC Insights

Source: IC Insights

- ❑ The fastest-growing chip markets are automotive, IoT, medical and wearables

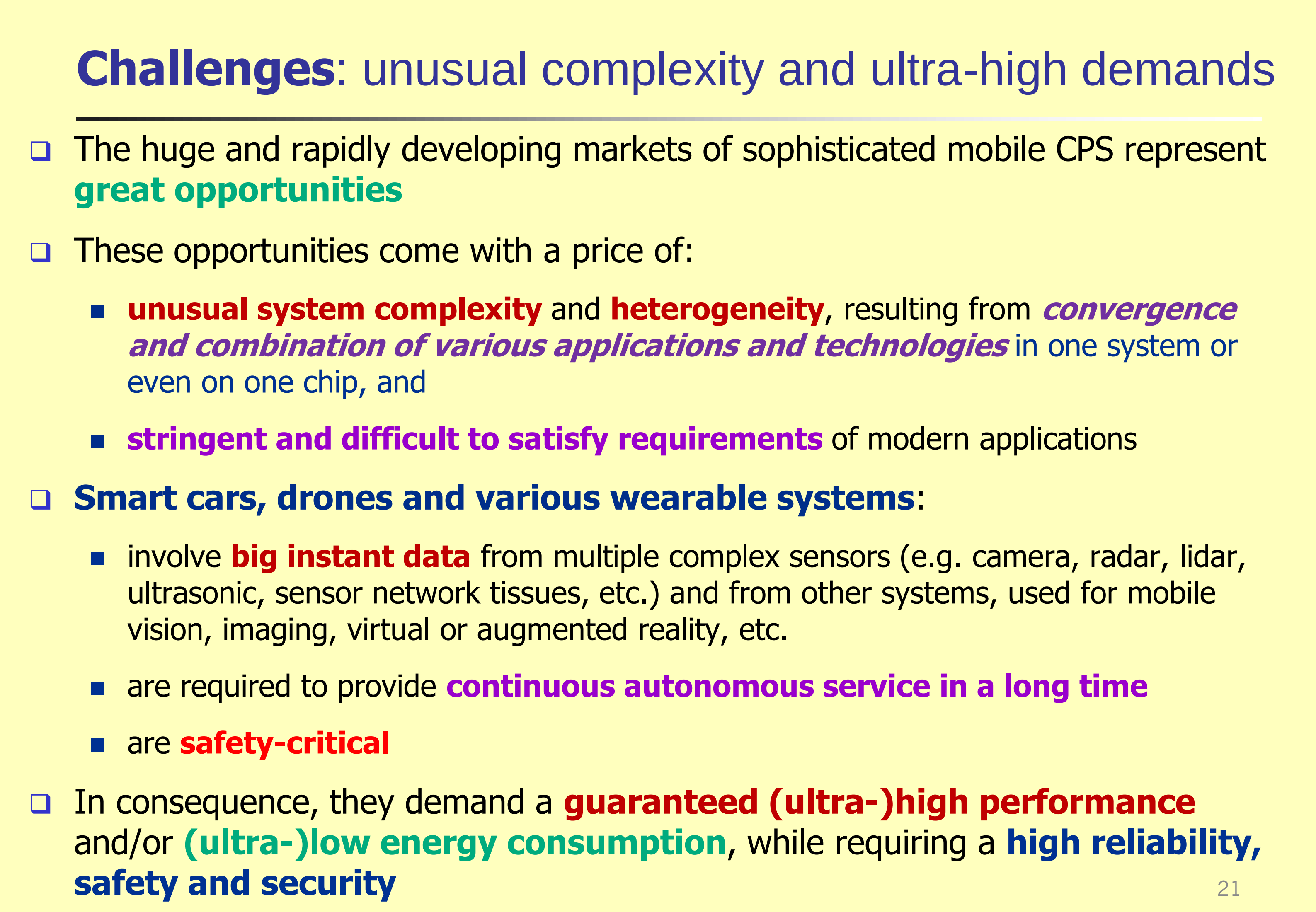
Semiconductor market related to CPS and IoT in 2019



1. Discrete, analog and optoelectronics and sensors
2. Information and Communications Technology infrastructure, including data centers and communication networks
Sources: SIA WSTS, Gartner

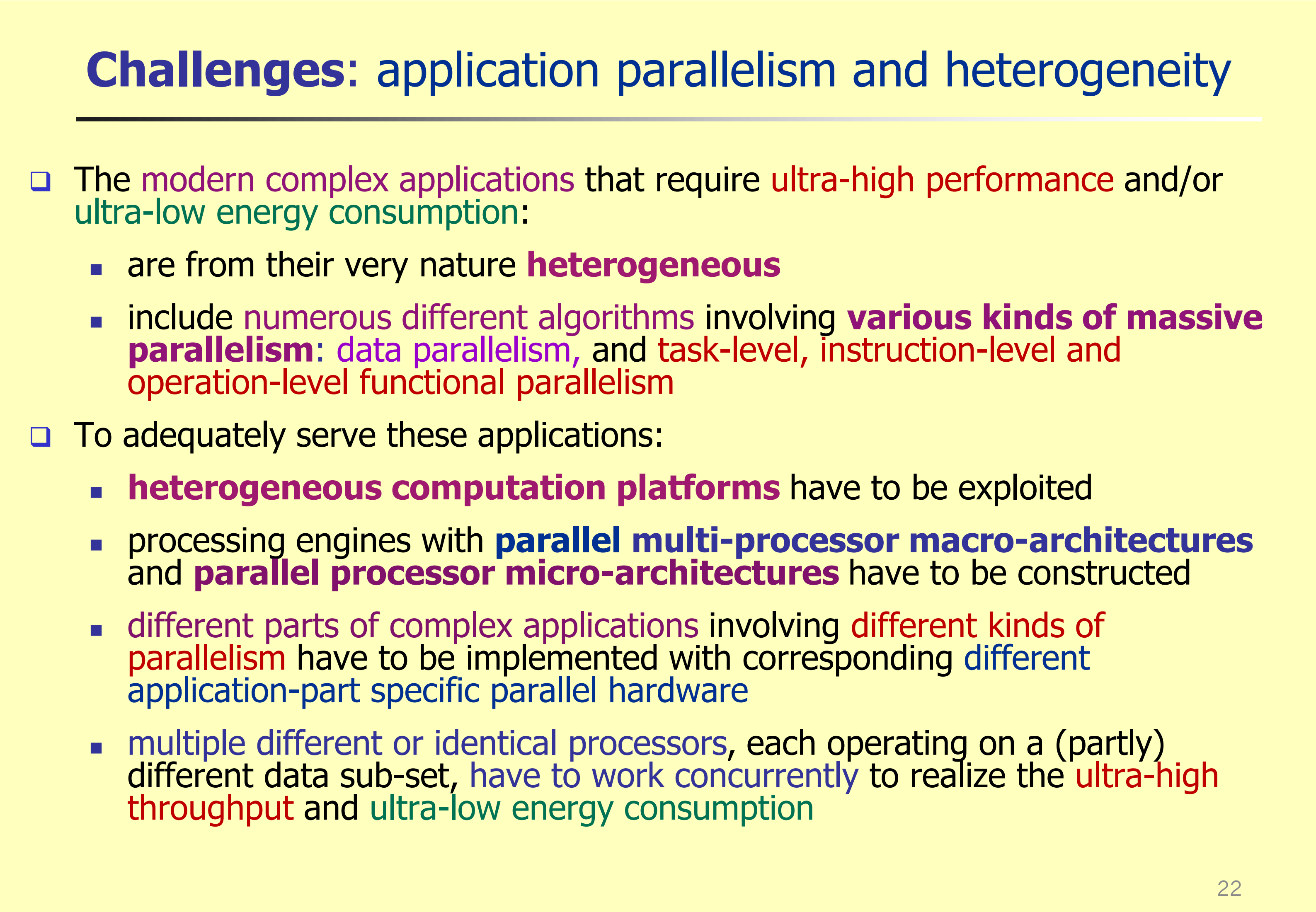
Source: SIA WSTS and Gartner

- ❑ PCs account for only 19%, while a large majority of the rest is related to CPS and IoT



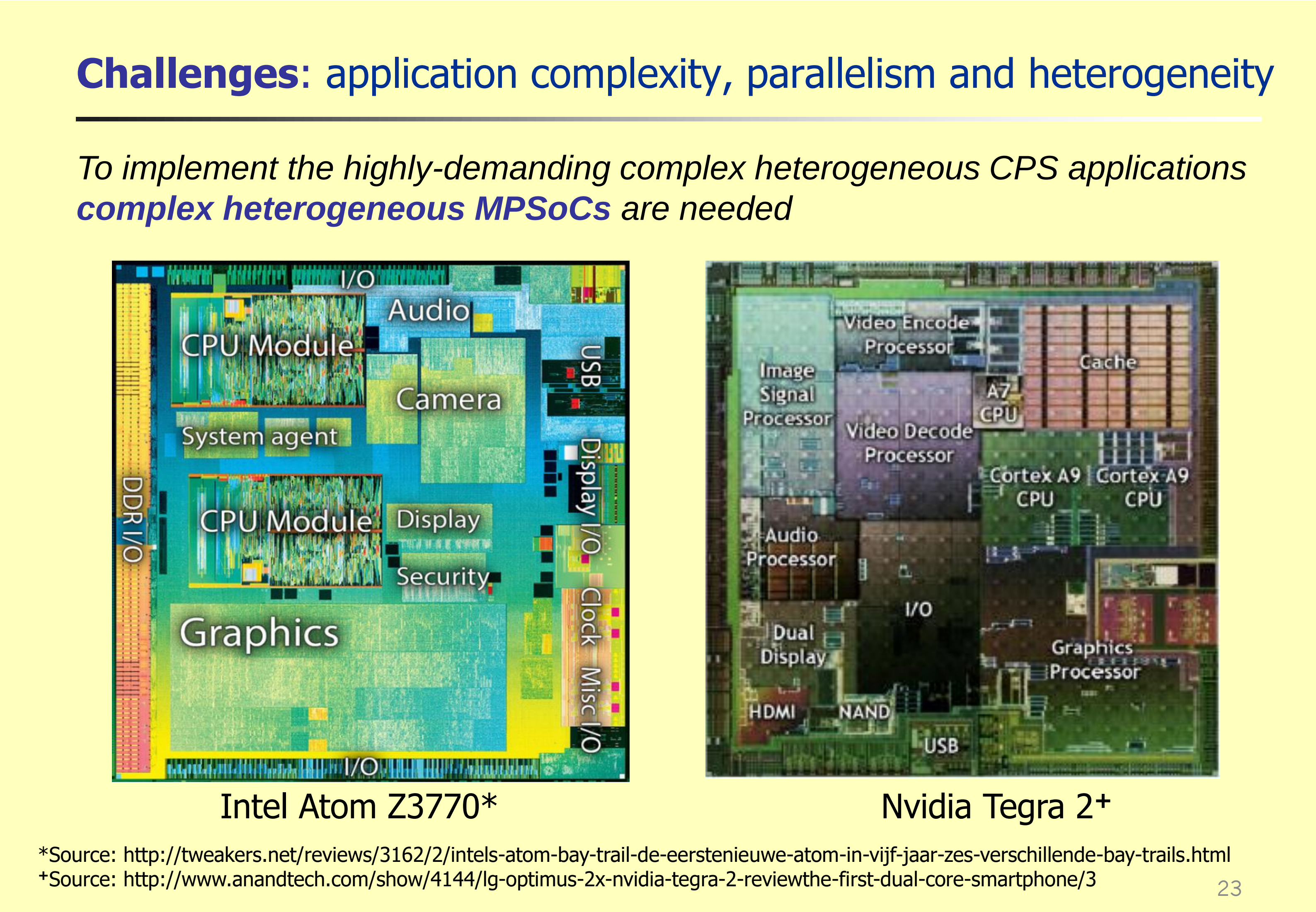
Challenges: unusual complexity and ultra-high demands

- The huge and rapidly developing markets of sophisticated mobile CPS represent **great opportunities**
- These opportunities come with a price of:
  - **unusual system complexity** and **heterogeneity**, resulting from ***convergence and combination of various applications and technologies*** in one system or even on one chip, and
  - **stringent and difficult to satisfy requirements** of modern applications
- **Smart cars, drones and various wearable systems**:
  - involve **big instant data** from multiple complex sensors (e.g. camera, radar, lidar, ultrasonic, sensor network tissues, etc.) and from other systems, used for mobile vision, imaging, virtual or augmented reality, etc.
  - are required to provide **continuous autonomous service in a long time**
  - are **safety-critical**
- In consequence, they demand a **guaranteed (ultra-)high performance** and/or **(ultra-)low energy consumption**, while requiring a **high reliability, safety and security**



Challenges: application parallelism and heterogeneity

- The modern complex applications that require ultra-high performance and/or ultra-low energy consumption:
  - are from their very nature **heterogeneous**
  - include numerous different algorithms involving **various kinds of massive parallelism**: data parallelism, and task-level, instruction-level and operation-level functional parallelism
- To adequately serve these applications:
  - **heterogeneous computation platforms** have to be exploited
  - processing engines with **parallel multi-processor macro-architectures** and **parallel processor micro-architectures** have to be constructed
  - different parts of complex applications involving different kinds of parallelism have to be implemented with corresponding different application-part specific parallel hardware
  - multiple different or identical processors, each operating on a (partly) different data sub-set, have to work concurrently to realize the ultra-high throughput and ultra-low energy consumption



Challenges: application complexity, parallelism and heterogeneity

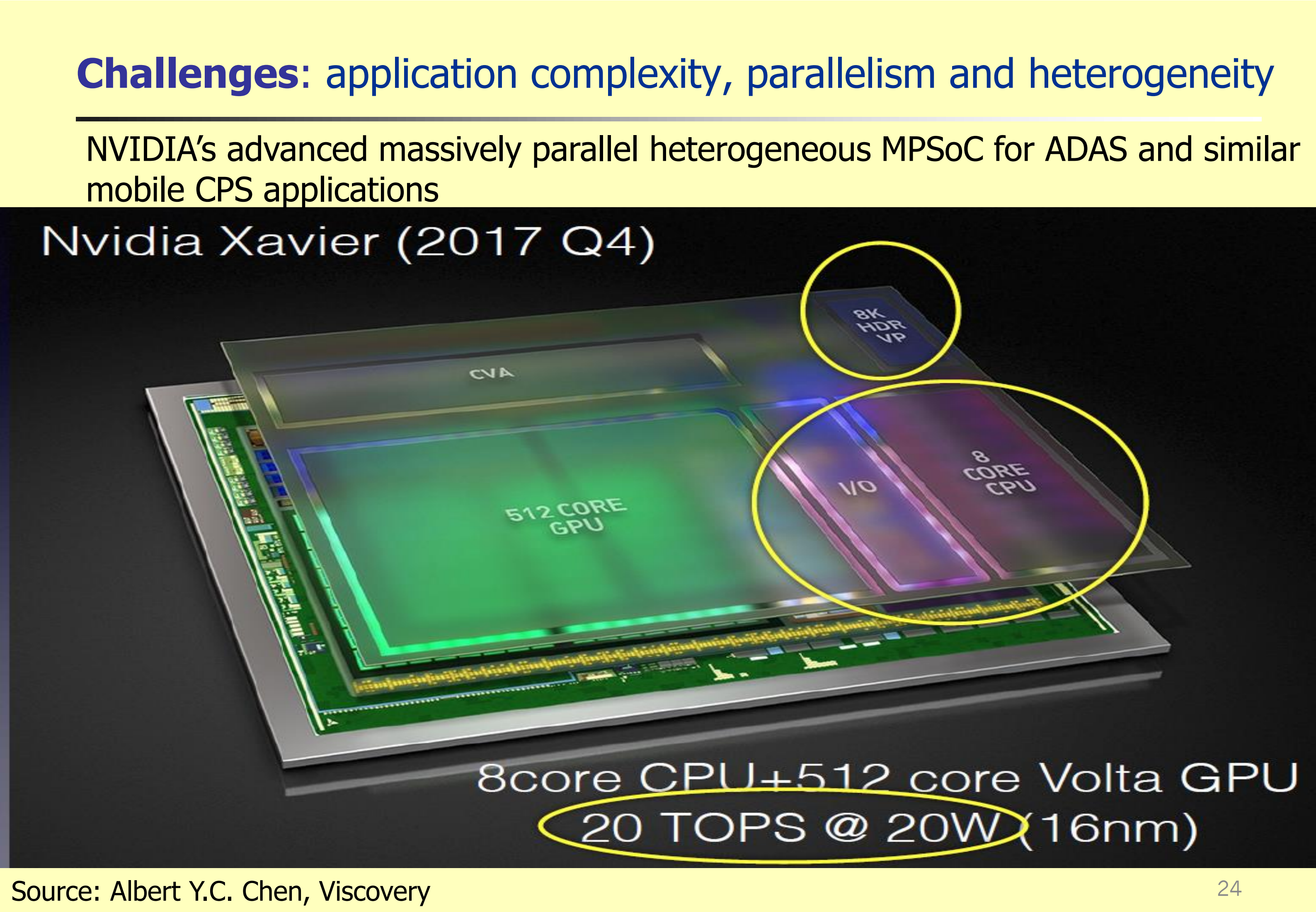
To implement the highly-demanding complex heterogeneous CPS applications ***complex heterogeneous MPSoCs*** *are needed*

Intel Atom Z3770*

Nvidia Tegra 2+

*Source: http://tweakers.net/reviews/3162/2/intels-atom-bay-trail-de-eerstenieuwe-atom-in-vijf-jaar-zes-verschillende-bay-trails.html
+Source: http://www.anandtech.com/show/4144/lg-optimus-2x-nvidia-tegra-2-reviewthe-first-dual-core-smartphone/3

23

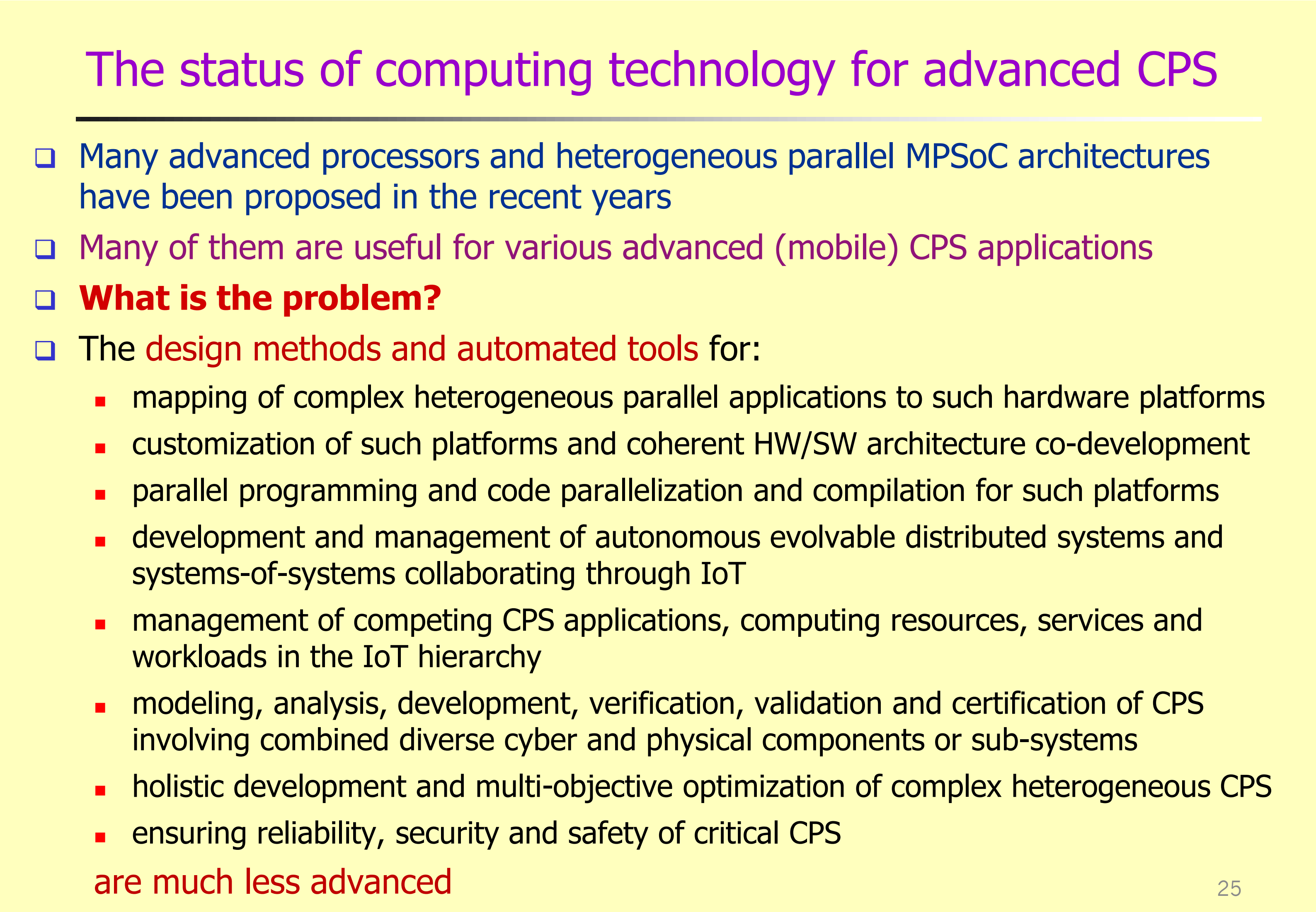


Challenges: application complexity, parallelism and heterogeneity

NVIDIA's advanced massively parallel heterogeneous MPSoC for ADAS and similar mobile CPS applications

Source: Albert Y.C. Chen, Viscovery

24

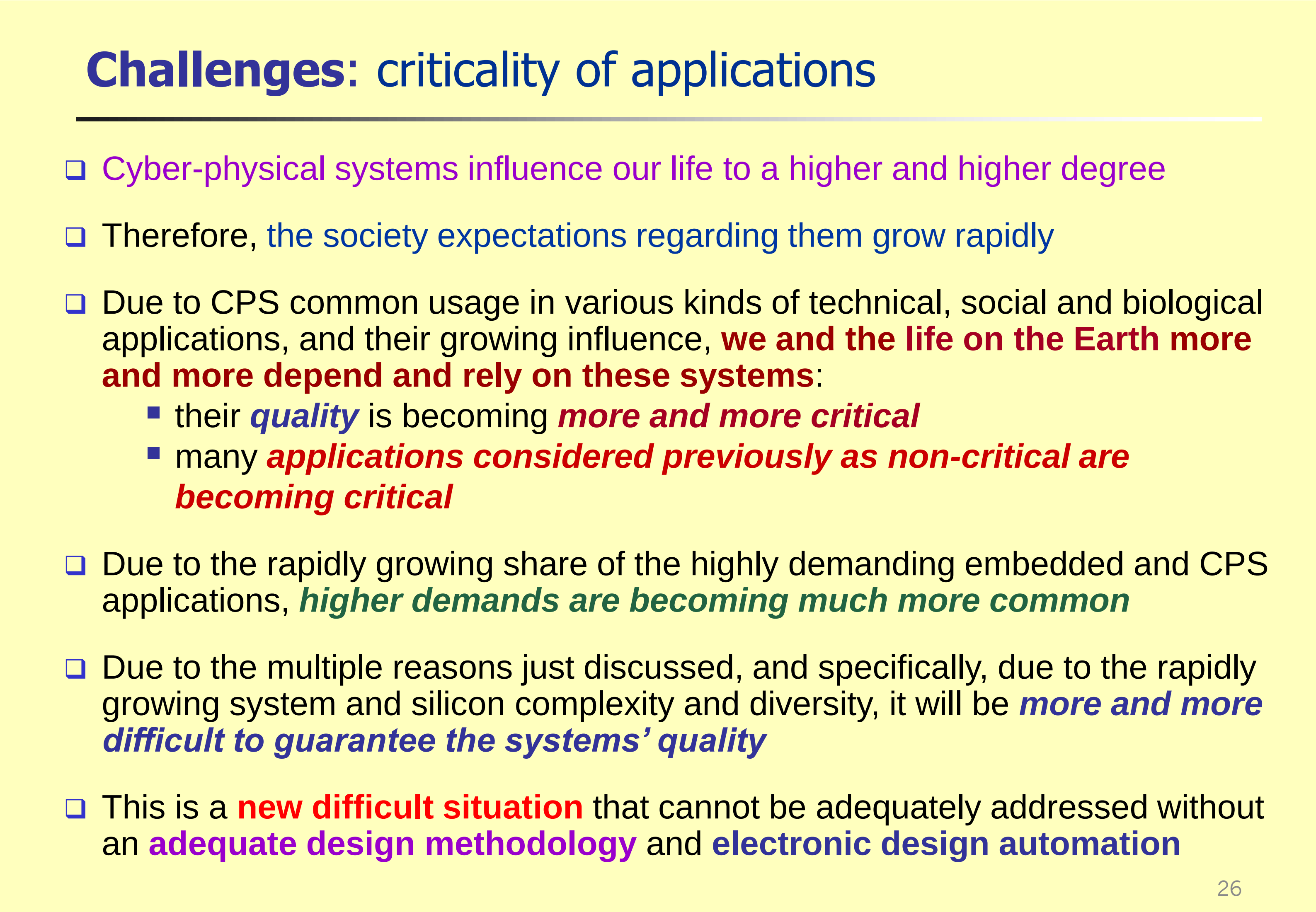


The status of computing technology for advanced CPS

- Many advanced processors and heterogeneous parallel MPSoC architectures have been proposed in the recent years
- Many of them are useful for various advanced (mobile) CPS applications
- **What is the problem?**
- The design methods and automated tools for:
  - mapping of complex heterogeneous parallel applications to such hardware platforms
  - customization of such platforms and coherent HW/SW architecture co-development
  - parallel programming and code parallelization and compilation for such platforms
  - development and management of autonomous evolvable distributed systems and systems-of-systems collaborating through IoT
  - management of competing CPS applications, computing resources, services and workloads in the IoT hierarchy
  - modeling, analysis, development, verification, validation and certification of CPS involving combined diverse cyber and physical components or sub-systems
  - holistic development and multi-objective optimization of complex heterogeneous CPS
  - ensuring reliability, security and safety of critical CPS

are much less advanced

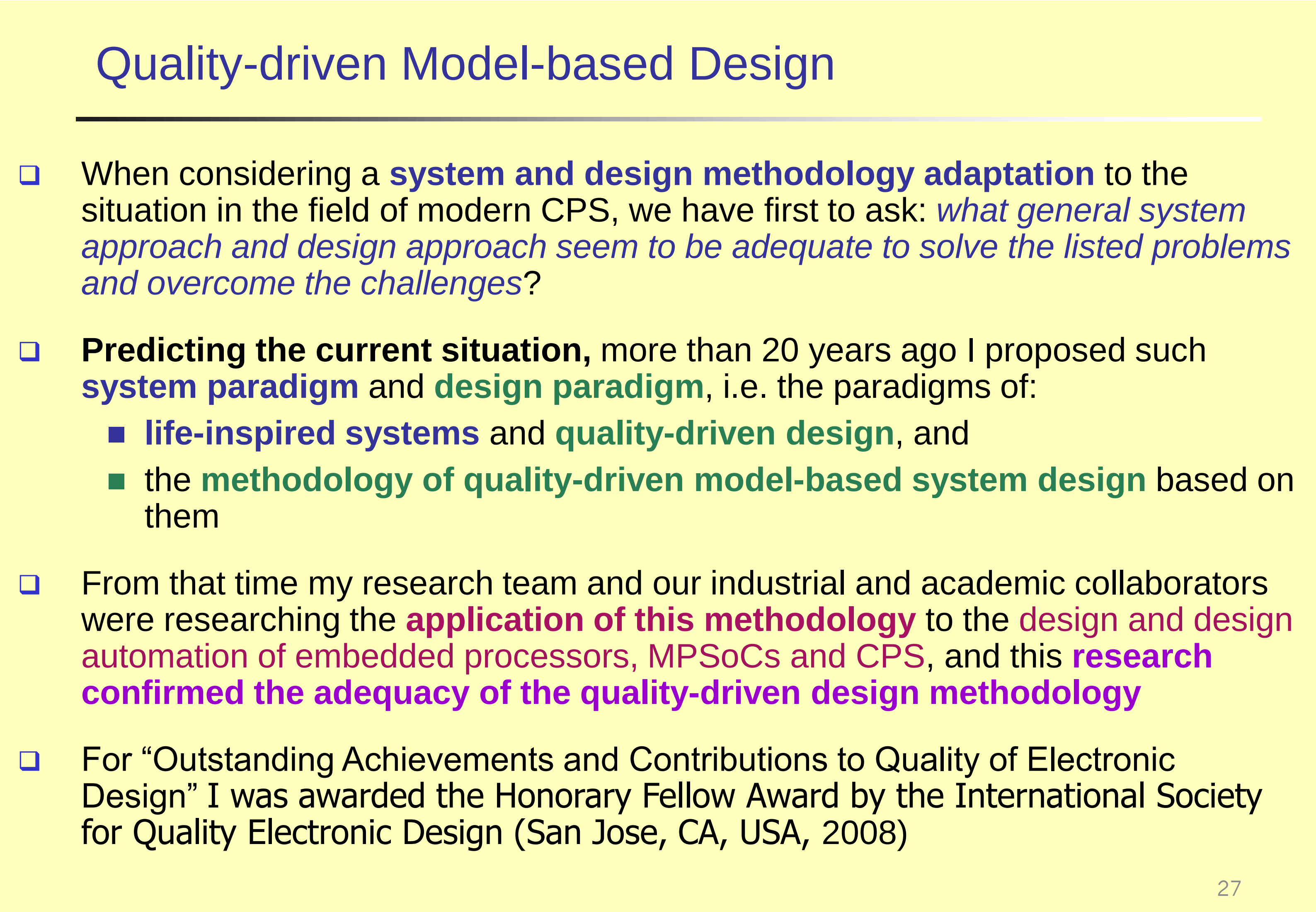
25



Challenges: criticality of applications

- Cyber-physical systems influence our life to a higher and higher degree
- Therefore, the society expectations regarding them grow rapidly
- Due to CPS common usage in various kinds of technical, social and biological applications, and their growing influence, **we and the life on the Earth more and more depend and rely on these systems**:
  - their ***quality*** is becoming ***more and more critical***
  - many ***applications considered previously as non-critical are becoming critical***
- Due to the rapidly growing share of the highly demanding embedded and CPS applications, ***higher demands are becoming much more common***
- Due to the multiple reasons just discussed, and specifically, due to the rapidly growing system and silicon complexity and diversity, it will be ***more and more difficult to guarantee the systems' quality***
- This is a **new difficult situation** that cannot be adequately addressed without an **adequate design methodology** and **electronic design automation**

26



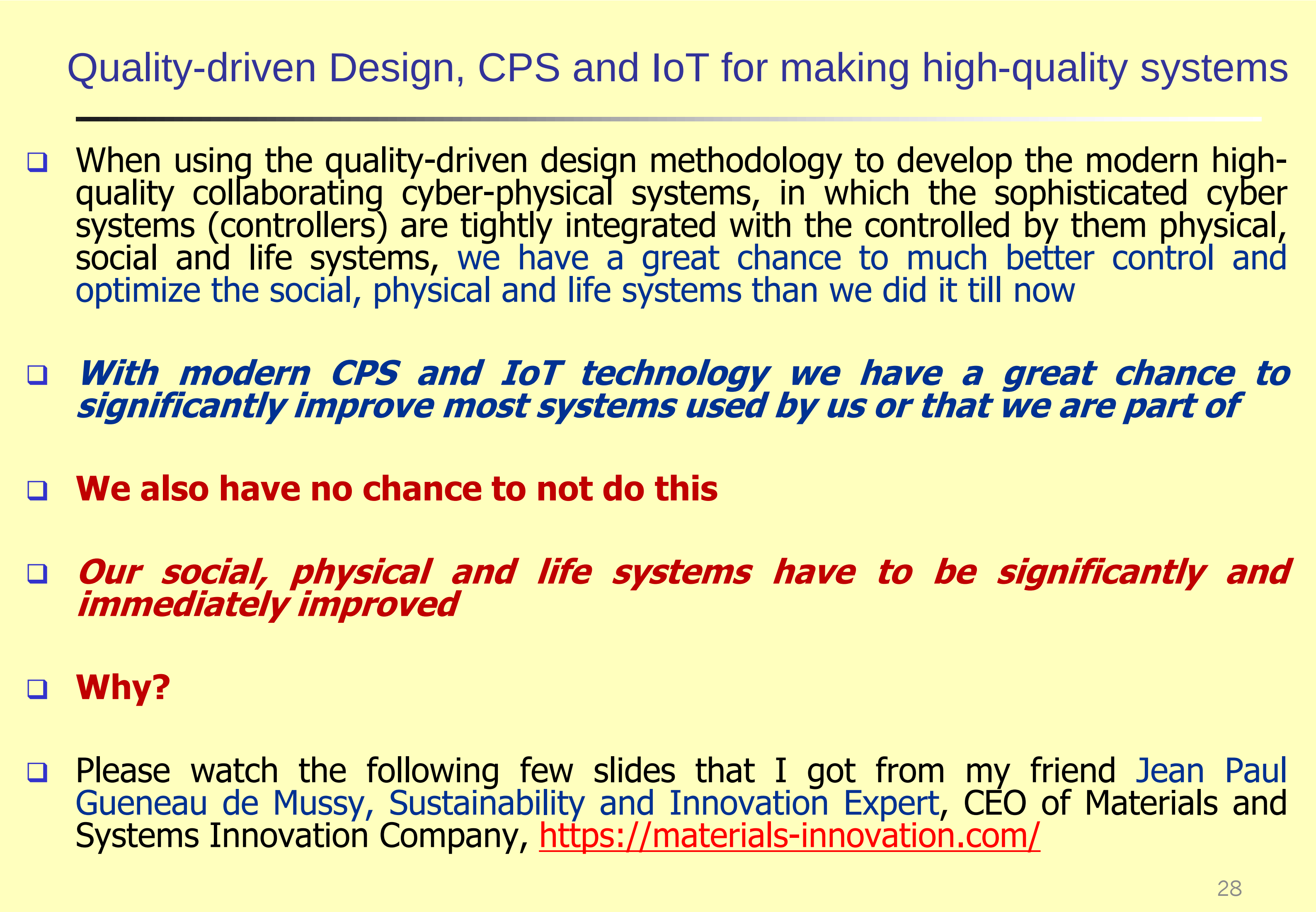
Quality-driven Model-based Design

- When considering a **system and design methodology adaptation** to the situation in the field of modern CPS, we have first to ask: *what general system approach and design approach seem to be adequate to solve the listed problems and overcome the challenges*?

- **Predicting the current situation,** more than 20 years ago I proposed such **system paradigm** and **design paradigm**, i.e. the paradigms of:
  - **life-inspired systems** and **quality-driven design**, and
  - the **methodology of quality-driven model-based system design** based on them

- From that time my research team and our industrial and academic collaborators were researching the **application of this methodology** to the design and design automation of embedded processors, MPSoCs and CPS, and this **research confirmed the adequacy of the quality-driven design methodology**

- For “Outstanding Achievements and Contributions to Quality of Electronic Design” I was awarded the Honorary Fellow Award by the International Society for Quality Electronic Design (San Jose, CA, USA, 2008)



Quality-driven Design, CPS and IoT for making high-quality systems

- ❑ When using the quality-driven design methodology to develop the modern high-quality collaborating cyber-physical systems, in which the sophisticated cyber systems (controllers) are tightly integrated with the controlled by them physical, social and life systems, we have a great chance to much better control and optimize the social, physical and life systems than we did it till now

- ❑ ***With modern CPS and IoT technology we have a great chance to significantly improve most systems used by us or that we are part of***

- ❑ **We also have no chance to not do this**

- ❑ ***Our social, physical and life systems have to be significantly and immediately improved***

- ❑ **Why?**

- ❑ Please watch the following few slides that I got from my friend Jean Paul Gueneau de Mussy, Sustainability and Innovation Expert, CEO of Materials and Systems Innovation Company, https://materials-innovation.com/

28

Overall costs of Climate Change

Jean Paul GUENEAU DE MUSSY | Materials-Innovation.com

Jean Paul GUENEAU DE MUSSY |

29

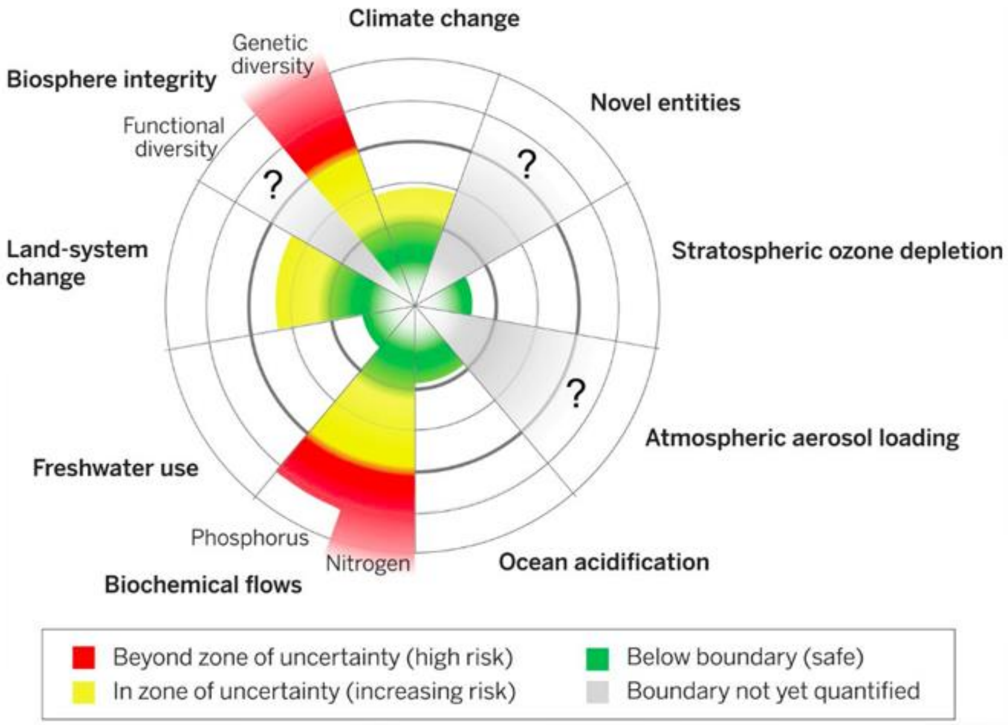
Biodiversity loss

Massive use of Resources

Jean Paul GUENEAU DE MUSSY | Materials-Innovation.com

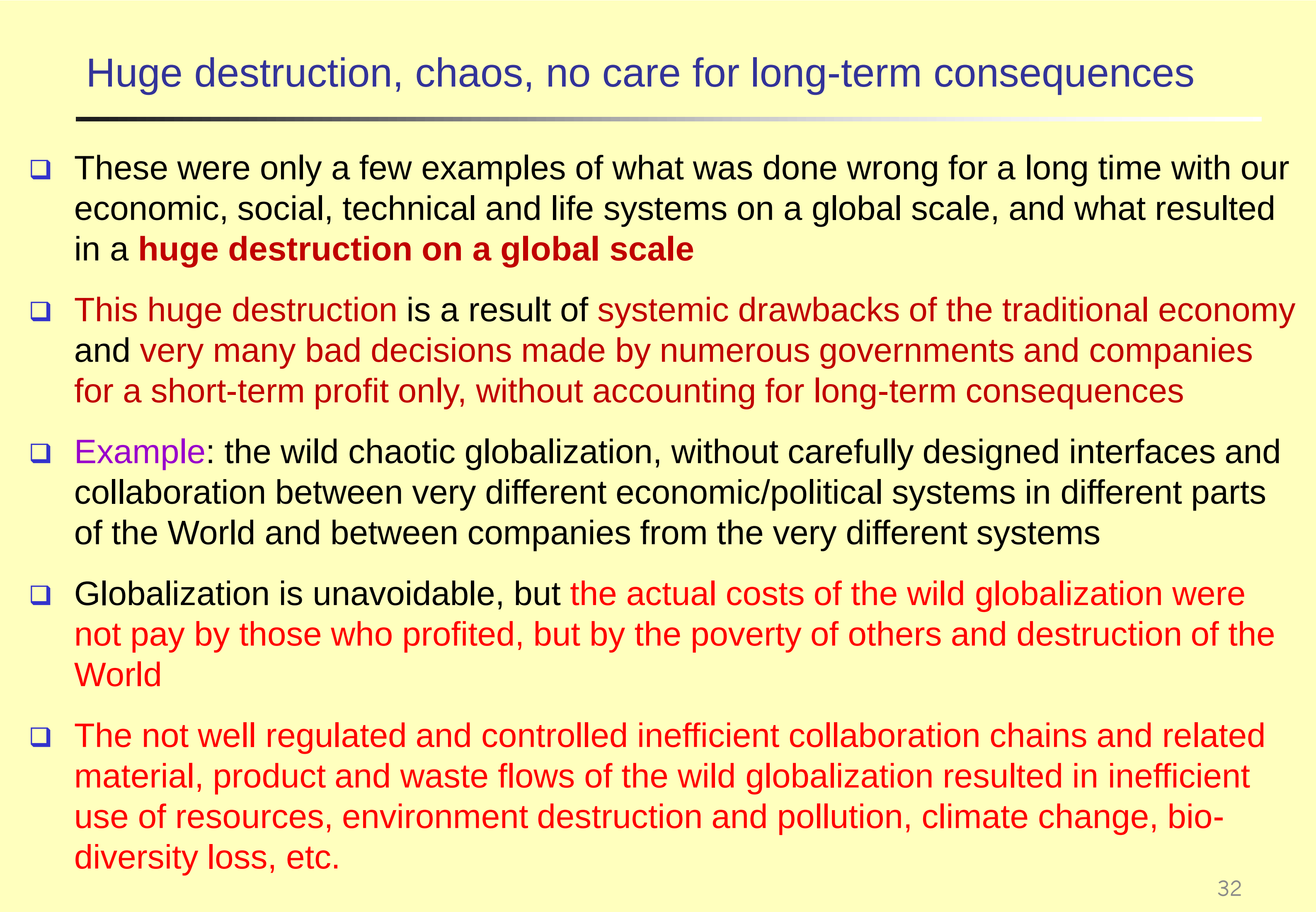
Jean Paul GUENEAU DE MUSSY |

Planetary Boundaries



Johan Rockström et all, February 2017, Volume 46, Issue 1, pp 4–17

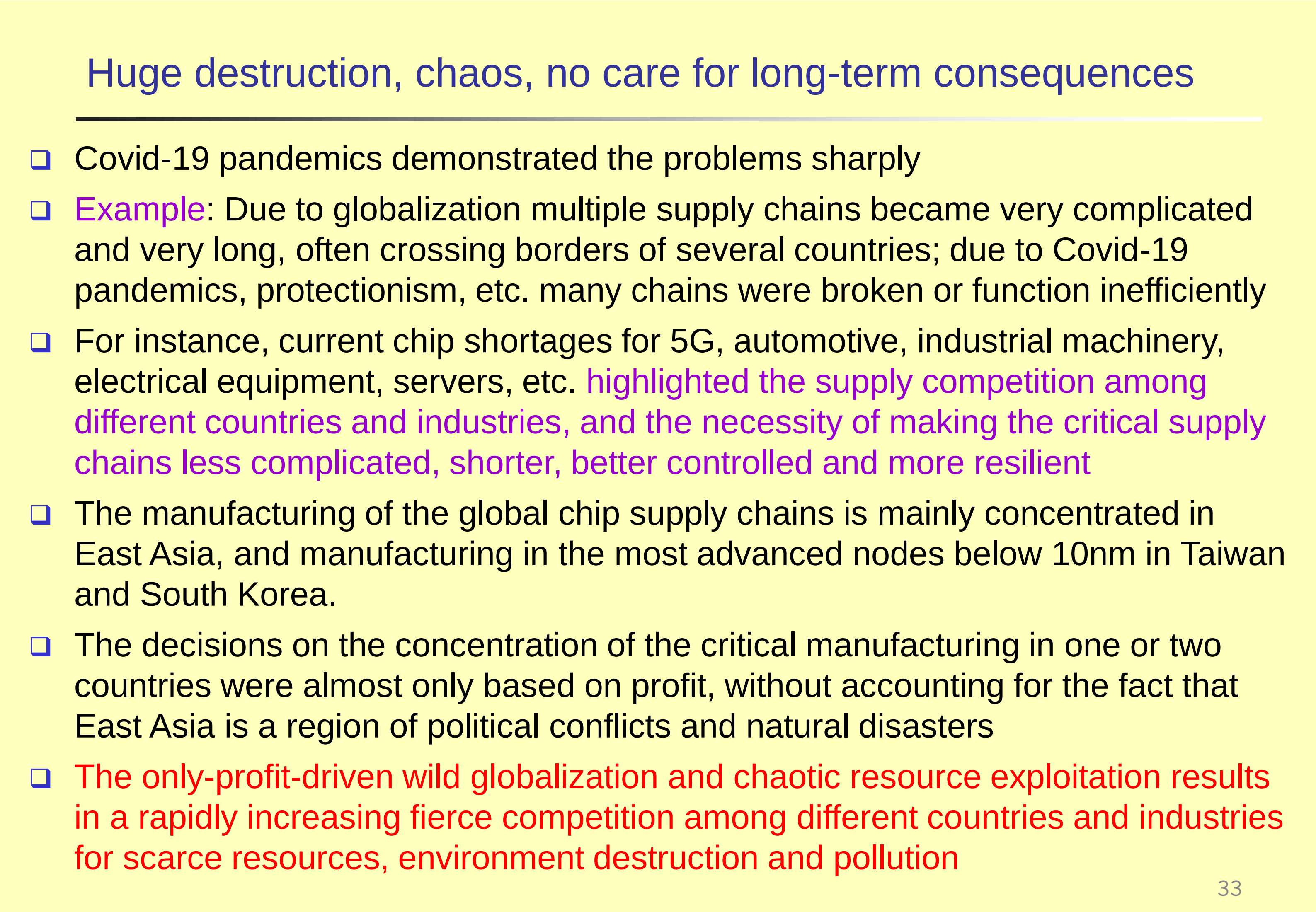
Jean Paul GUENEAU DE MUSSY |



Huge destruction, chaos, no care for long-term consequences

- These were only a few examples of what was done wrong for a long time with our economic, social, technical and life systems on a global scale, and what resulted in a **huge destruction on a global scale**
- This huge destruction is a result of systemic drawbacks of the traditional economy and very many bad decisions made by numerous governments and companies for a short-term profit only, without accounting for long-term consequences
- Example: the wild chaotic globalization, without carefully designed interfaces and collaboration between very different economic/political systems in different parts of the World and between companies from the very different systems
- Globalization is unavoidable, but the actual costs of the wild globalization were not pay by those who profited, but by the poverty of others and destruction of the World
- The not well regulated and controlled inefficient collaboration chains and related material, product and waste flows of the wild globalization resulted in inefficient use of resources, environment destruction and pollution, climate change, bio-diversity loss, etc.

32



Huge destruction, chaos, no care for long-term consequences

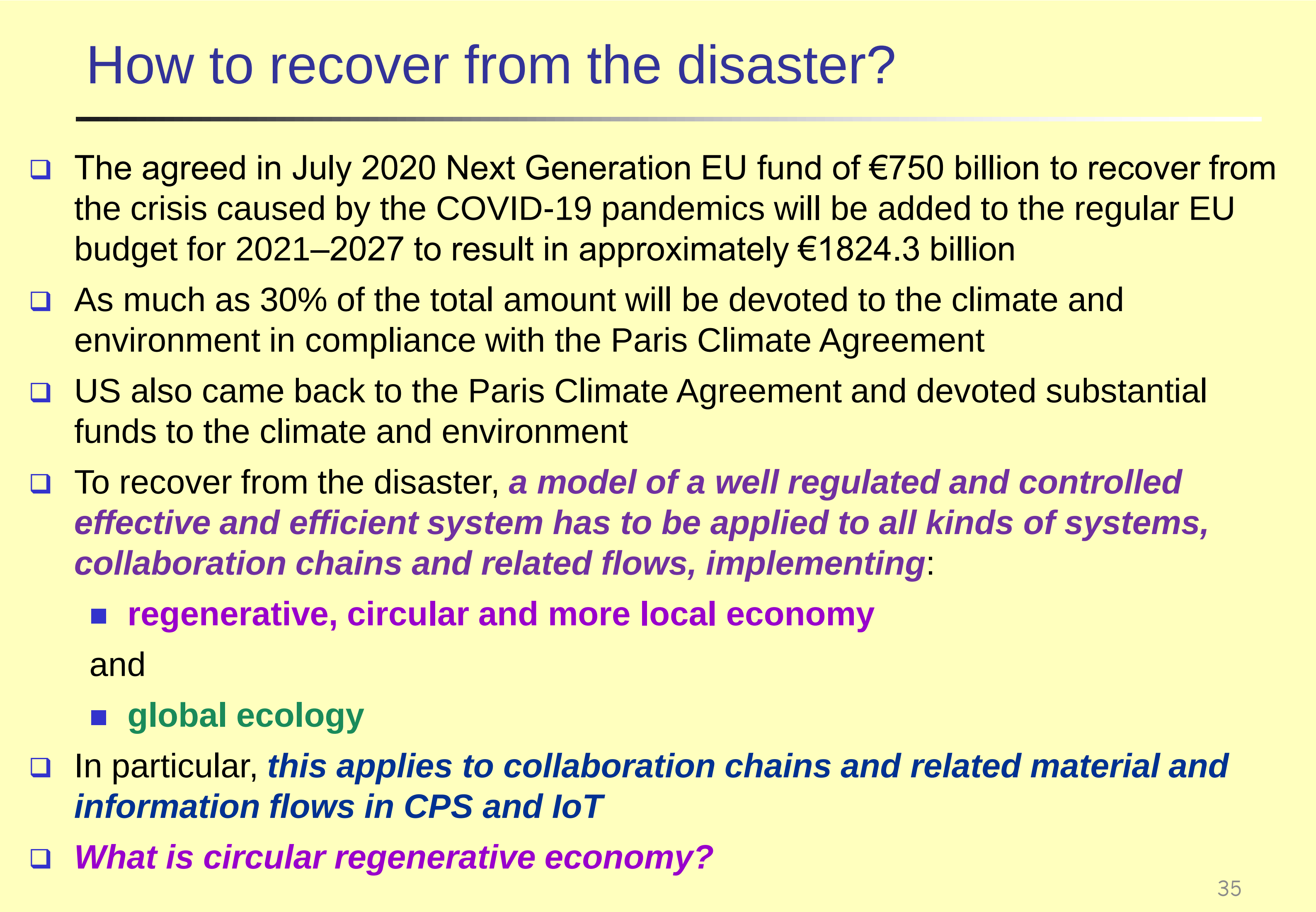
- Covid-19 pandemics demonstrated the problems sharply
- Example: Due to globalization multiple supply chains became very complicated and very long, often crossing borders of several countries; due to Covid-19 pandemics, protectionism, etc. many chains were broken or function inefficiently
- For instance, current chip shortages for 5G, automotive, industrial machinery, electrical equipment, servers, etc. highlighted the supply competition among different countries and industries, and the necessity of making the critical supply chains less complicated, shorter, better controlled and more resilient
- The manufacturing of the global chip supply chains is mainly concentrated in East Asia, and manufacturing in the most advanced nodes below 10nm in Taiwan and South Korea.
- The decisions on the concentration of the critical manufacturing in one or two countries were almost only based on profit, without accounting for the fact that East Asia is a region of political conflicts and natural disasters
- The only-profit-driven wild globalization and chaotic resource exploitation results in a rapidly increasing fierce competition among different countries and industries for scarce resources, environment destruction and pollution

33

EUROPE Recognizes the CLIMATE and POLUTION CRISIS and starts to take serious measures

EU President **Ursula von der Leyen** unveiled Europe's "**Green Deal**" plan to fight the crises on Dec. 11, 2019

It represents a stepwise incremental approach to solve the problems

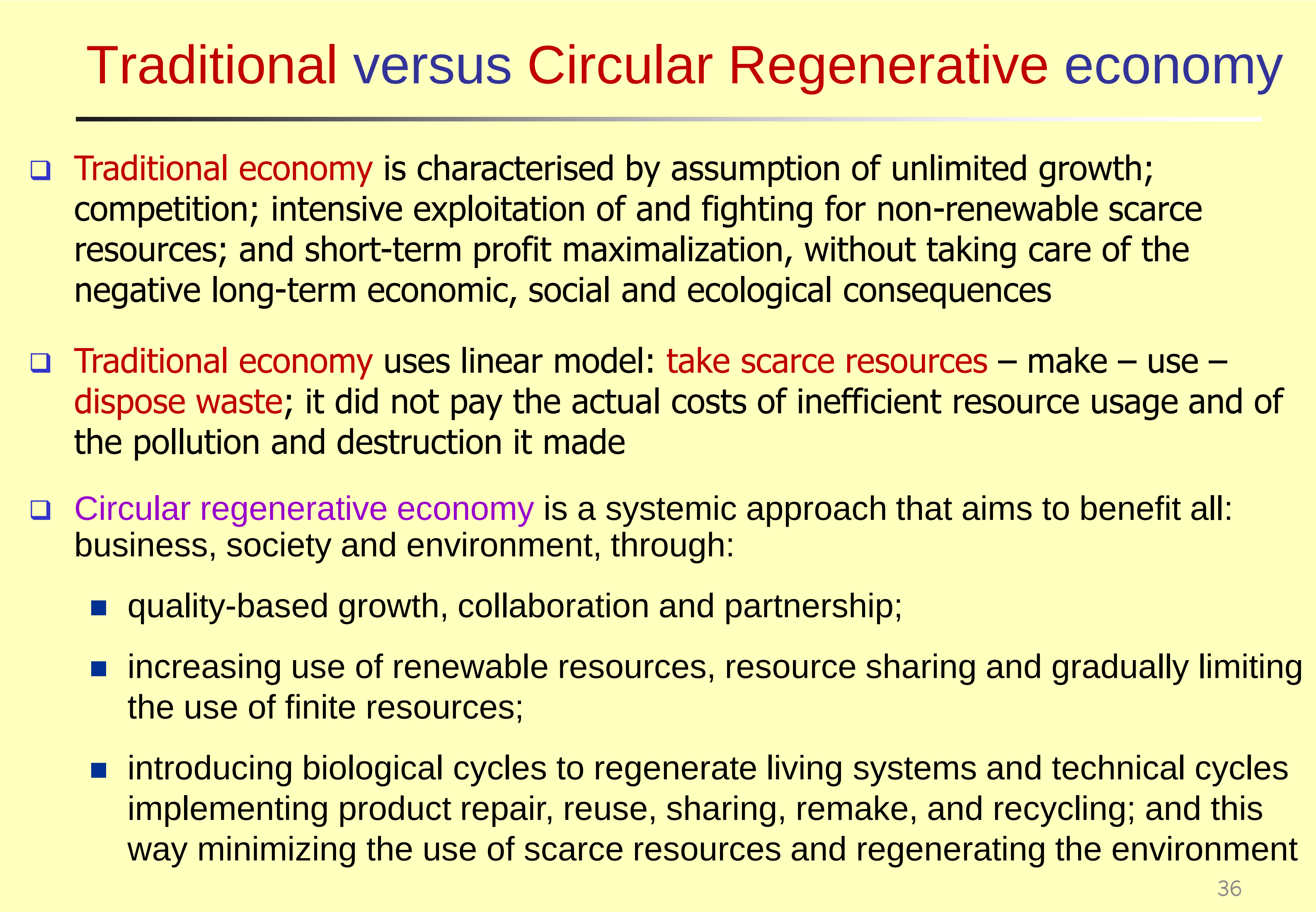


How to recover from the disaster?

- The agreed in July 2020 Next Generation EU fund of €750 billion to recover from the crisis caused by the COVID-19 pandemics will be added to the regular EU budget for 2021–2027 to result in approximately €1824.3 billion
- As much as 30% of the total amount will be devoted to the climate and environment in compliance with the Paris Climate Agreement
- US also came back to the Paris Climate Agreement and devoted substantial funds to the climate and environment
- To recover from the disaster, ***a model of a well regulated and controlled effective and efficient system has to be applied to all kinds of systems, collaboration chains and related flows, implementing***:
  - **regenerative, circular and more local economy**

  and

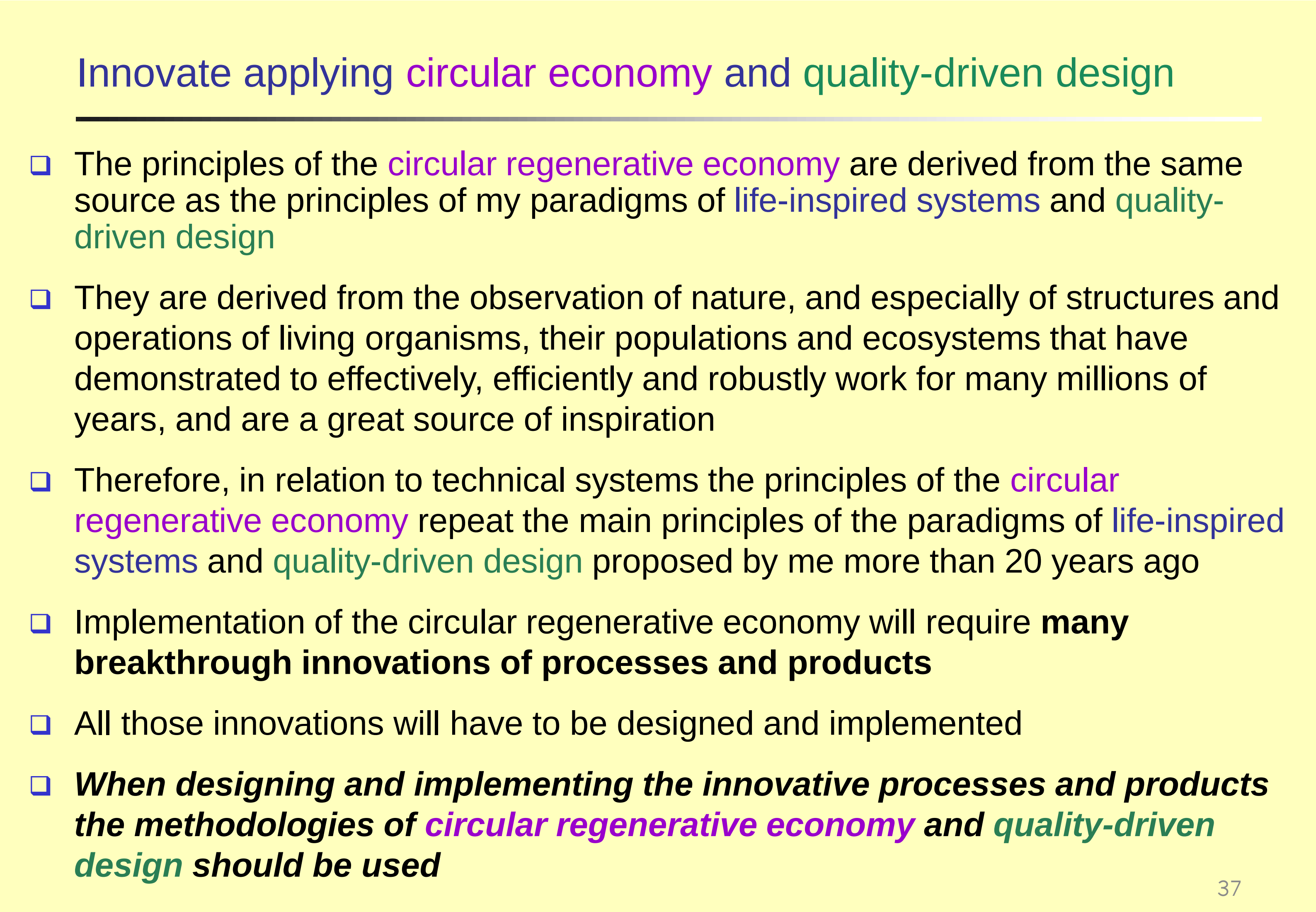
  - **global ecology**
- In particular, ***this applies to collaboration chains and related material and information flows in CPS and IoT***
- ***What is circular regenerative economy?***



Traditional versus Circular Regenerative economy

- Traditional economy is characterised by assumption of unlimited growth; competition; intensive exploitation of and fighting for non-renewable scarce resources; and short-term profit maximalization, without taking care of the negative long-term economic, social and ecological consequences
- Traditional economy uses linear model: take scarce resources – make – use – dispose waste; it did not pay the actual costs of inefficient resource usage and of the pollution and destruction it made
- Circular regenerative economy is a systemic approach that aims to benefit all: business, society and environment, through:
    - quality-based growth, collaboration and partnership;
    - increasing use of renewable resources, resource sharing and gradually limiting the use of finite resources;
    - introducing biological cycles to regenerate living systems and technical cycles implementing product repair, reuse, sharing, remake, and recycling; and this way minimizing the use of scarce resources and regenerating the environment

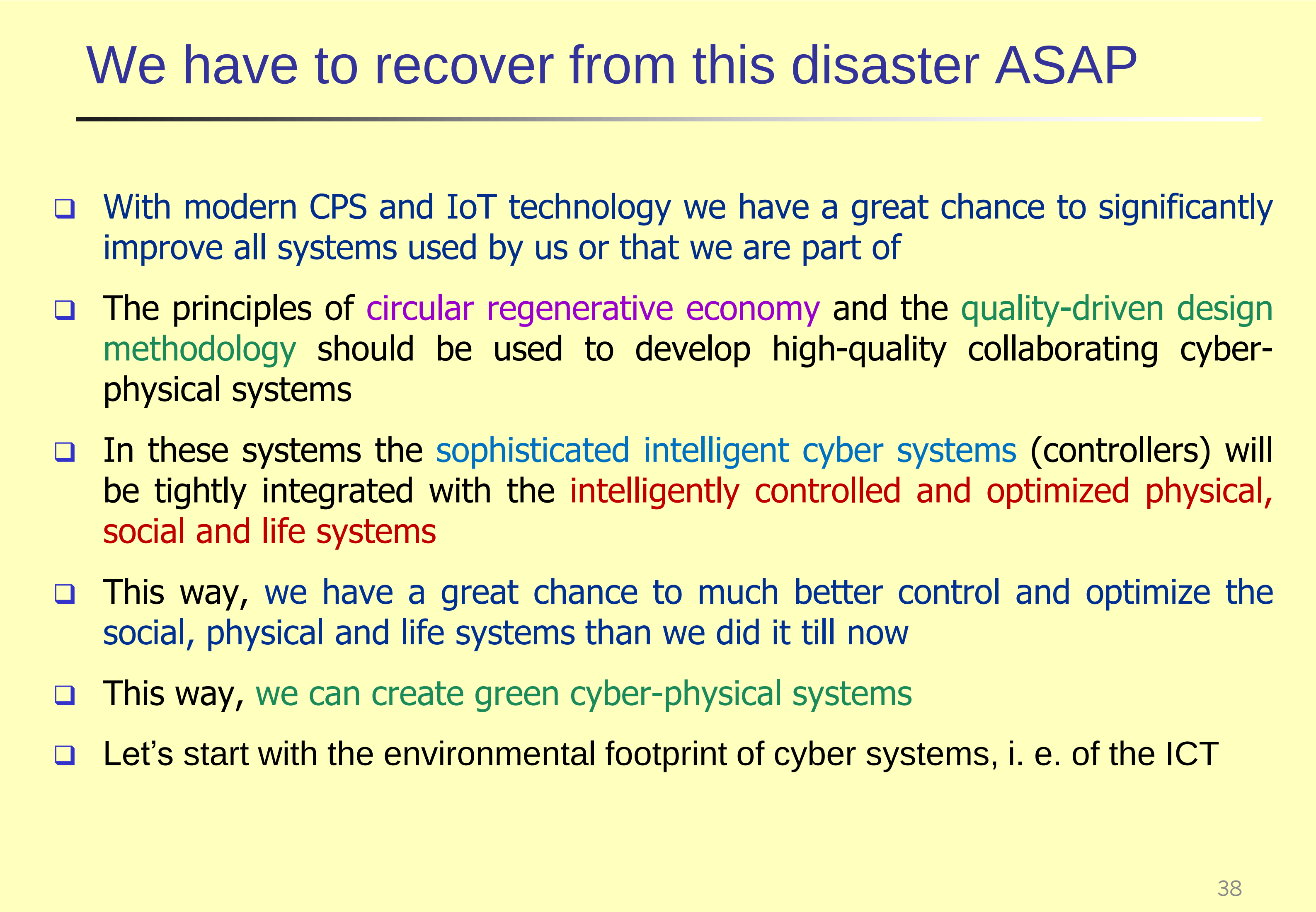
36



Innovate applying circular economy and quality-driven design

- The principles of the circular regenerative economy are derived from the same source as the principles of my paradigms of life-inspired systems and quality-driven design
- They are derived from the observation of nature, and especially of structures and operations of living organisms, their populations and ecosystems that have demonstrated to effectively, efficiently and robustly work for many millions of years, and are a great source of inspiration
- Therefore, in relation to technical systems the principles of the circular regenerative economy repeat the main principles of the paradigms of life-inspired systems and quality-driven design proposed by me more than 20 years ago
- Implementation of the circular regenerative economy will require **many breakthrough innovations of processes and products**
- All those innovations will have to be designed and implemented
- ***When designing and implementing the innovative processes and products the methodologies of circular regenerative economy and quality-driven design should be used***

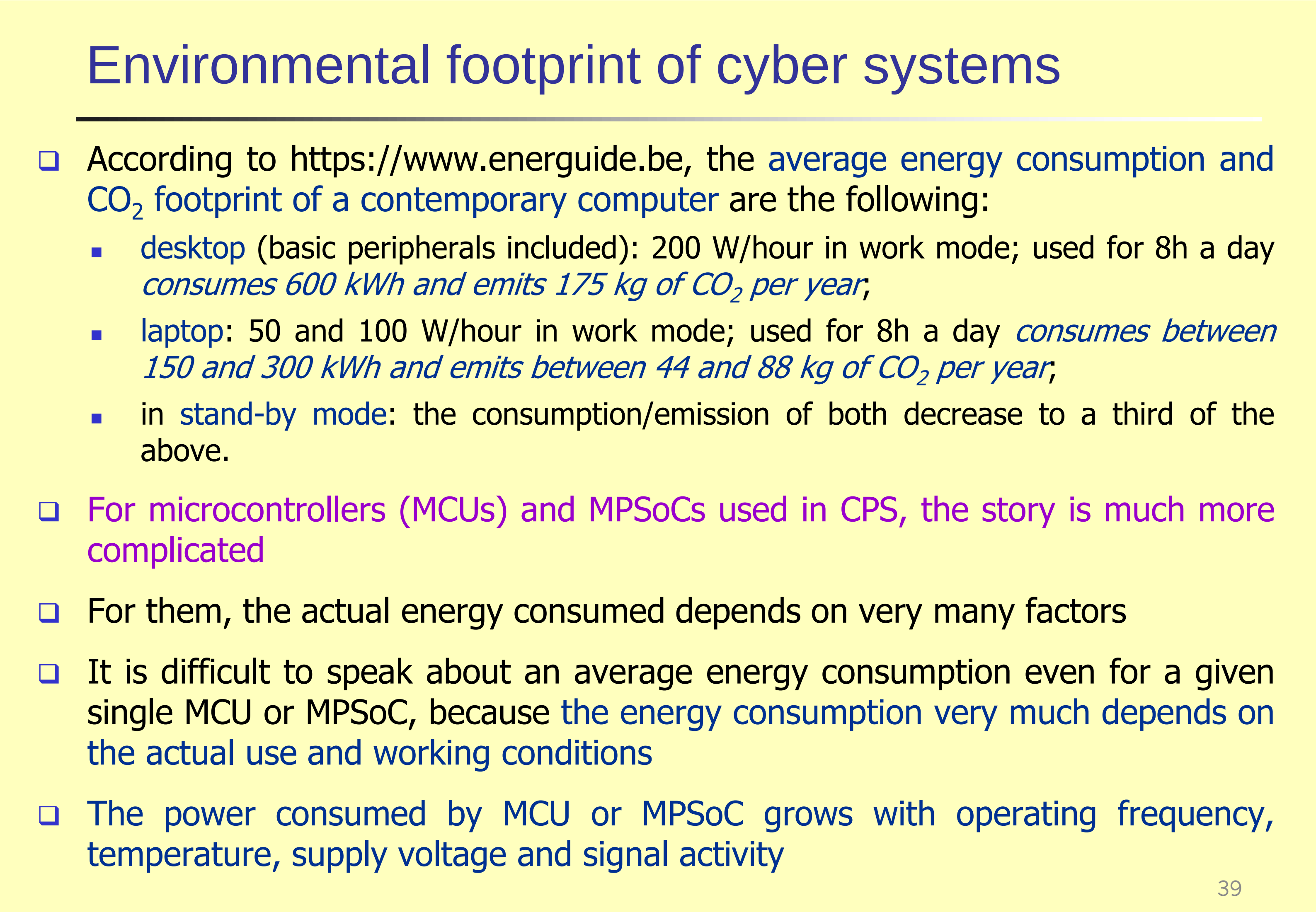
37



We have to recover from this disaster ASAP

- ❑ With modern CPS and IoT technology we have a great chance to significantly improve all systems used by us or that we are part of
- ❑ The principles of circular regenerative economy and the quality-driven design methodology should be used to develop high-quality collaborating cyber-physical systems
- ❑ In these systems the sophisticated intelligent cyber systems (controllers) will be tightly integrated with the intelligently controlled and optimized physical, social and life systems
- ❑ This way, we have a great chance to much better control and optimize the social, physical and life systems than we did it till now
- ❑ This way, we can create green cyber-physical systems
- ❑ Let's start with the environmental footprint of cyber systems, i. e. of the ICT

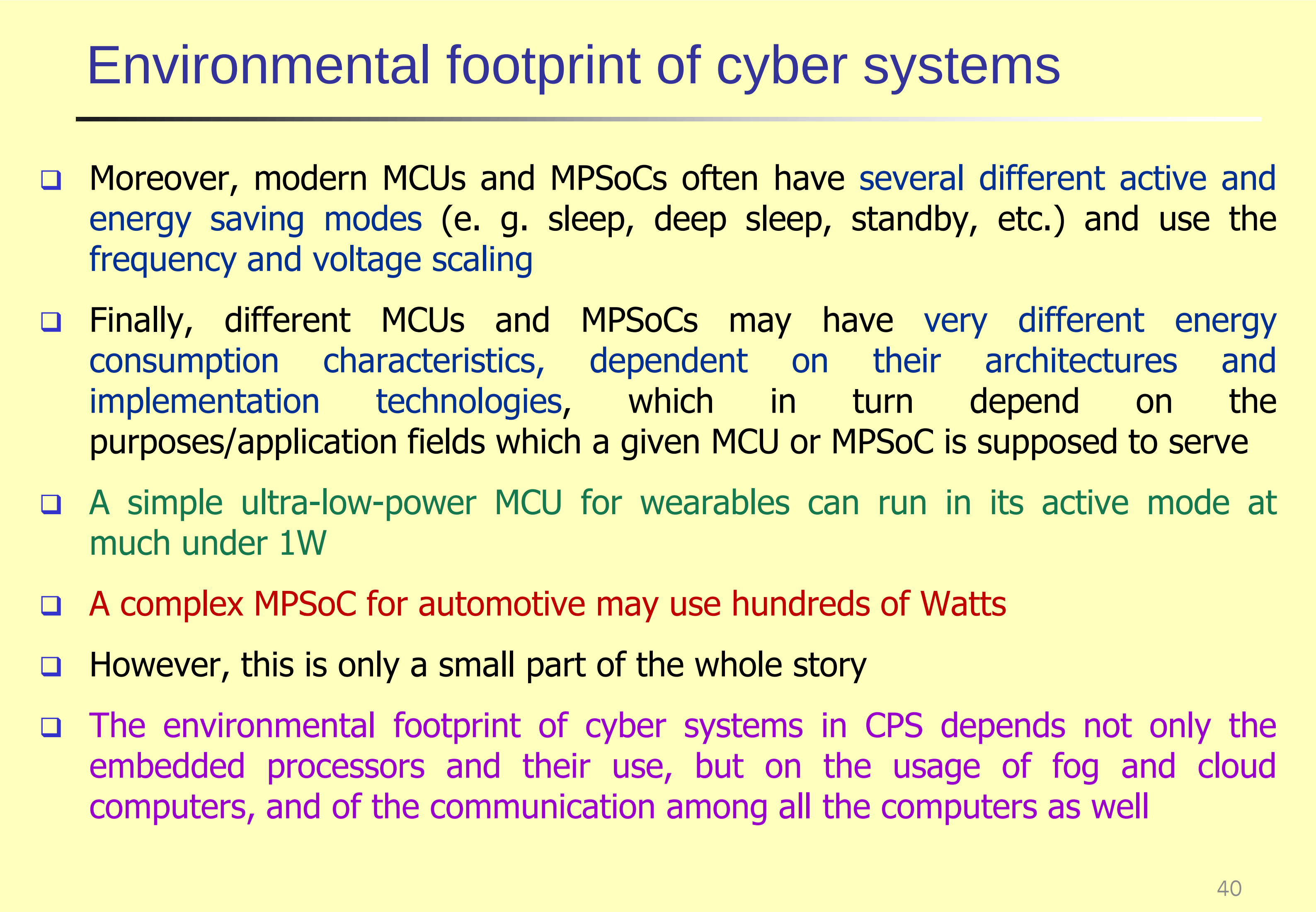
38



Environmental footprint of cyber systems

- According to https://www.energuide.be, the average energy consumption and CO_2 footprint of a contemporary computer are the following:
  - desktop (basic peripherals included): 200 W/hour in work mode; used for 8h a day *consumes 600 kWh and emits 175 kg of CO_2 per year*;
  - laptop: 50 and 100 W/hour in work mode; used for 8h a day *consumes between 150 and 300 kWh and emits between 44 and 88 kg of CO_2 per year*;
  - in stand-by mode: the consumption/emission of both decrease to a third of the above.
- For microcontrollers (MCUs) and MPSoCs used in CPS, the story is much more complicated
- For them, the actual energy consumed depends on very many factors
- It is difficult to speak about an average energy consumption even for a given single MCU or MPSoC, because the energy consumption very much depends on the actual use and working conditions
- The power consumed by MCU or MPSoC grows with operating frequency, temperature, supply voltage and signal activity

39

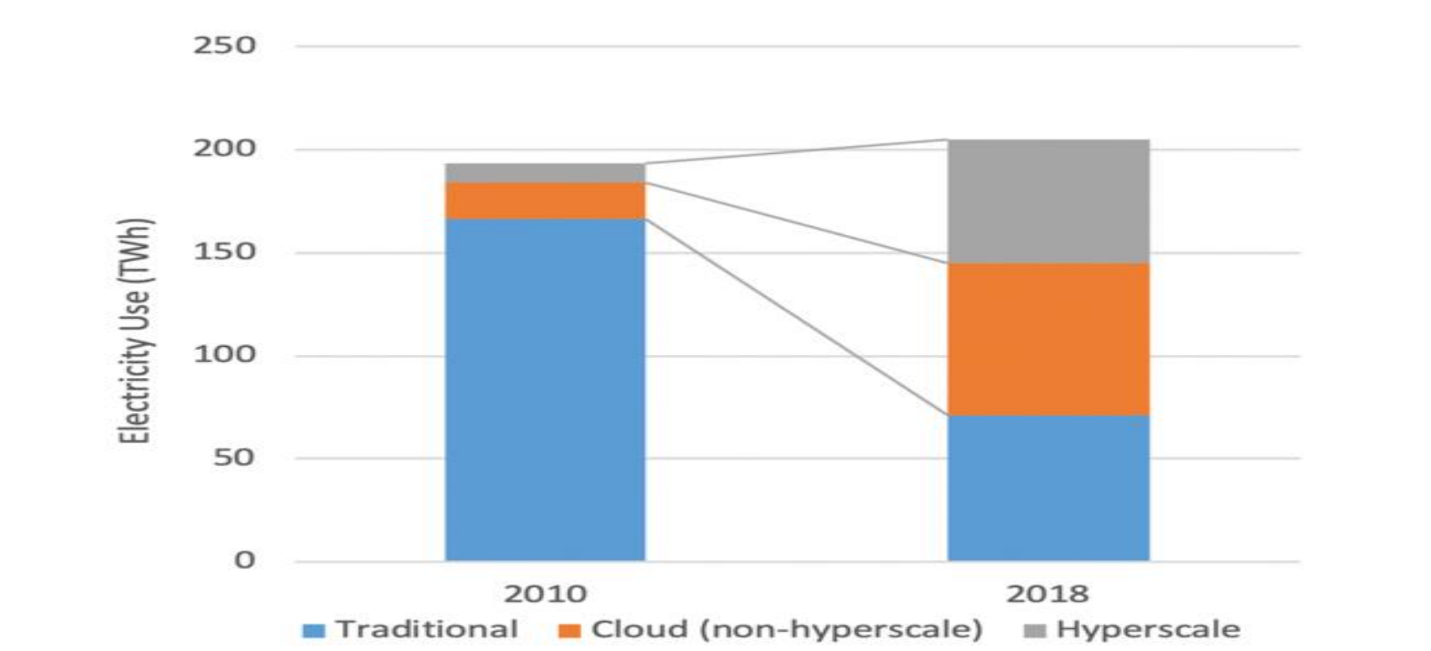


Environmental footprint of cyber systems

- Moreover, modern MCUs and MPSoCs often have several different active and energy saving modes (e. g. sleep, deep sleep, standby, etc.) and use the frequency and voltage scaling
- Finally, different MCUs and MPSoCs may have very different energy consumption characteristics, dependent on their architectures and implementation technologies, which in turn depend on the purposes/application fields which a given MCU or MPSoC is supposed to serve
- A simple ultra-low-power MCU for wearables can run in its active mode at much under 1W
- A complex MPSoC for automotive may use hundreds of Watts
- However, this is only a small part of the whole story
- The environmental footprint of cyber systems in CPS depends not only the embedded processors and their use, but on the usage of fog and cloud computers, and of the communication among all the computers as well

40

Environmental footprint of cyber systems



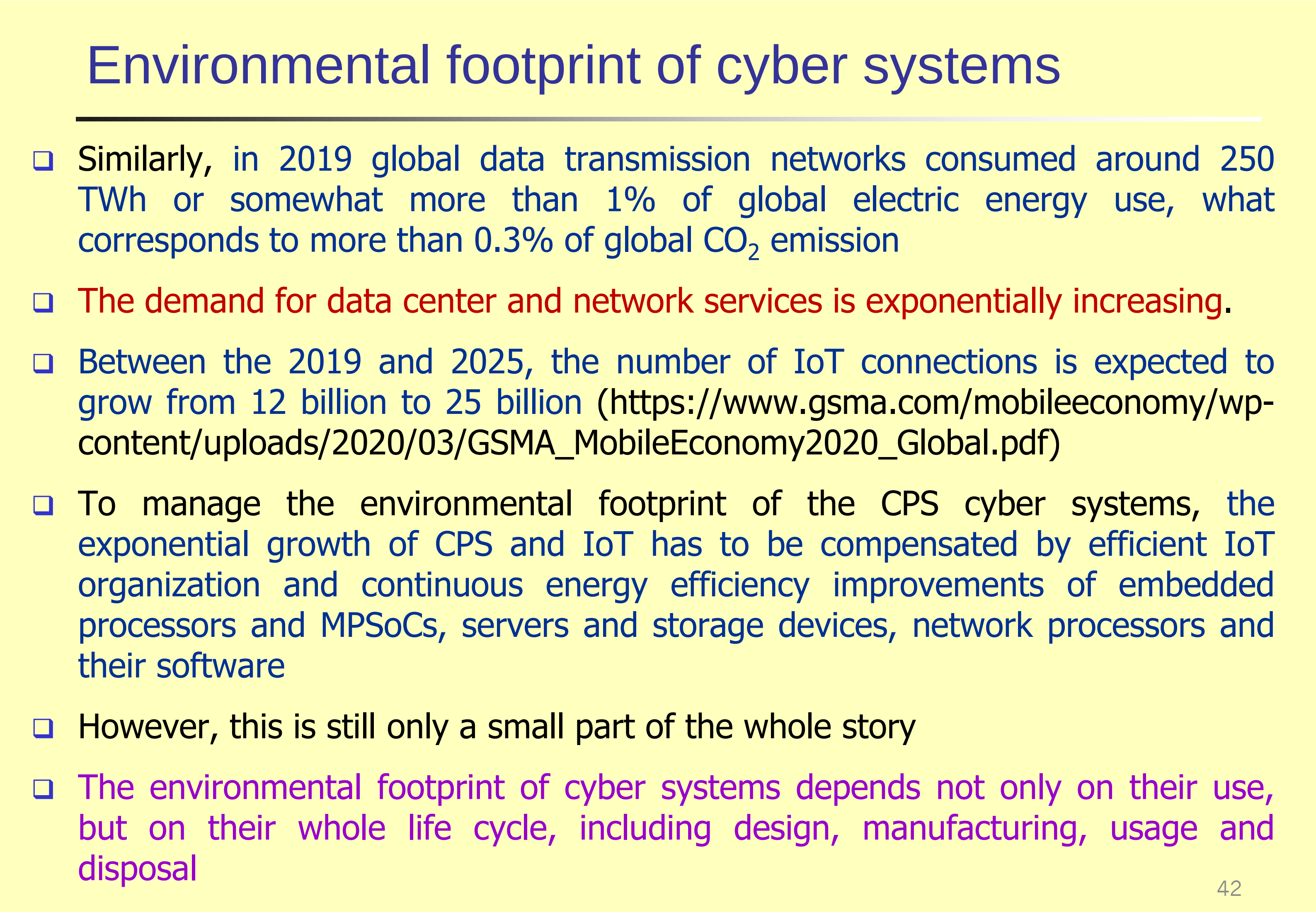
Source: https://energyinnovation.org/2020/03/17/

Figure 2. Estimated global data electricity use by data center type, 2010 and 2018. Source: Masanet et al. 2020.

- ❑ In 2018 global data centers consumed approximately 205TWh, what is more than the electric energy consumption of a medium country
- ❑ It represents 1% of global electric energy use and 0.3% of global CO_2 emission

41

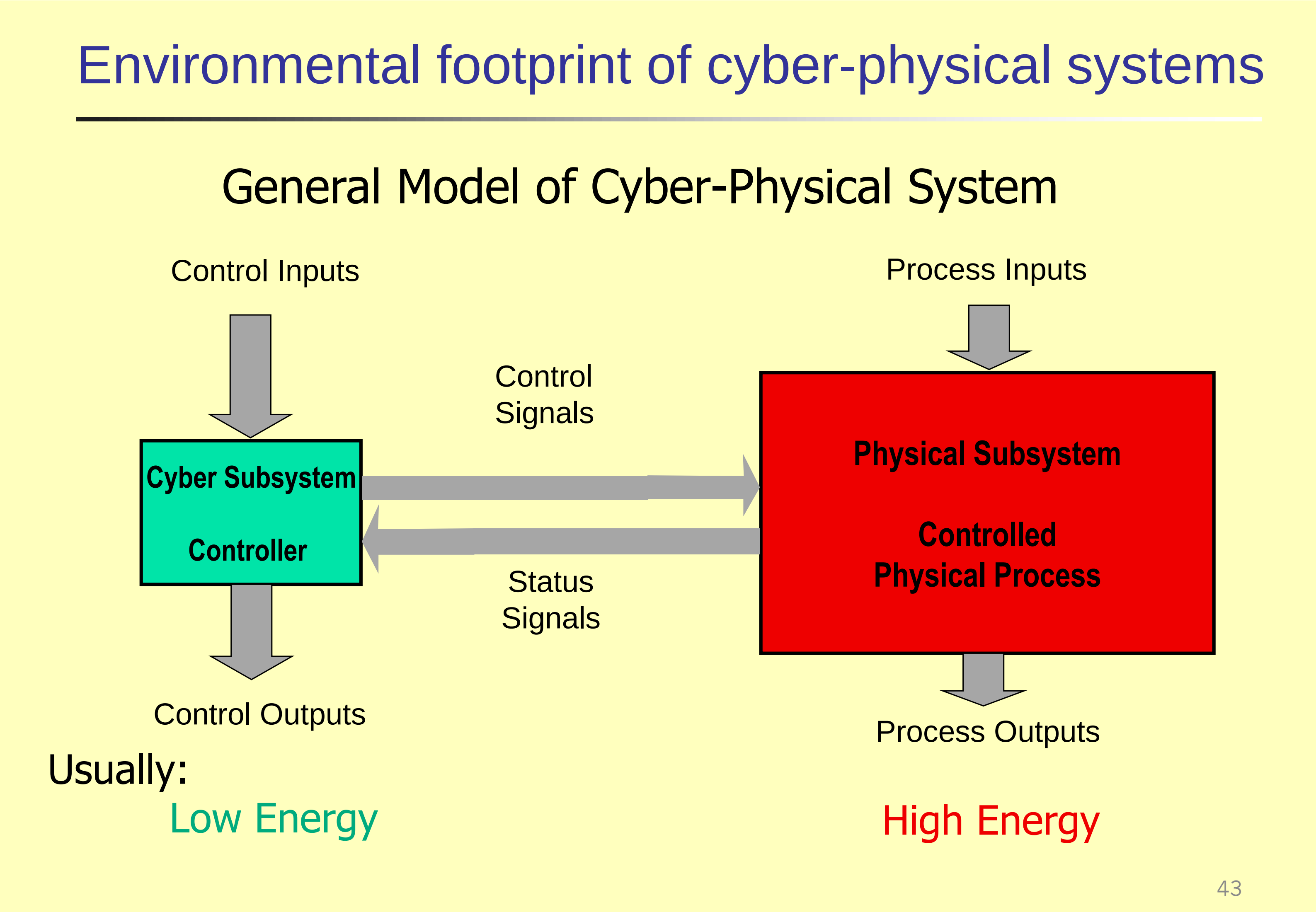
©MECO.net



Environmental footprint of cyber systems

- Similarly, in 2019 global data transmission networks consumed around 250 TWh or somewhat more than 1% of global electric energy use, what corresponds to more than 0.3% of global CO_2 emission
- The demand for data center and network services is exponentially increasing.
- Between the 2019 and 2025, the number of IoT connections is expected to grow from 12 billion to 25 billion (https://www.gsma.com/mobileeconomy/wp-content/uploads/2020/03/GSMA_MobileEconomy2020_Global.pdf)
- To manage the environmental footprint of the CPS cyber systems, the exponential growth of CPS and IoT has to be compensated by efficient IoT organization and continuous energy efficiency improvements of embedded processors and MPSoCs, servers and storage devices, network processors and their software
- However, this is still only a small part of the whole story
- The environmental footprint of cyber systems depends not only on their use, but on their whole life cycle, including design, manufacturing, usage and disposal

42



Environmental footprint of cyber-physical systems

General Model of Cyber-Physical System

Control Inputs

Process Inputs

Cyber Subsystem

Controller

Control Signals

Status Signals

Physical Subsystem

Controlled Physical Process

Control Outputs

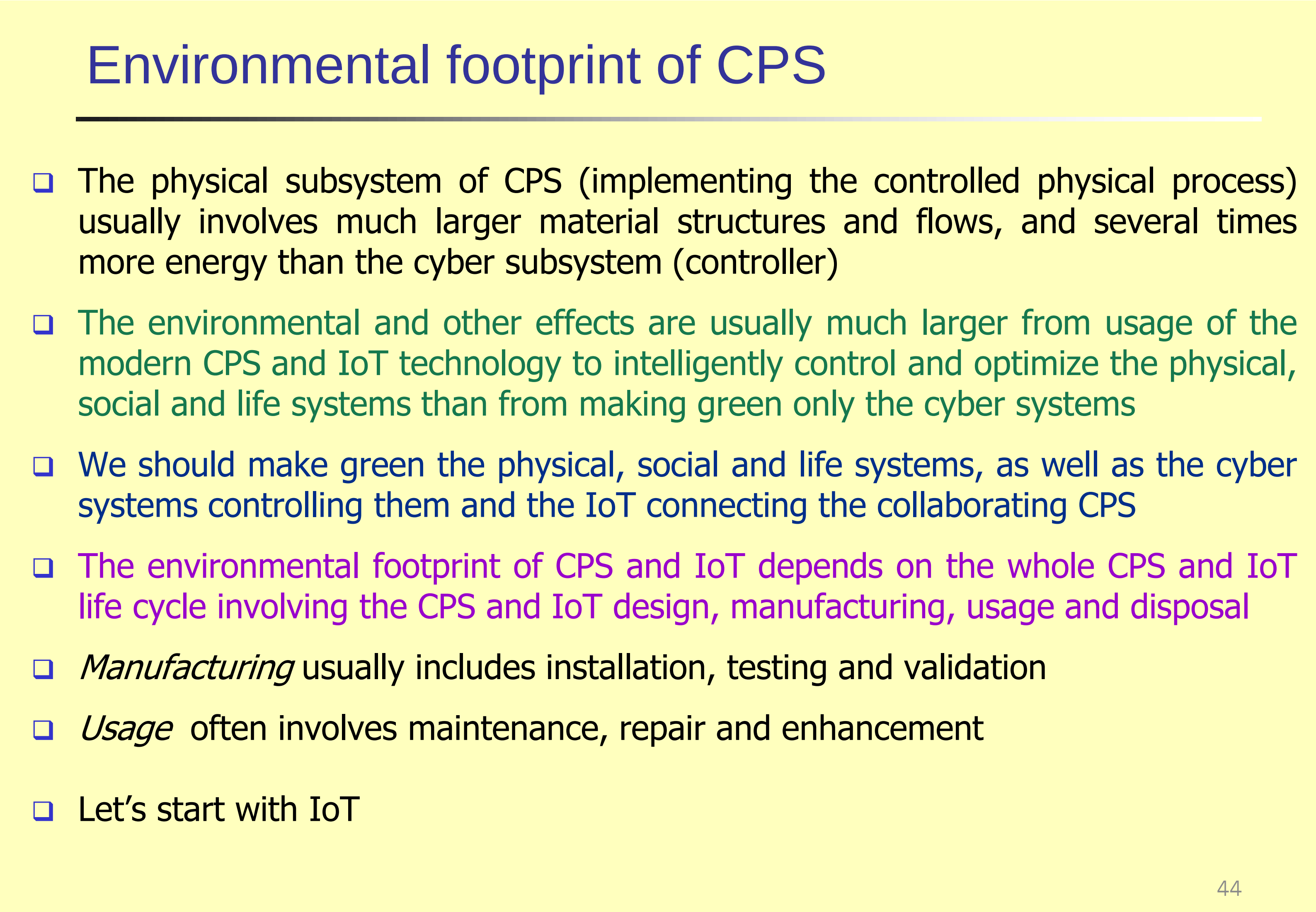
Process Outputs

Usually:

Low Energy

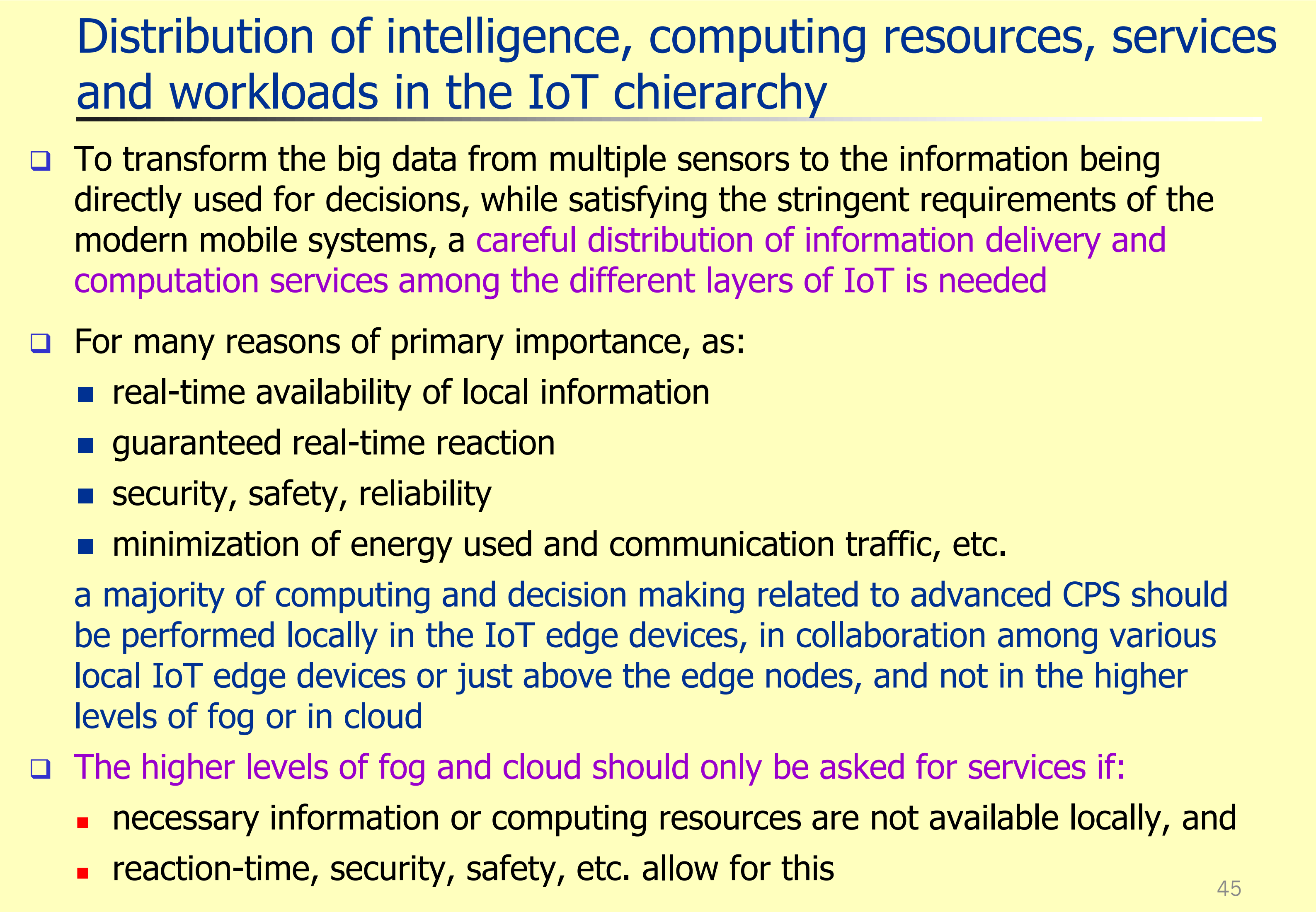
High Energy

43



Environmental footprint of CPS

- The physical subsystem of CPS (implementing the controlled physical process) usually involves much larger material structures and flows, and several times more energy than the cyber subsystem (controller)
- The environmental and other effects are usually much larger from usage of the modern CPS and IoT technology to intelligently control and optimize the physical, social and life systems than from making green only the cyber systems
- We should make green the physical, social and life systems, as well as the cyber systems controlling them and the IoT connecting the collaborating CPS
- The environmental footprint of CPS and IoT depends on the whole CPS and IoT life cycle involving the CPS and IoT design, manufacturing, usage and disposal
- *Manufacturing* usually includes installation, testing and validation
- *Usage* often involves maintenance, repair and enhancement
- Let's start with IoT

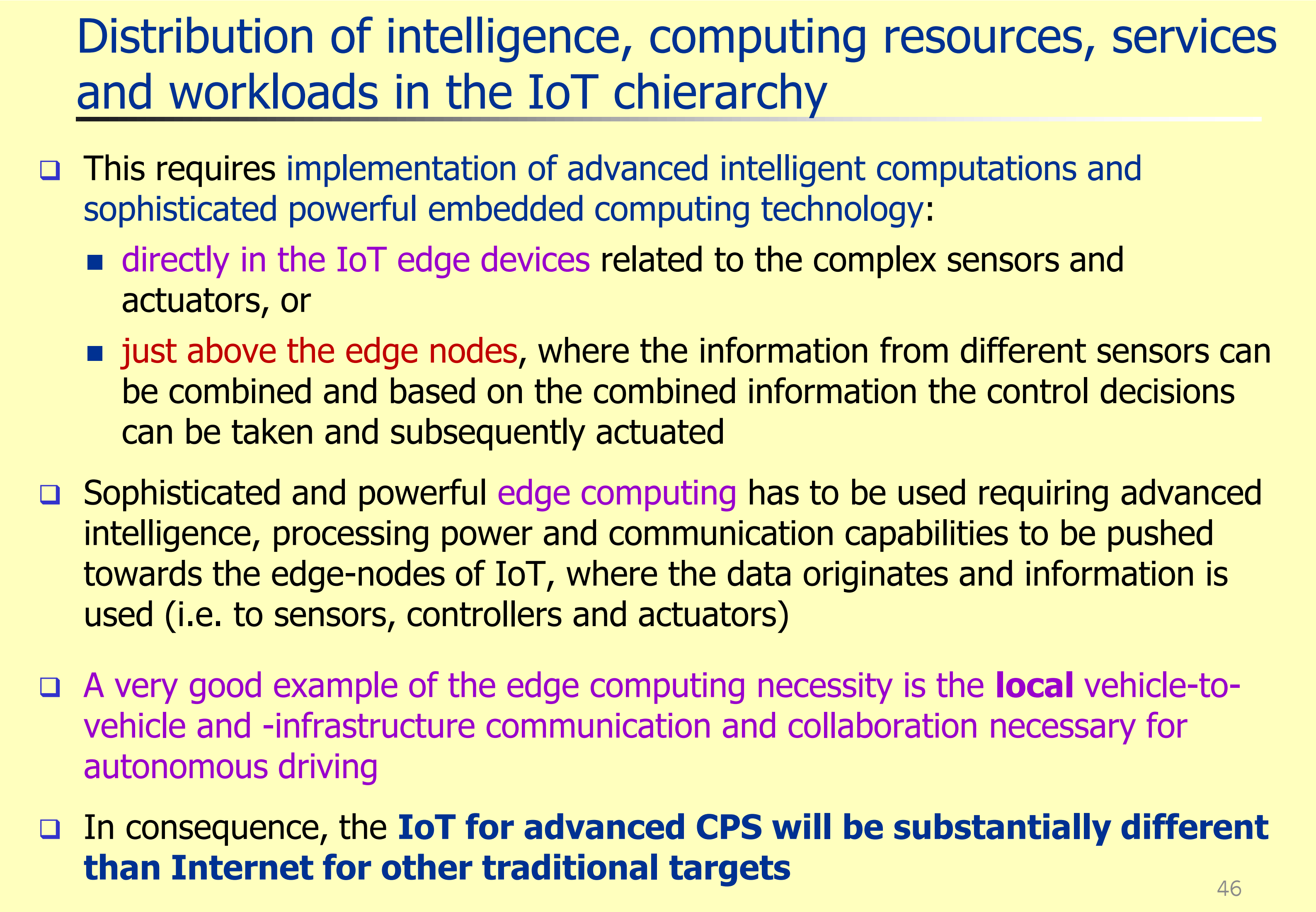


Distribution of intelligence, computing resources, services and workloads in the IoT chierarchy

- To transform the big data from multiple sensors to the information being directly used for decisions, while satisfying the stringent requirements of the modern mobile systems, a careful distribution of information delivery and computation services among the different layers of IoT is needed
- For many reasons of primary importance, as:
  - real-time availability of local information
  - guaranteed real-time reaction
  - security, safety, reliability
  - minimization of energy used and communication traffic, etc.

  a majority of computing and decision making related to advanced CPS should be performed locally in the IoT edge devices, in collaboration among various local IoT edge devices or just above the edge nodes, and not in the higher levels of fog or in cloud
- The higher levels of fog and cloud should only be asked for services if:
  - necessary information or computing resources are not available locally, and
  - reaction-time, security, safety, etc. allow for this

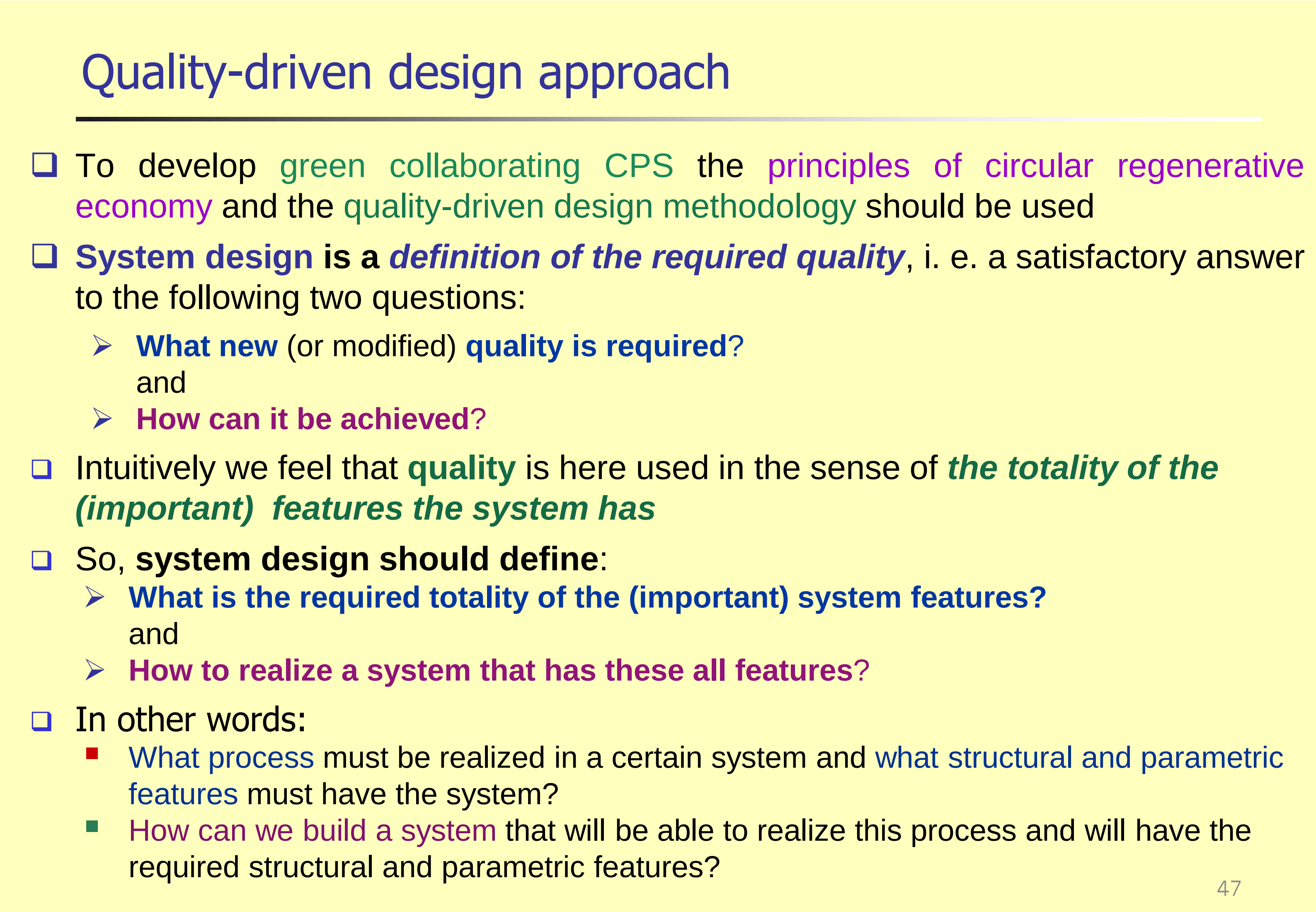
45



Distribution of intelligence, computing resources, services and workloads in the IoT chierarchy

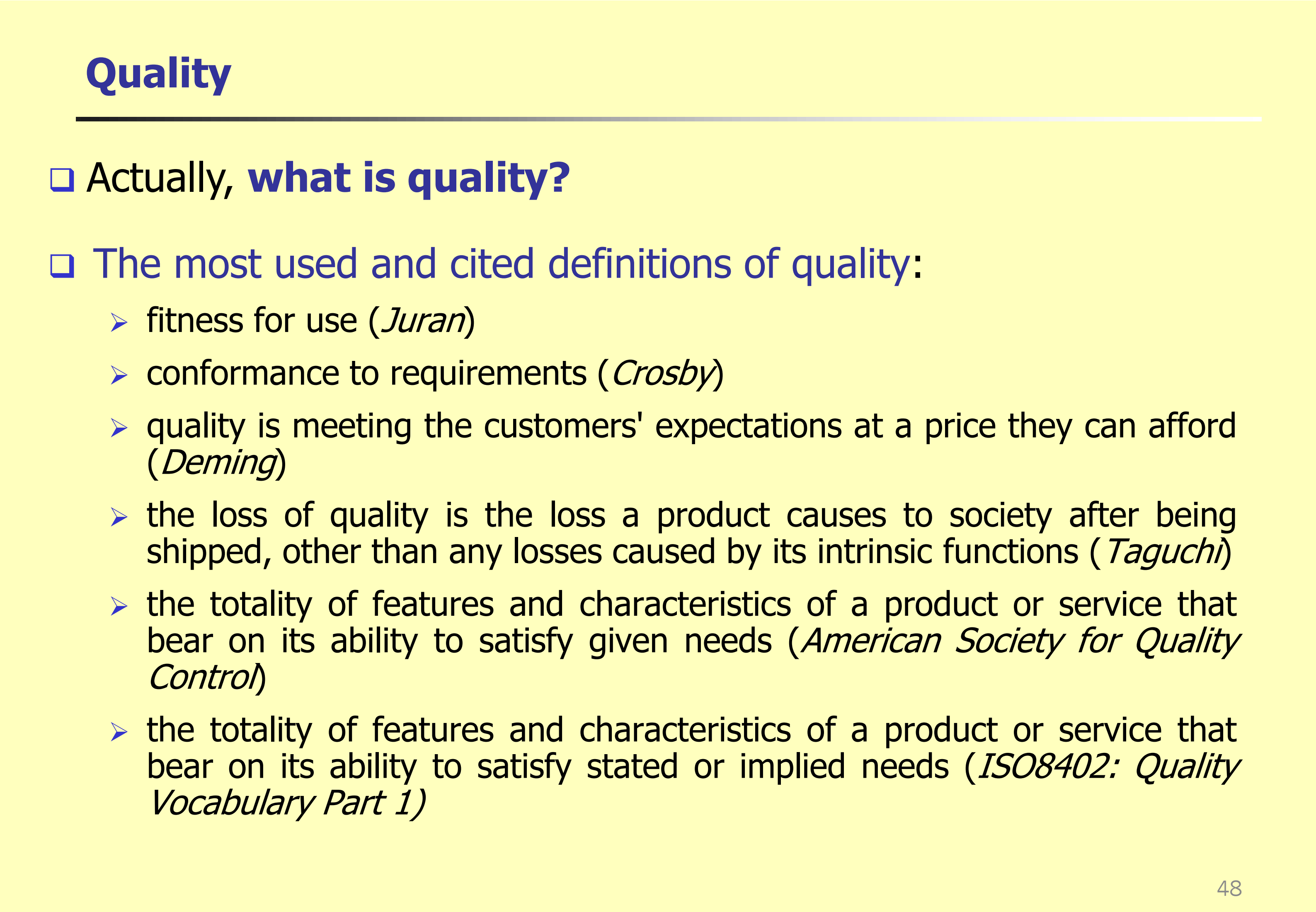
- This requires implementation of advanced intelligent computations and sophisticated powerful embedded computing technology:
  - directly in the IoT edge devices related to the complex sensors and actuators, or
  - just above the edge nodes, where the information from different sensors can be combined and based on the combined information the control decisions can be taken and subsequently actuated
- Sophisticated and powerful edge computing has to be used requiring advanced intelligence, processing power and communication capabilities to be pushed towards the edge-nodes of IoT, where the data originates and information is used (i.e. to sensors, controllers and actuators)
- A very good example of the edge computing necessity is the **local** vehicle-to-vehicle and -infrastructure communication and collaboration necessary for autonomous driving
- In consequence, the **IoT for advanced CPS will be substantially different than Internet for other traditional targets**

46



Quality-driven design approach

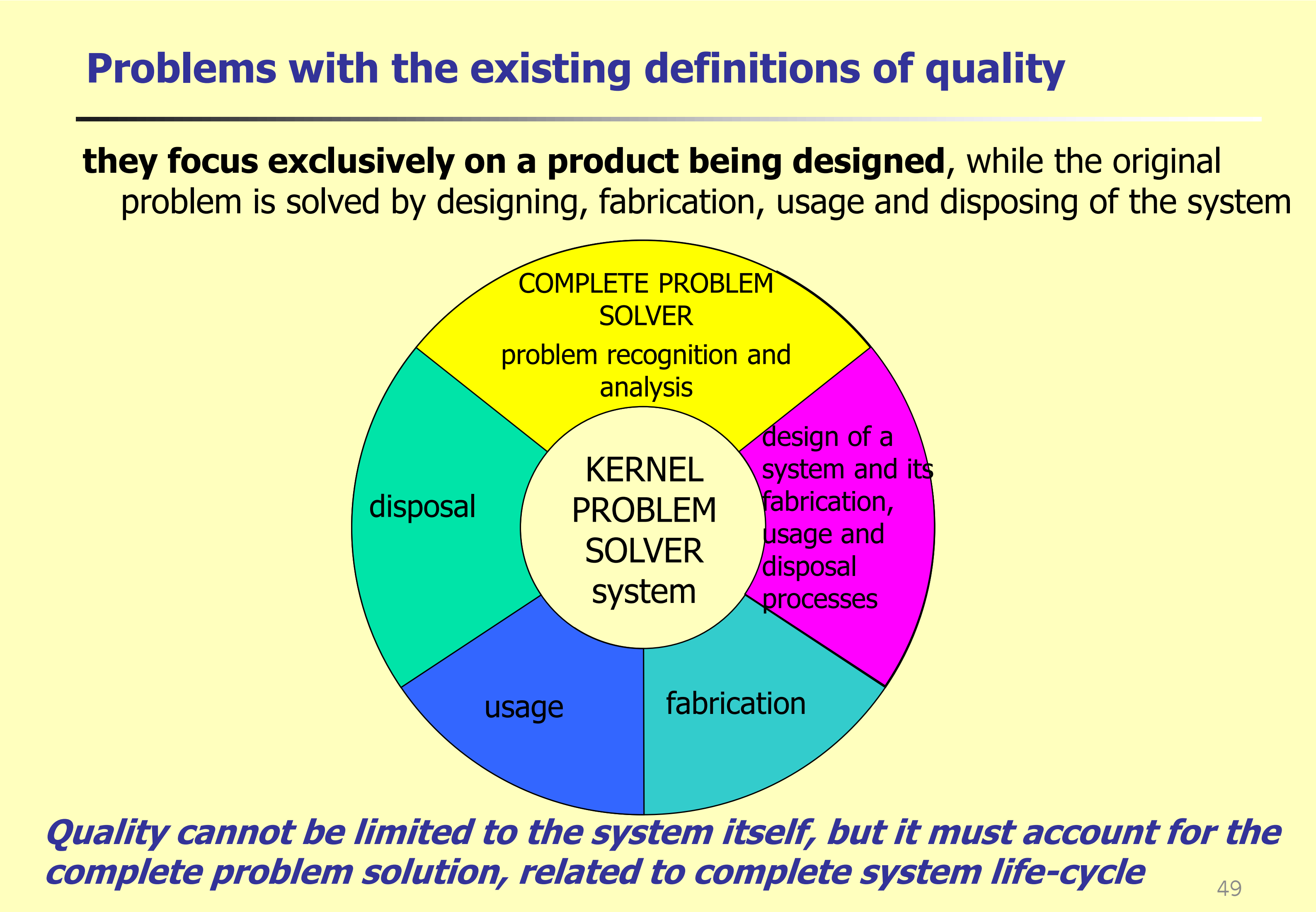
- To develop green collaborating CPS the principles of circular regenerative economy and the quality-driven design methodology should be used
- **System design is a *definition of the required quality***, i. e. a satisfactory answer to the following two questions:
  - **What new** (or modified) **quality is required**?
    and
  - **How can it be achieved**?
- Intuitively we feel that **quality** is here used in the sense of ***the totality of the (important) features the system has***
- So, **system design should define**:
  - **What is the required totality of the (important) system features?**
    and
  - **How to realize a system that has these all features**?
- In other words:
  - What process must be realized in a certain system and what structural and parametric features must have the system?
  - How can we build a system that will be able to realize this process and will have the required structural and parametric features?



Quality

- ❑ Actually, **what is quality?**
- ❑ The most used and cited definitions of quality:
  - fitness for use (*Juran*)
  - conformance to requirements (*Crosby*)
  - quality is meeting the customers' expectations at a price they can afford (*Deming*)
  - the loss of quality is the loss a product causes to society after being shipped, other than any losses caused by its intrinsic functions (*Taguchi*)
  - the totality of features and characteristics of a product or service that bear on its ability to satisfy given needs (*American Society for Quality Control*)
  - the totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs (*ISO8402: Quality Vocabulary Part 1)*

48



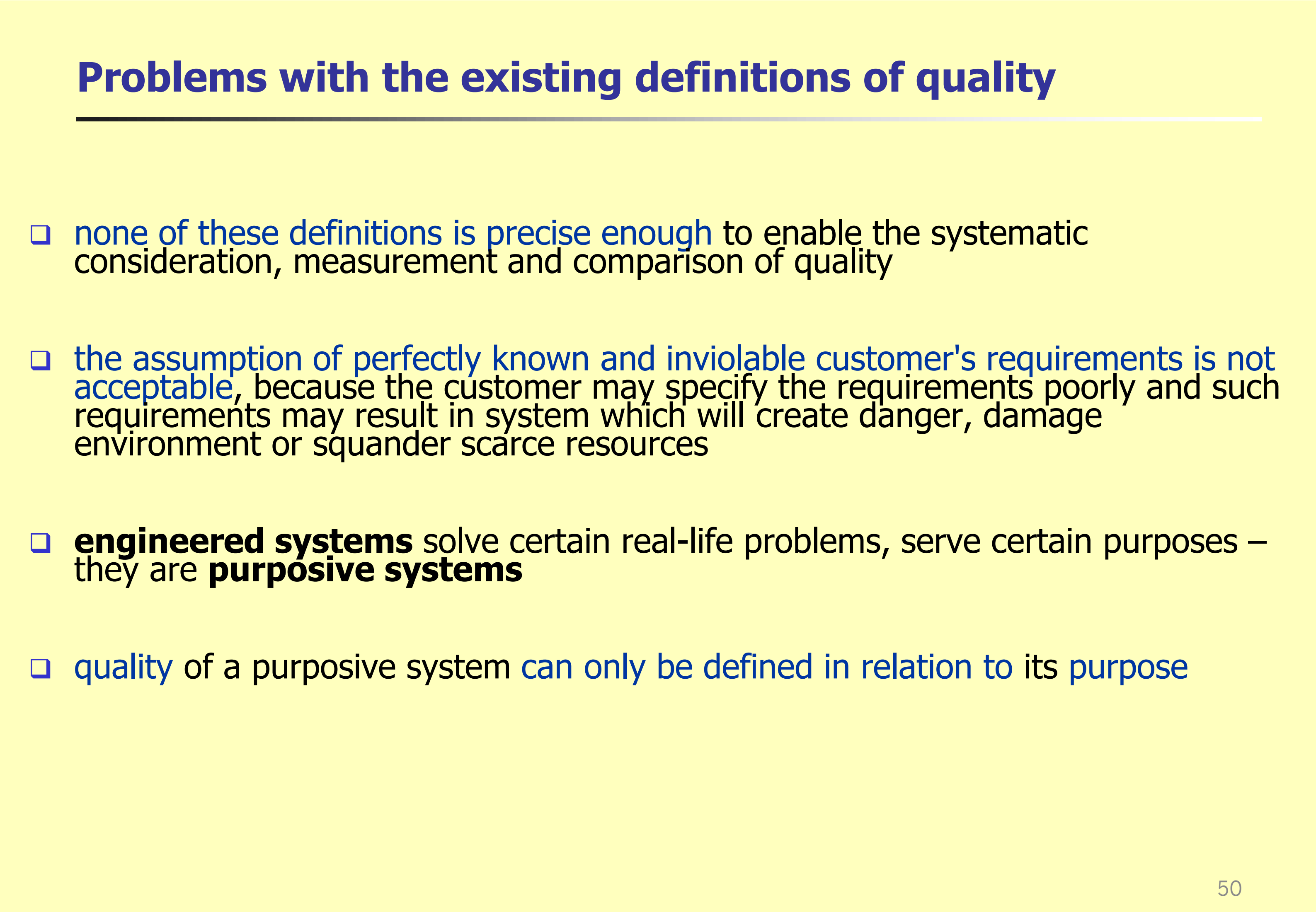
Problems with the existing definitions of quality

they focus exclusively on a product being designed, while the original problem is solved by designing, fabrication, usage and disposing of the system

COMPLETE PROBLEM SOLVER
problem recognition and analysis
design of a system and its fabrication, usage and disposal processes
fabrication
usage
disposal
KERNEL PROBLEM SOLVER system

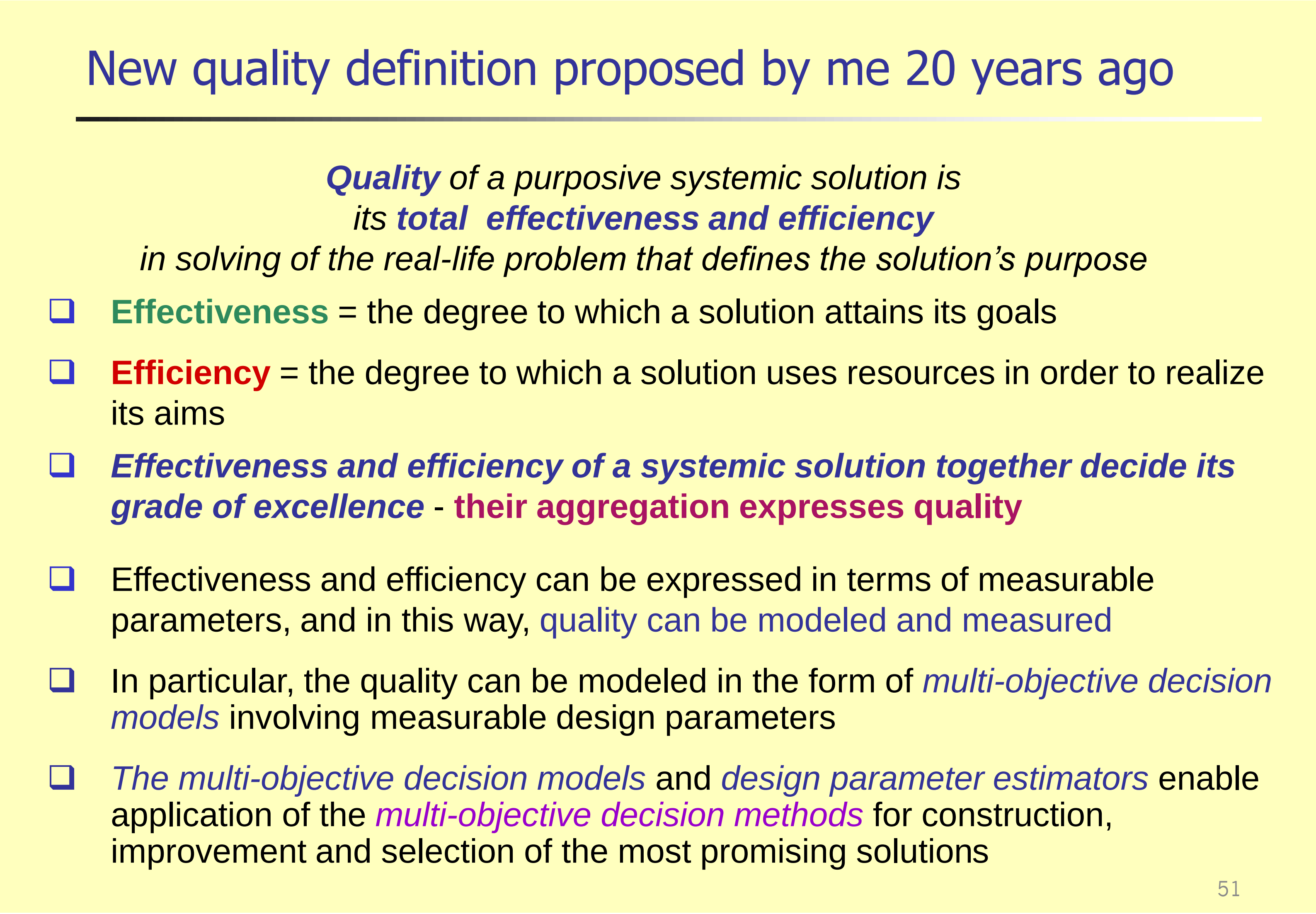
Quality cannot be limited to the system itself, but it must account for the complete problem solution, related to complete system life-cycle

49



Problems with the existing definitions of quality

- none of these definitions is precise enough to enable the systematic consideration, measurement and comparison of quality
- the assumption of perfectly known and inviolable customer's requirements is not acceptable, because the customer may specify the requirements poorly and such requirements may result in system which will create danger, damage environment or squander scarce resources
- **engineered systems** solve certain real-life problems, serve certain purposes – they are **purposive systems**
- quality of a purposive system can only be defined in relation to its purpose

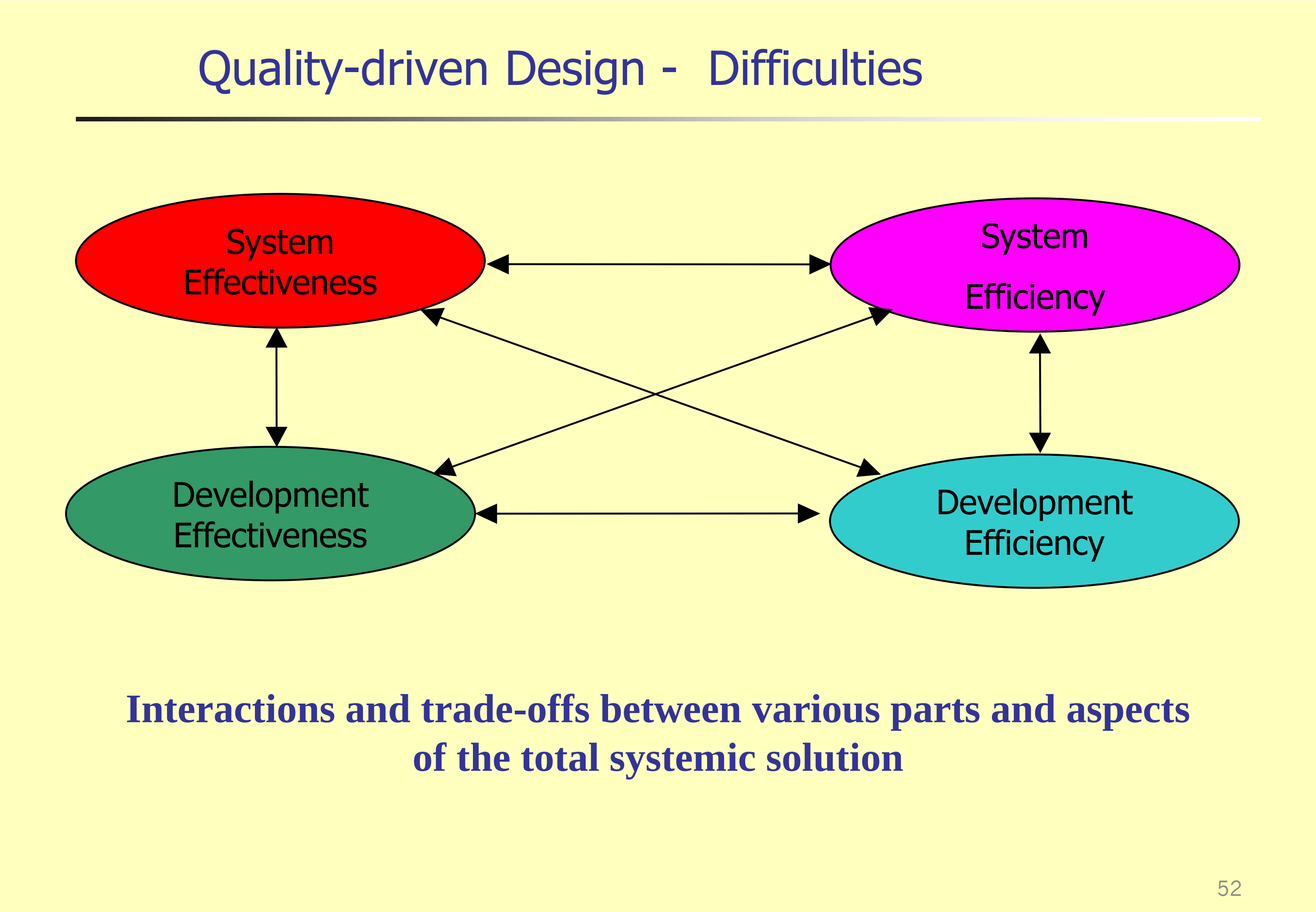


New quality definition proposed by me 20 years ago

***Quality** of a purposive systemic solution is*
*its **total effectiveness and efficiency***
in solving of the real-life problem that defines the solution's purpose

- ❑ **Effectiveness** = the degree to which a solution attains its goals
- ❑ **Efficiency** = the degree to which a solution uses resources in order to realize its aims
- ❑ ***Effectiveness and efficiency of a systemic solution together decide its grade of excellence*** - **their aggregation expresses quality**
- ❑ Effectiveness and efficiency can be expressed in terms of measurable parameters, and in this way, quality can be modeled and measured
- ❑ In particular, the quality can be modeled in the form of *multi-objective decision models* involving measurable design parameters
- ❑ *The multi-objective decision models* and *design parameter estimators* enable application of the *multi-objective decision methods* for construction, improvement and selection of the most promising solutions

51



Quality-driven Design - Difficulties

System Effectiveness

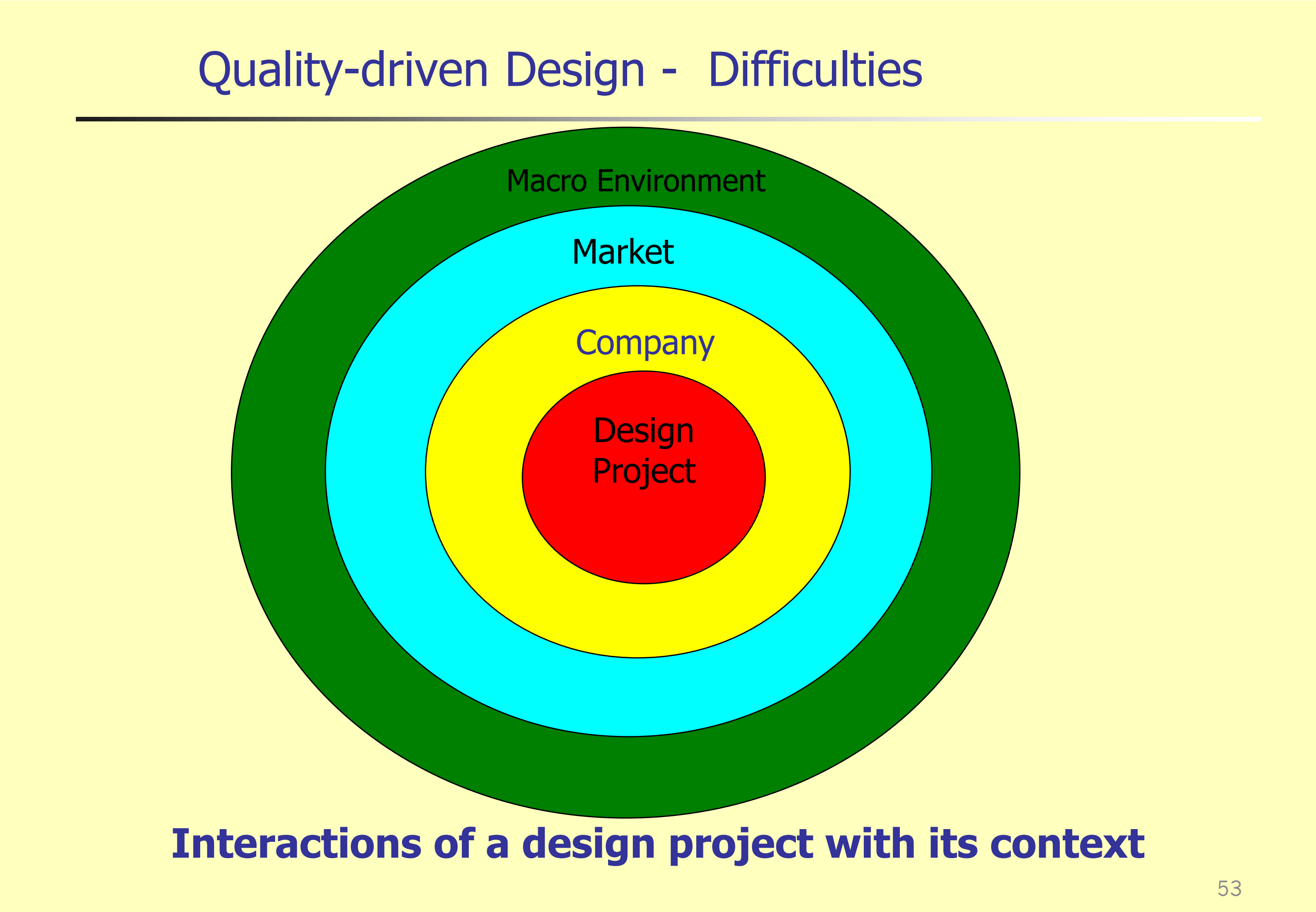
System Efficiency

Development Effectiveness

Development Efficiency

Interactions and trade-offs between various parts and aspects of the total systemic solution

52



Quality-driven Design - Difficulties

Macro Environment

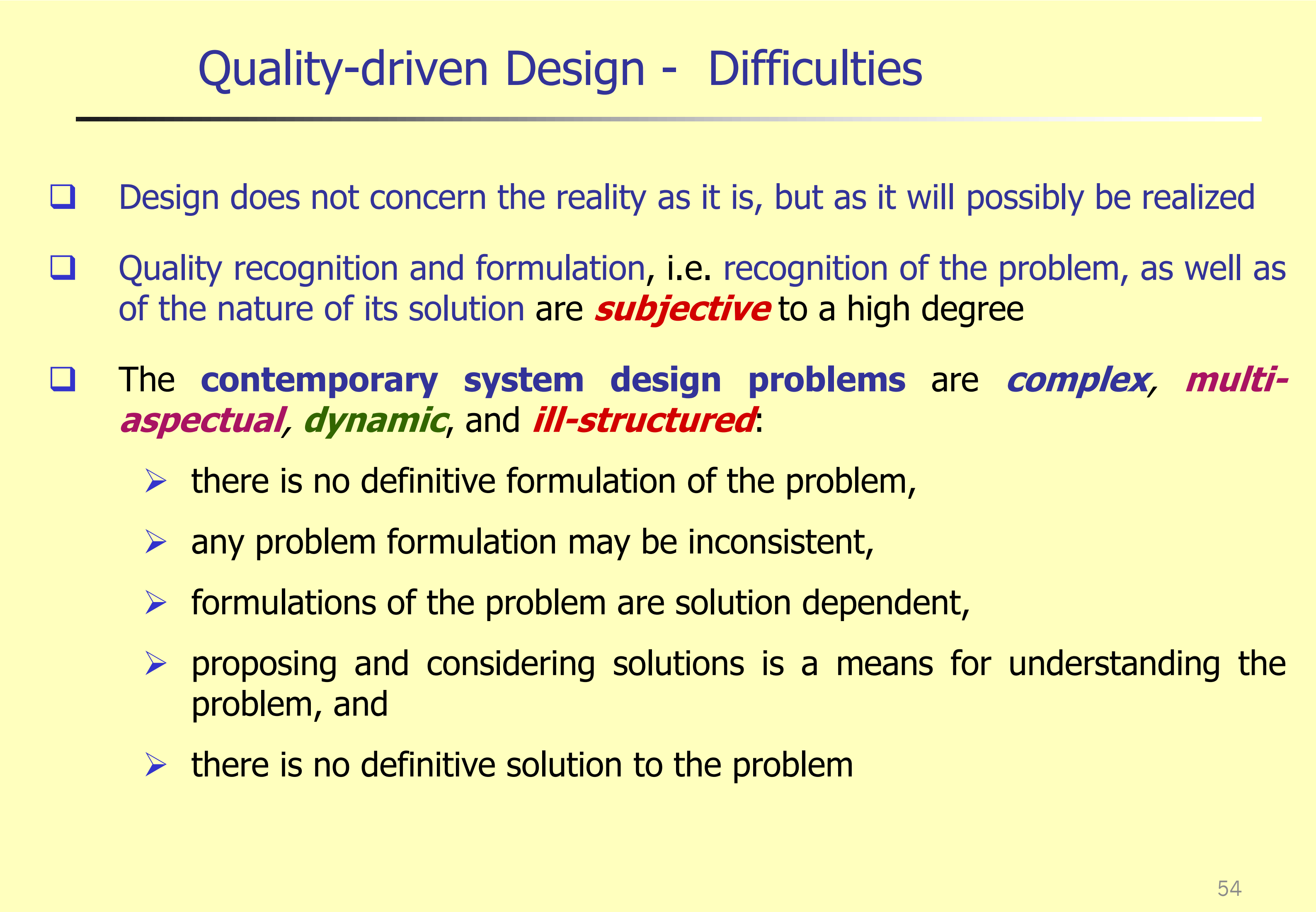
Market

Company

Design Project

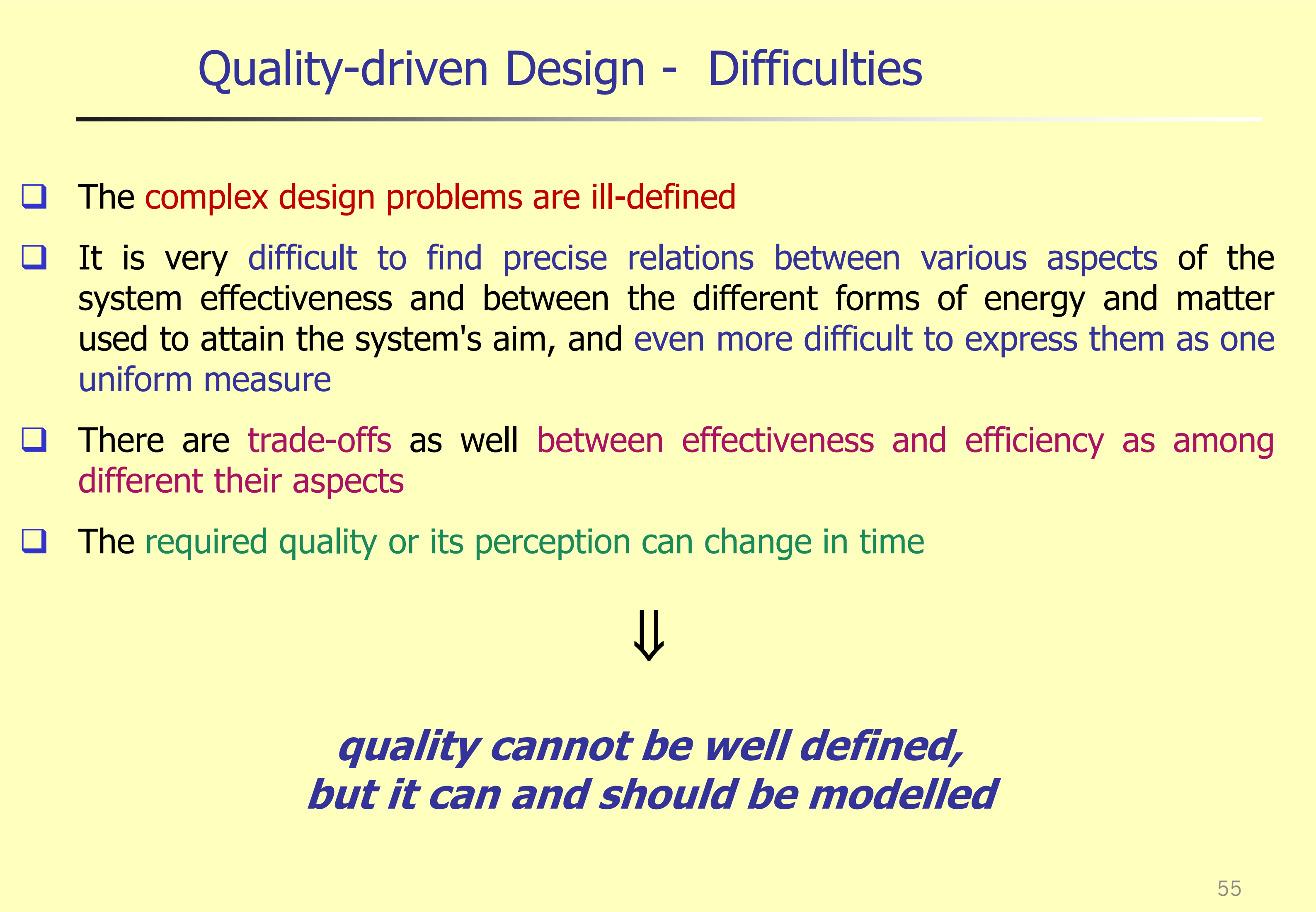
Interactions of a design project with its context

53



Quality-driven Design - Difficulties

- ❑ Design does not concern the reality as it is, but as it will possibly be realized
- ❑ Quality recognition and formulation, i.e. recognition of the problem, as well as of the nature of its solution are ***subjective*** to a high degree
- ❑ The **contemporary system design problems** are ***complex***, ***multi-aspectual***, ***dynamic***, and ***ill-structured***:
  - ➢ there is no definitive formulation of the problem,
  - ➢ any problem formulation may be inconsistent,
  - ➢ formulations of the problem are solution dependent,
  - ➢ proposing and considering solutions is a means for understanding the problem, and
  - ➢ there is no definitive solution to the problem

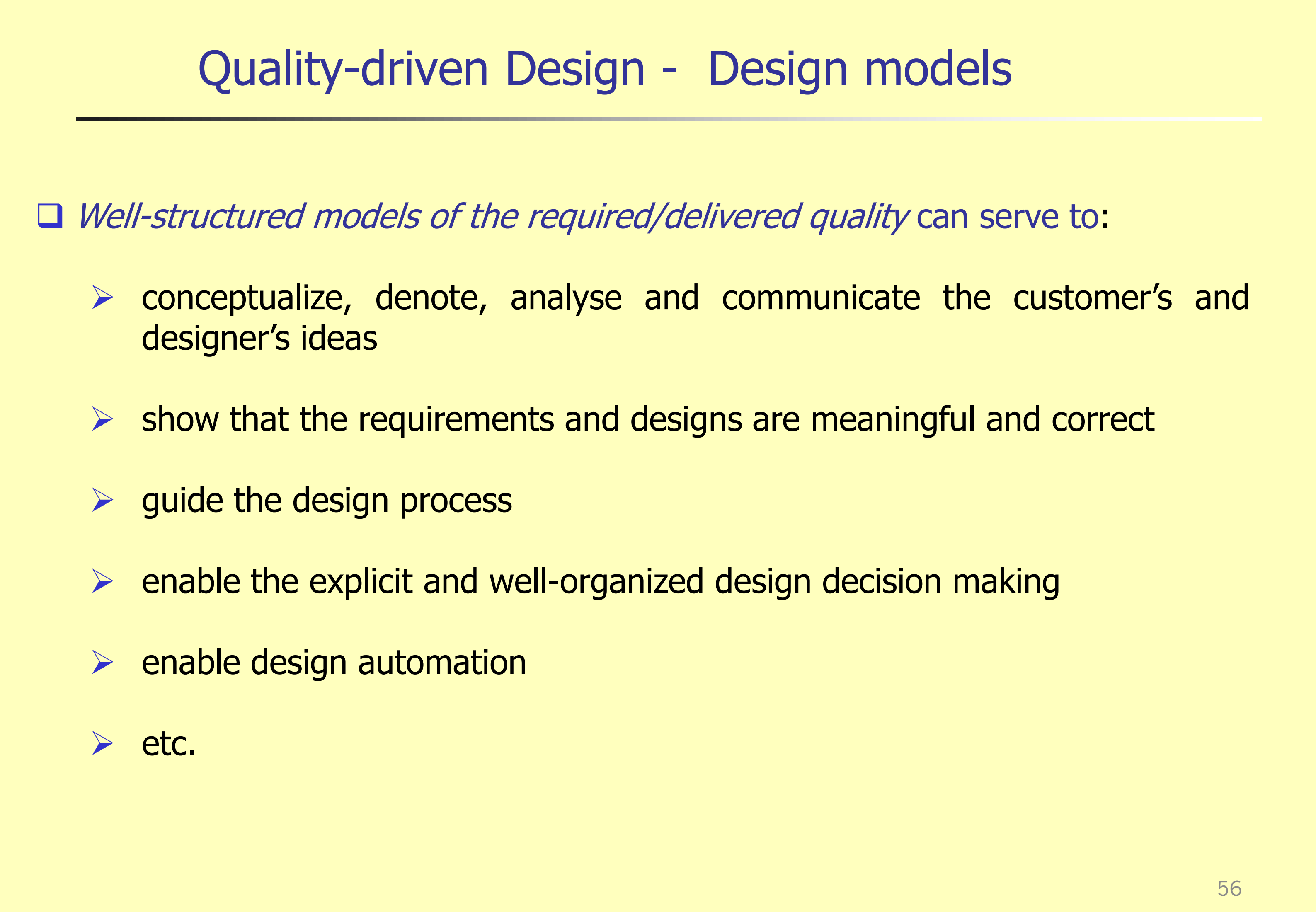


Quality-driven Design - Difficulties

- The complex design problems are ill-defined
- It is very difficult to find precise relations between various aspects of the system effectiveness and between the different forms of energy and matter used to attain the system's aim, and even more difficult to express them as one uniform measure
- There are trade-offs as well between effectiveness and efficiency as among different their aspects
- The required quality or its perception can change in time

⇓

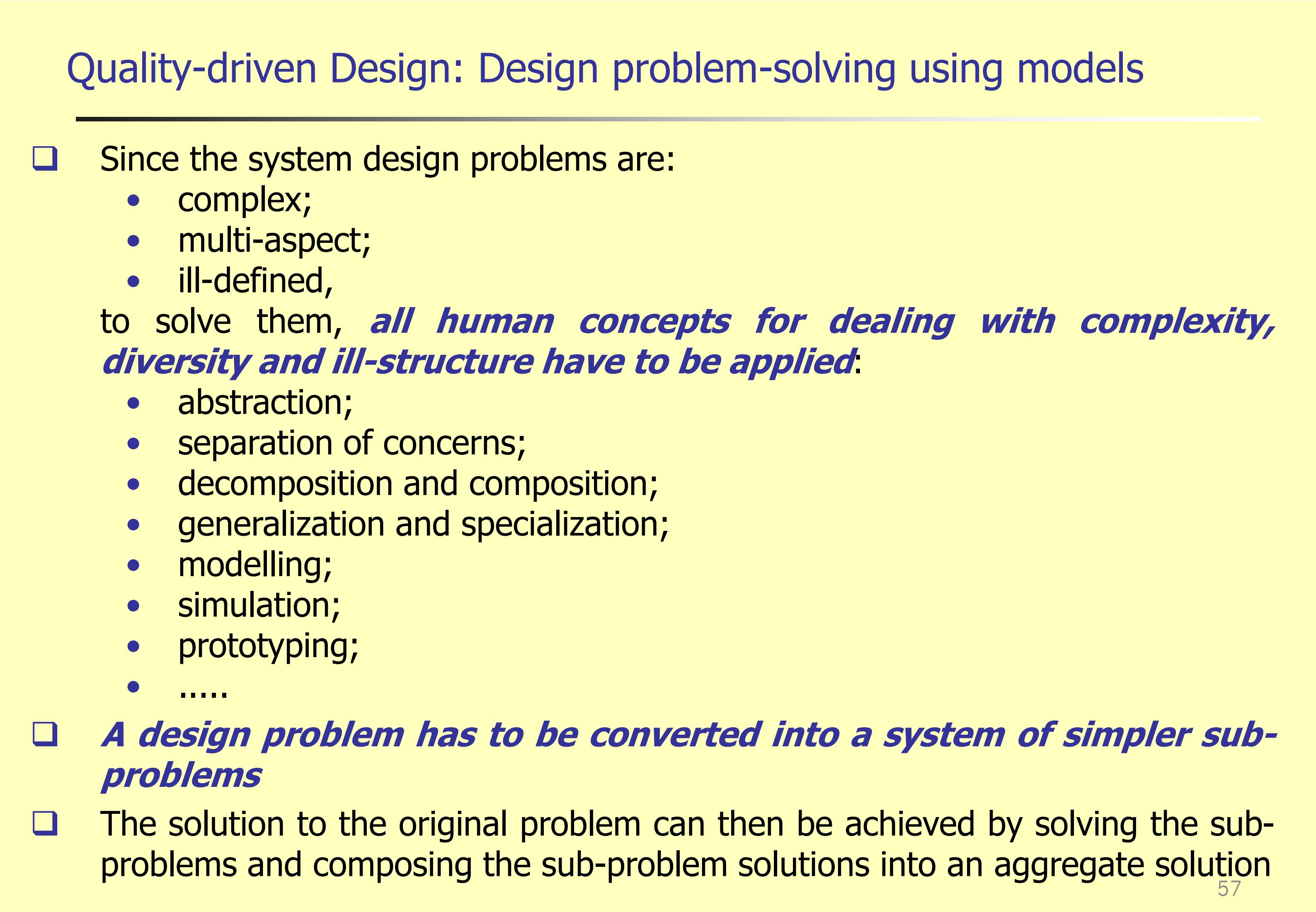
quality cannot be well defined,
but it can and should be modelled



Quality-driven Design - Design models

- *Well-structured models of the required/delivered quality* can serve to:
  - conceptualize, denote, analyse and communicate the customer's and designer's ideas
  - show that the requirements and designs are meaningful and correct
  - guide the design process
  - enable the explicit and well-organized design decision making
  - enable design automation
  - etc.

56



Quality-driven Design: Design problem-solving using models

❑ Since the system design problems are:

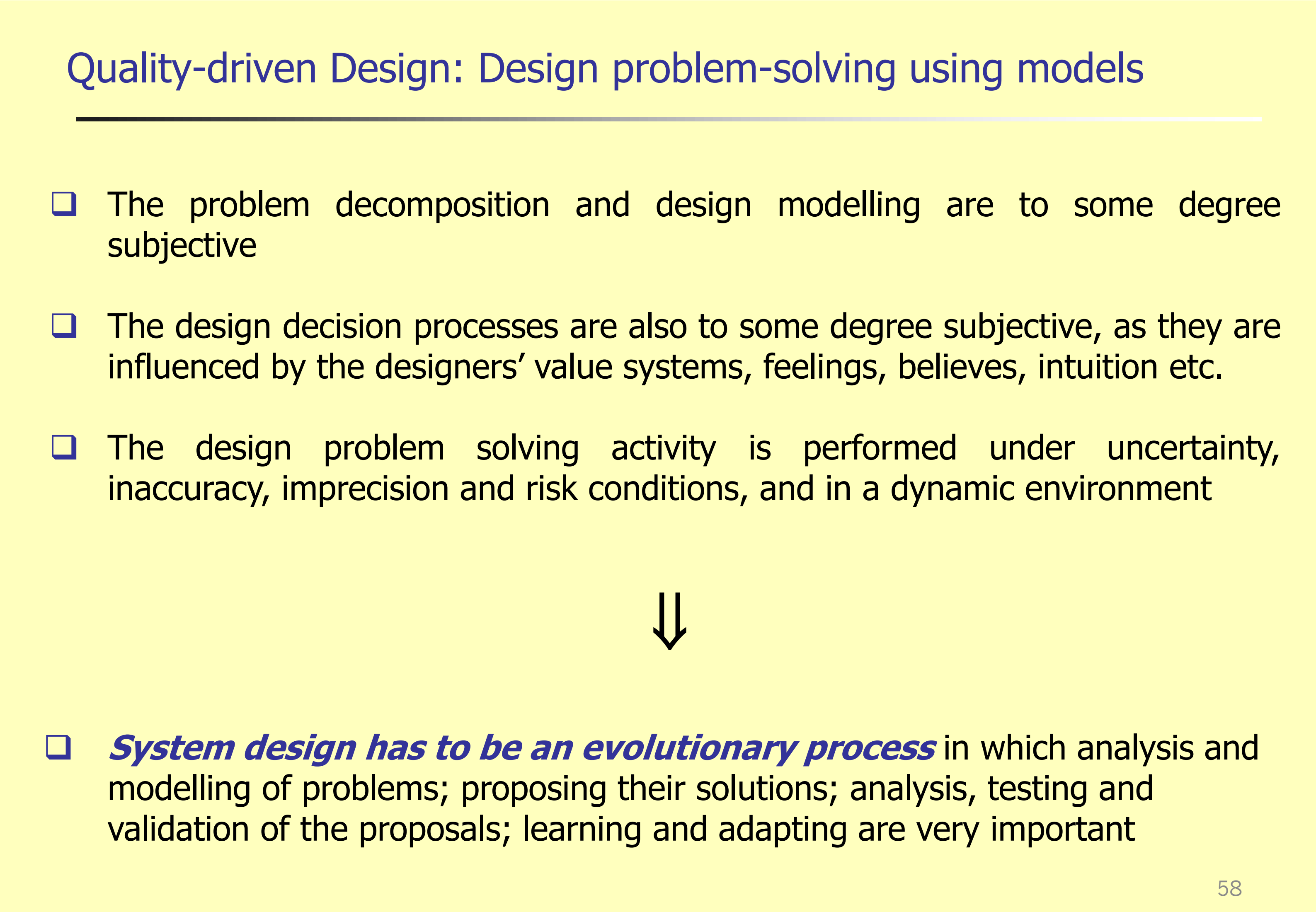
- complex;
- multi-aspect;
- ill-defined,

to solve them, ***all human concepts for dealing with complexity, diversity and ill-structure have to be applied***:

- abstraction;
- separation of concerns;
- decomposition and composition;
- generalization and specialization;
- modelling;
- simulation;
- prototyping;
- .....

❑ ***A design problem has to be converted into a system of simpler sub-problems***

❑ The solution to the original problem can then be achieved by solving the sub-problems and composing the sub-problem solutions into an aggregate solution



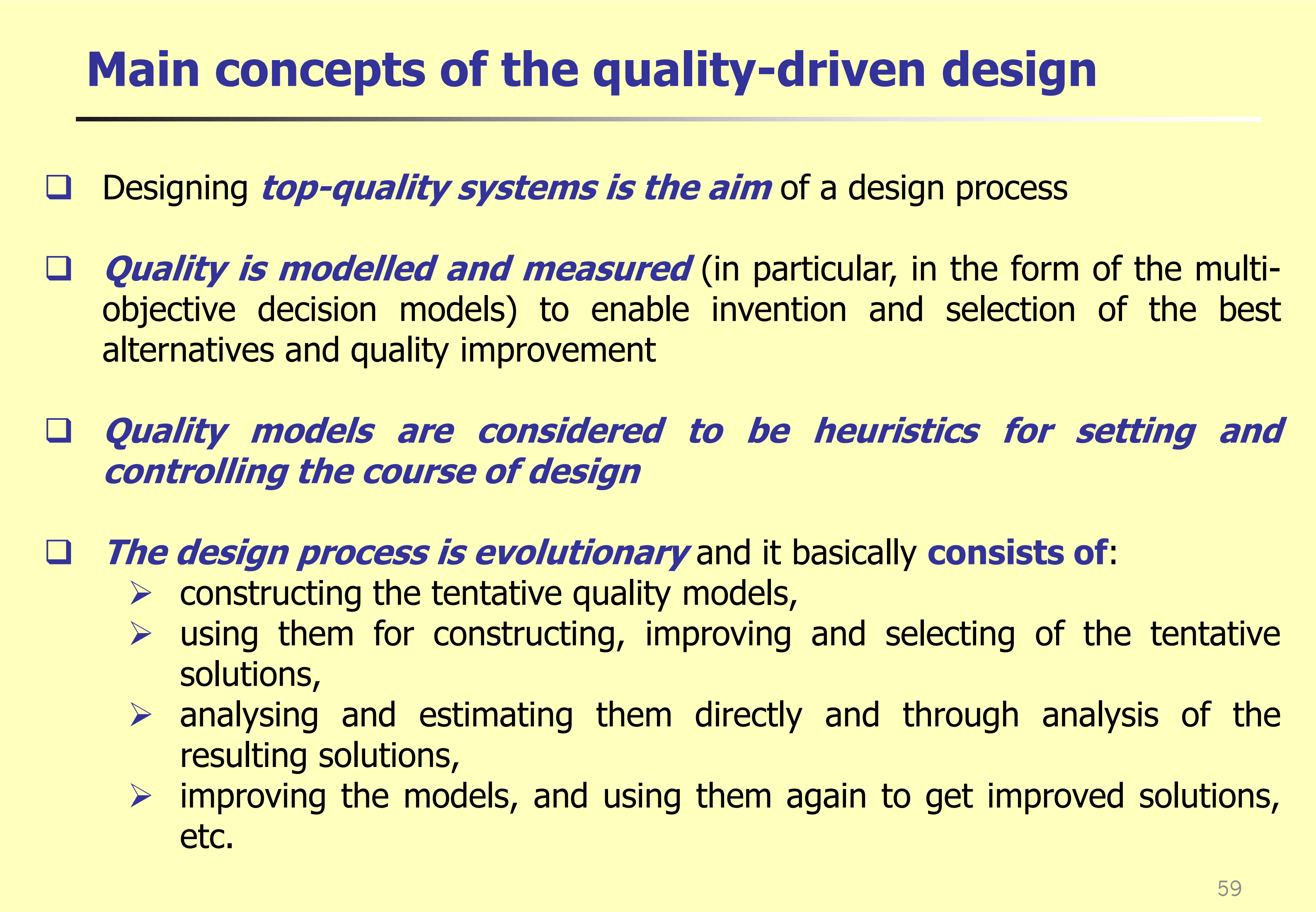
Quality-driven Design: Design problem-solving using models

- ❑ The problem decomposition and design modelling are to some degree subjective
- ❑ The design decision processes are also to some degree subjective, as they are influenced by the designers' value systems, feelings, believes, intuition etc.
- ❑ The design problem solving activity is performed under uncertainty, inaccuracy, imprecision and risk conditions, and in a dynamic environment

⇓

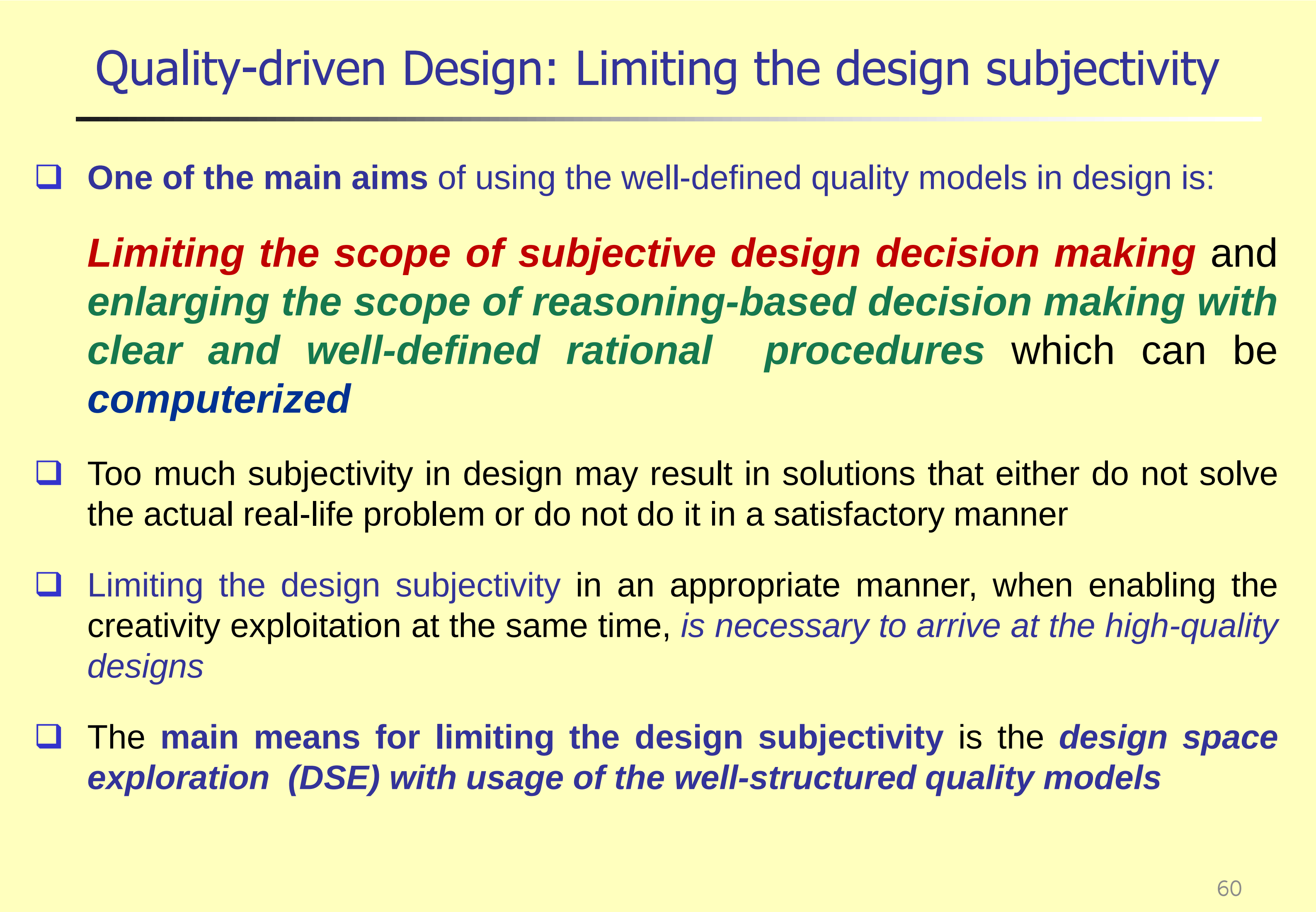
- ❑ ***System design has to be an evolutionary process*** in which analysis and modelling of problems; proposing their solutions; analysis, testing and validation of the proposals; learning and adapting are very important

58



Main concepts of the quality-driven design

- ❑ Designing ***top-quality systems is the aim*** of a design process
- ❑ ***Quality is modelled and measured*** (in particular, in the form of the multi-objective decision models) to enable invention and selection of the best alternatives and quality improvement
- ❑ ***Quality models are considered to be heuristics for setting and controlling the course of design***
- ❑ ***The design process is evolutionary*** and it basically **consists of**:
  - ➢ constructing the tentative quality models,
  - ➢ using them for constructing, improving and selecting of the tentative solutions,
  - ➢ analysing and estimating them directly and through analysis of the resulting solutions,
  - ➢ improving the models, and using them again to get improved solutions, etc.



Quality-driven Design: Limiting the design subjectivity

- **One of the main aims** of using the well-defined quality models in design is:

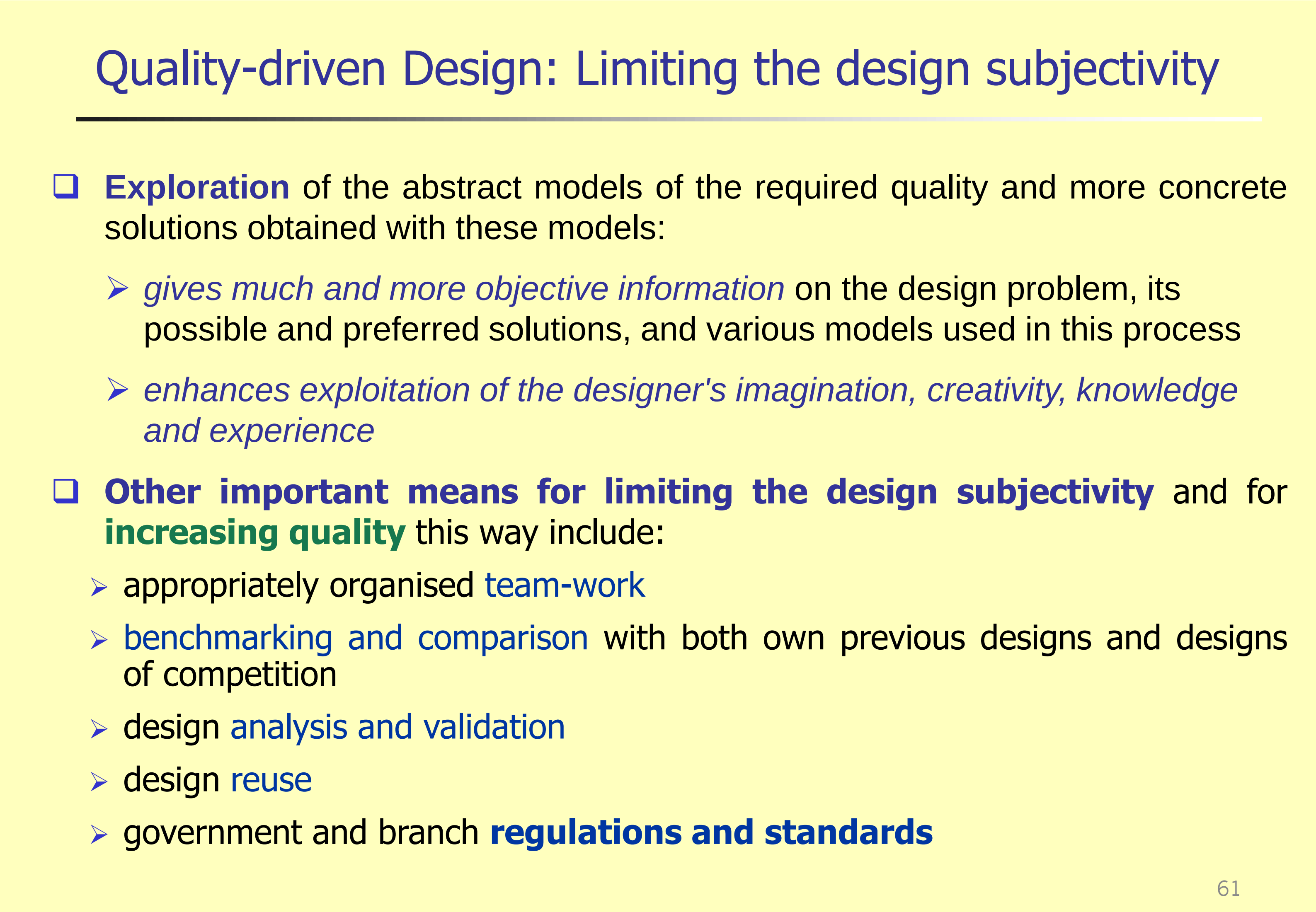
  Limiting the scope of subjective design decision making and ***enlarging the scope of reasoning-based decision making with clear and well-defined rational procedures*** which can be ***computerized***

- Too much subjectivity in design may result in solutions that either do not solve the actual real-life problem or do not do it in a satisfactory manner

- Limiting the design subjectivity in an appropriate manner, when enabling the creativity exploitation at the same time, *is necessary to arrive at the high-quality designs*

- The **main means for limiting the design subjectivity** is the ***design space exploration (DSE) with usage of the well-structured quality models***

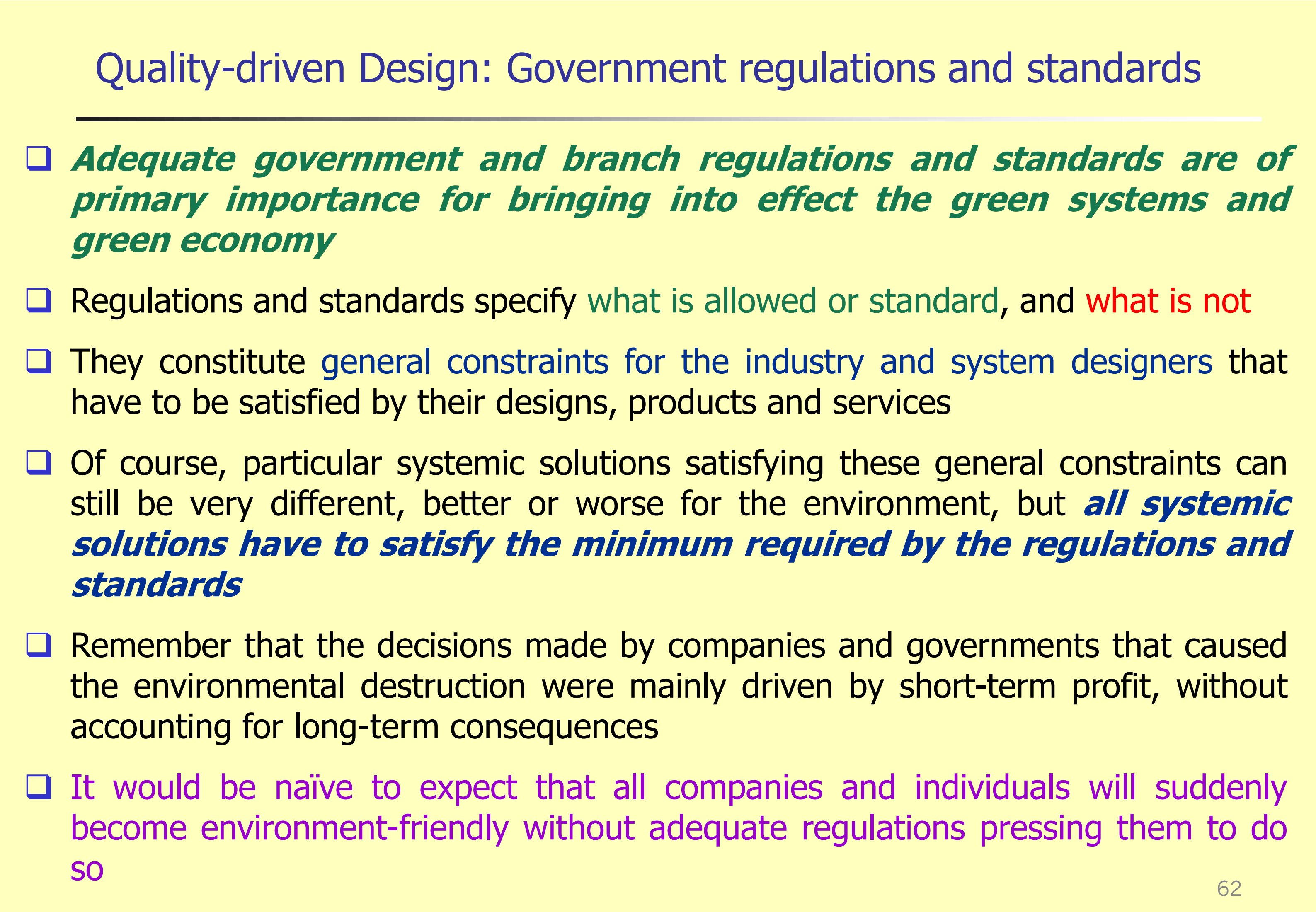
60



Quality-driven Design: Limiting the design subjectivity

- **Exploration** of the abstract models of the required quality and more concrete solutions obtained with these models:
  - *gives much and more objective information* on the design problem, its possible and preferred solutions, and various models used in this process
  - *enhances exploitation of the designer's imagination, creativity, knowledge and experience*
- **Other important means for limiting the design subjectivity** and for **increasing quality** this way include:
  - appropriately organised team-work
  - benchmarking and comparison with both own previous designs and designs of competition
  - design analysis and validation
  - design reuse
  - government and branch **regulations and standards**

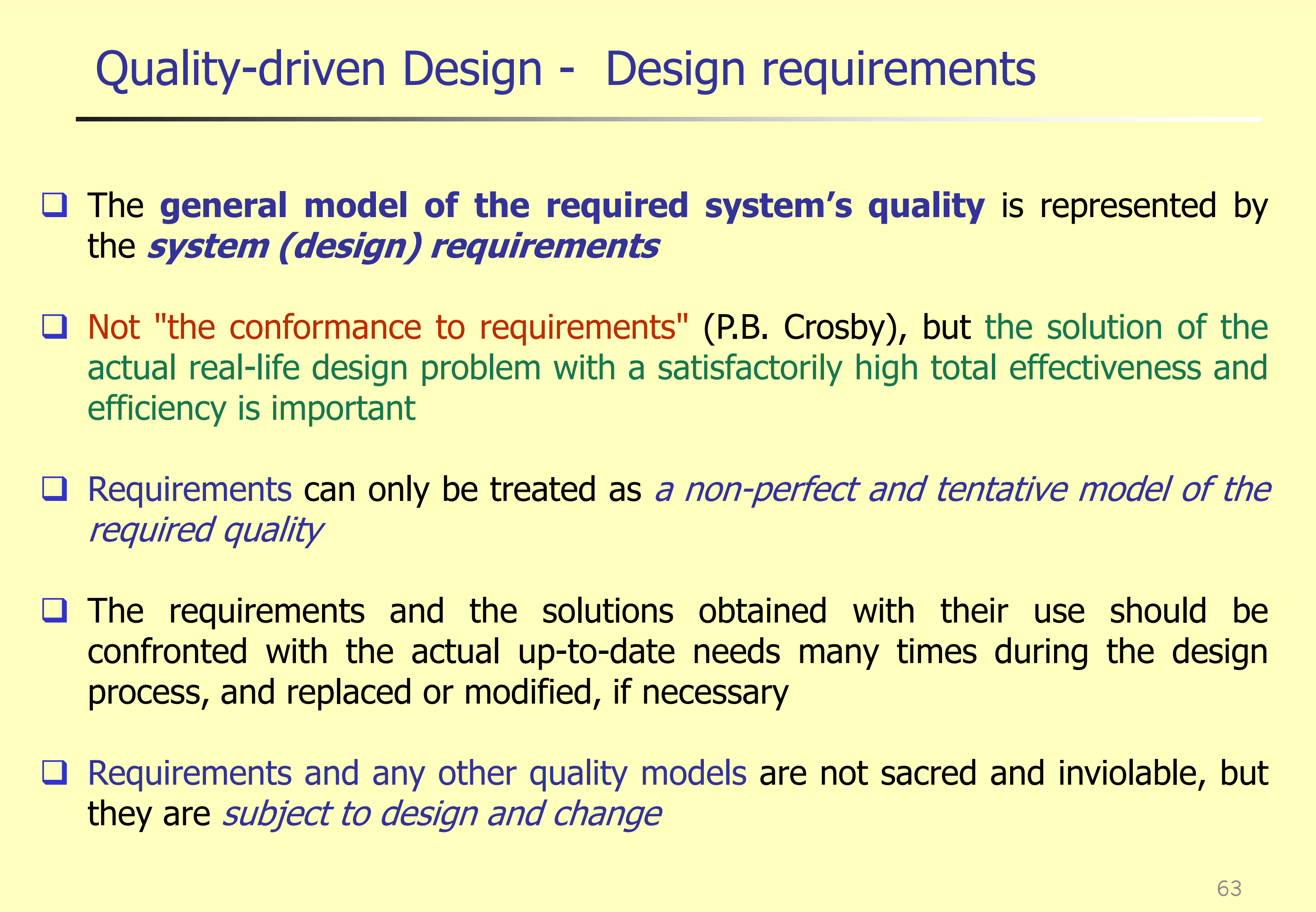
61



Quality-driven Design: Government regulations and standards

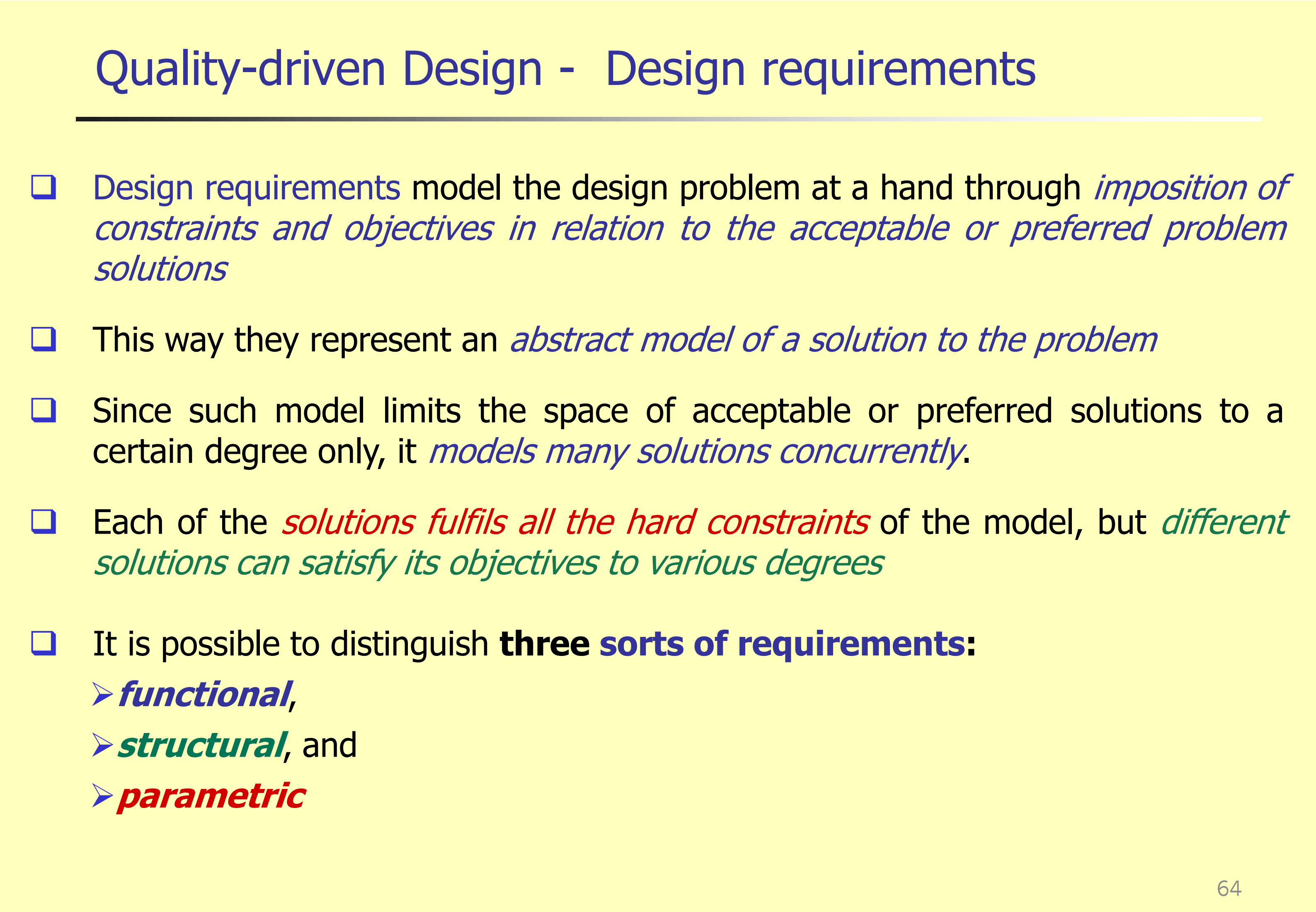
- ***Adequate government and branch regulations and standards are of primary importance for bringing into effect the green systems and green economy***
- Regulations and standards specify what is allowed or standard, and what is not
- They constitute general constraints for the industry and system designers that have to be satisfied by their designs, products and services
- Of course, particular systemic solutions satisfying these general constraints can still be very different, better or worse for the environment, but ***all systemic solutions have to satisfy the minimum required by the regulations and standards***
- Remember that the decisions made by companies and governments that caused the environmental destruction were mainly driven by short-term profit, without accounting for long-term consequences
- It would be naïve to expect that all companies and individuals will suddenly become environment-friendly without adequate regulations pressing them to do so

62



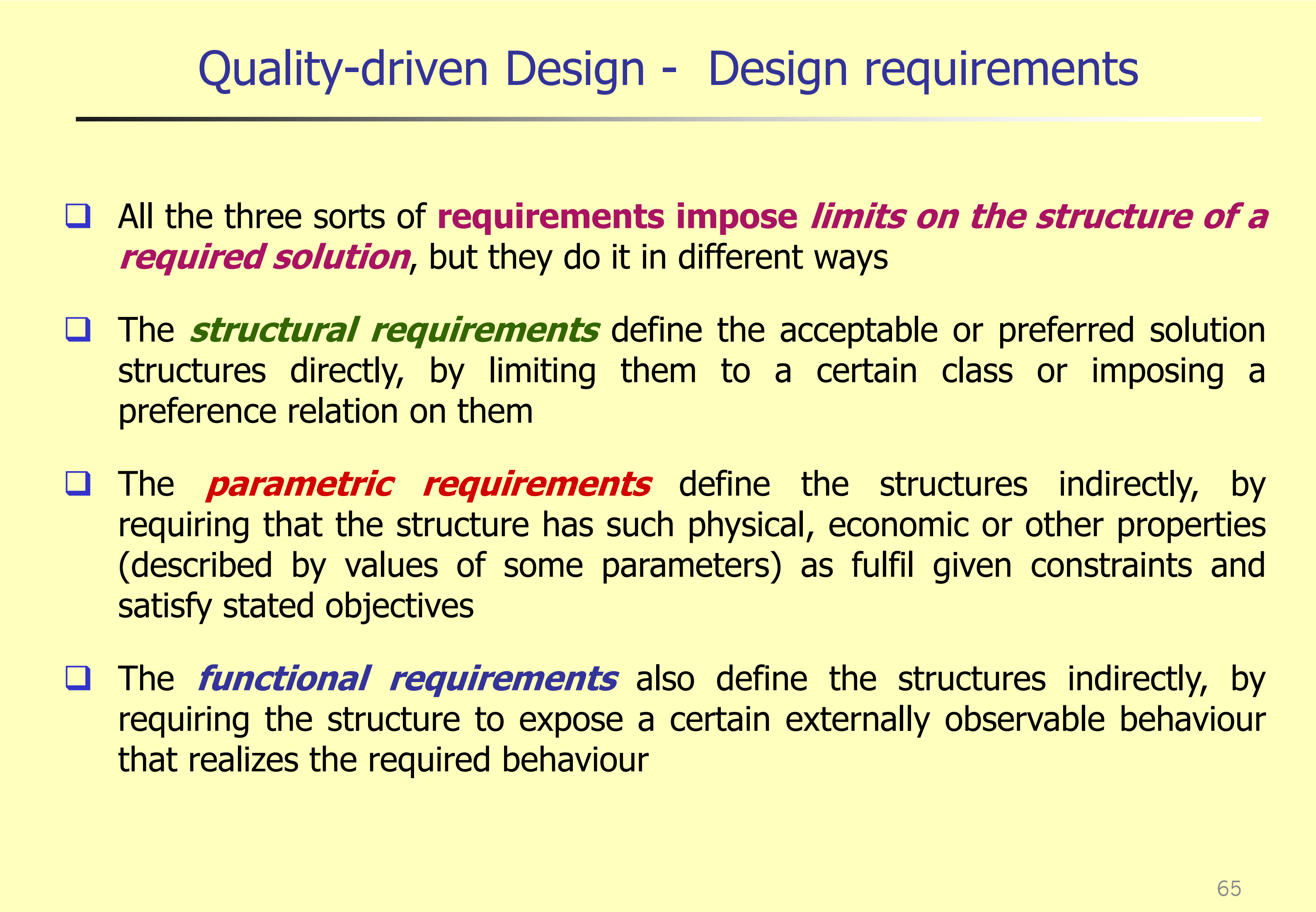
Quality-driven Design - Design requirements

- The **general model of the required system's quality** is represented by the ***system (design) requirements***
- Not "the conformance to requirements" (P.B. Crosby), but the solution of the actual real-life design problem with a satisfactorily high total effectiveness and efficiency is important
- Requirements can only be treated as *a non-perfect and tentative model of the required quality*
- The requirements and the solutions obtained with their use should be confronted with the actual up-to-date needs many times during the design process, and replaced or modified, if necessary
- Requirements and any other quality models are not sacred and inviolable, but they are *subject to design and change*



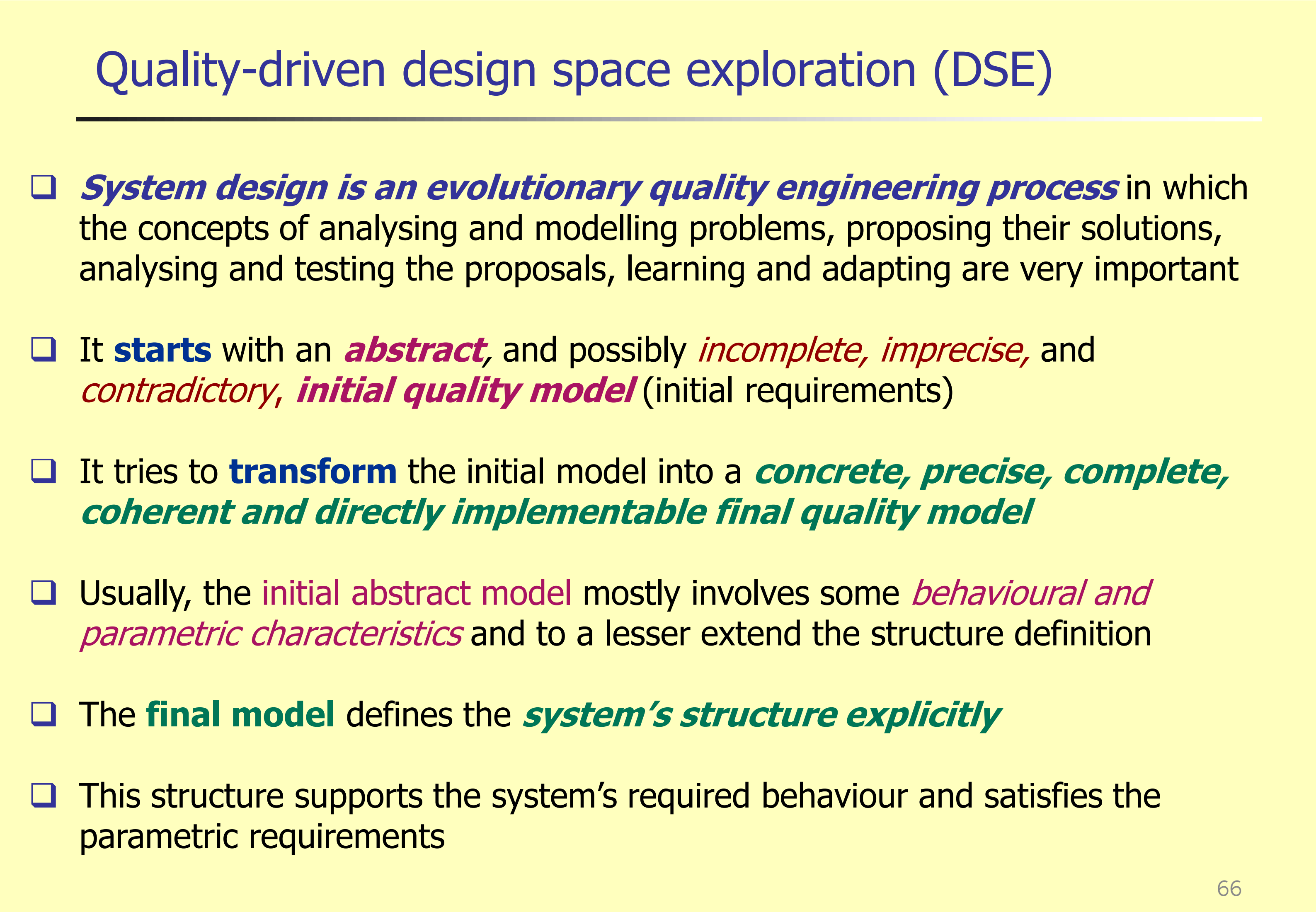
Quality-driven Design - Design requirements

- ❑ Design requirements model the design problem at a hand through *imposition of constraints and objectives in relation to the acceptable or preferred problem solutions*
- ❑ This way they represent an *abstract model of a solution to the problem*
- ❑ Since such model limits the space of acceptable or preferred solutions to a certain degree only, it *models many solutions concurrently*.
- ❑ Each of the *solutions fulfils all the hard constraints* of the model, but *different solutions can satisfy its objectives to various degrees*
- ❑ It is possible to distinguish **three sorts of requirements:**
  - ➢ ***functional***,
  - ➢ ***structural***, and
  - ➢ ***parametric***



Quality-driven Design - Design requirements

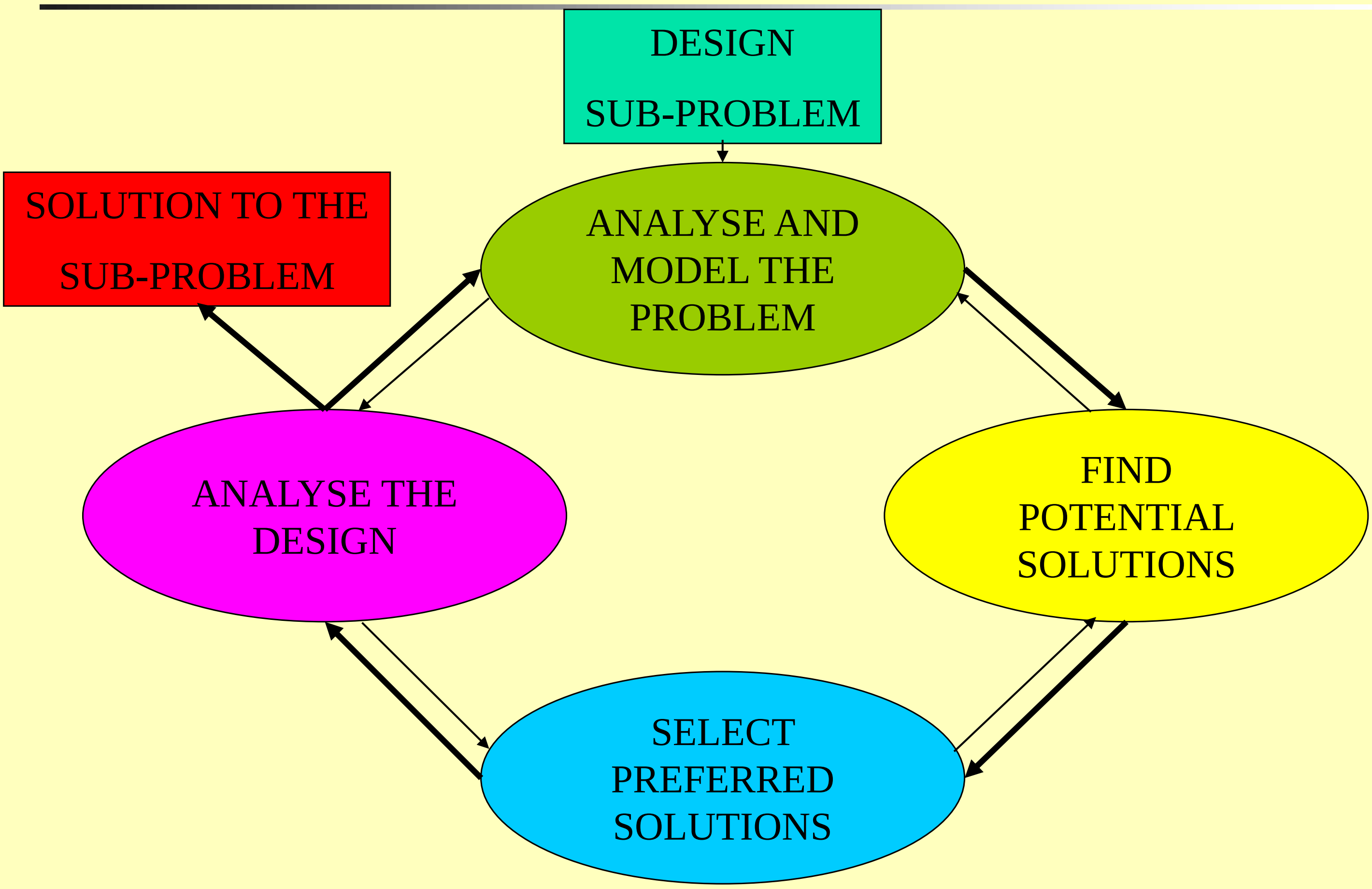
- ❑ All the three sorts of **requirements impose *limits on the structure of a required solution***, but they do it in different ways
- ❑ The ***structural requirements*** define the acceptable or preferred solution structures directly, by limiting them to a certain class or imposing a preference relation on them
- ❑ The ***parametric requirements*** define the structures indirectly, by requiring that the structure has such physical, economic or other properties (described by values of some parameters) as fulfil given constraints and satisfy stated objectives
- ❑ The ***functional requirements*** also define the structures indirectly, by requiring the structure to expose a certain externally observable behaviour that realizes the required behaviour



Quality-driven design space exploration (DSE)

- ***System design is an evolutionary quality engineering process*** in which the concepts of analysing and modelling problems, proposing their solutions, analysing and testing the proposals, learning and adapting are very important
- It **starts** with an ***abstract***, and possibly *incomplete, imprecise,* and *contradictory*, ***initial quality model*** (initial requirements)
- It tries to **transform** the initial model into a ***concrete, precise, complete, coherent and directly implementable final quality model***
- Usually, the initial abstract model mostly involves some *behavioural and parametric characteristics* and to a lesser extend the structure definition
- The **final model** defines the ***system's structure explicitly***
- This structure supports the system's required behaviour and satisfies the parametric requirements

Generic model of the quality-driven design space exploration



DESIGN SUB-PROBLEM

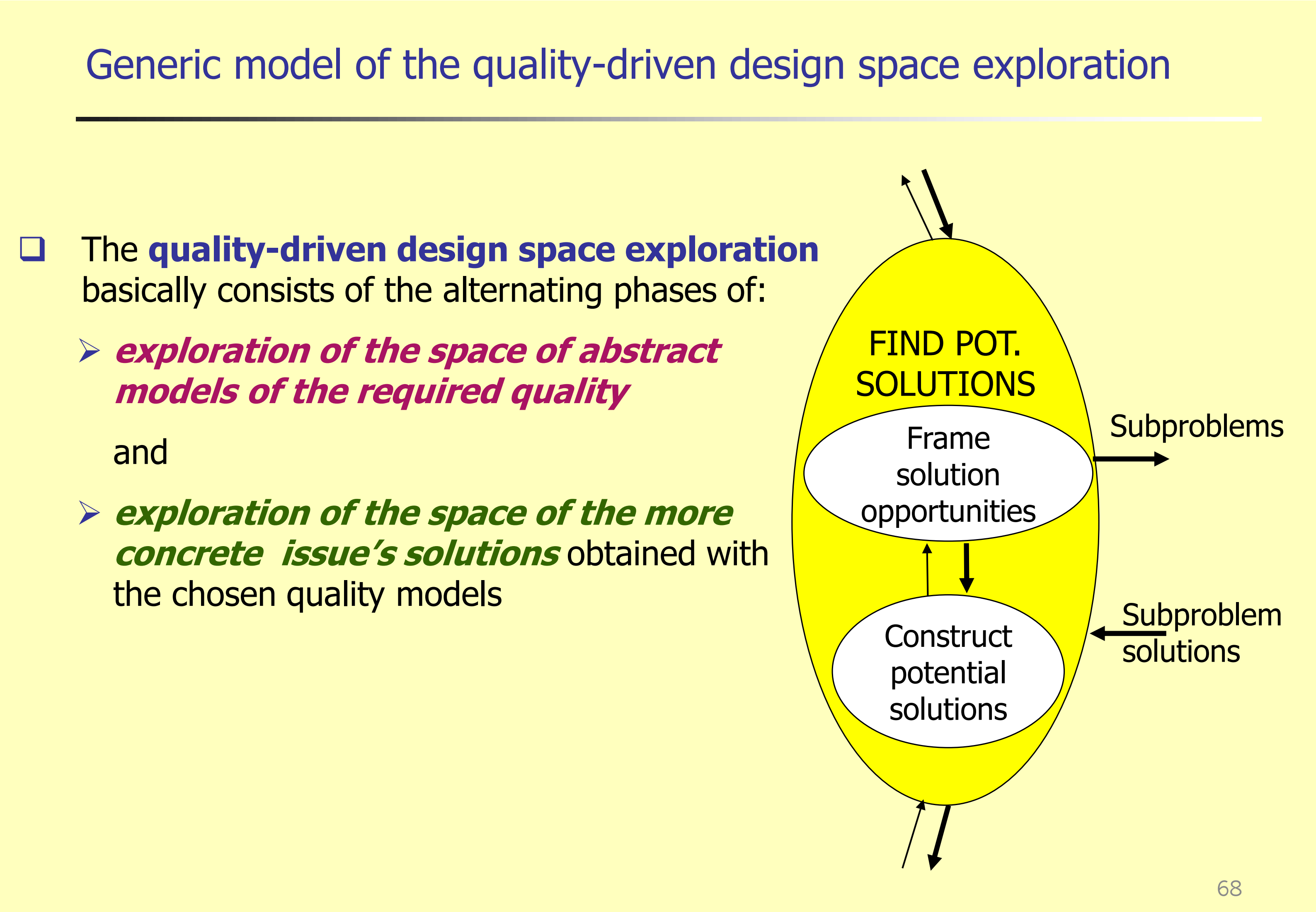
ANALYSE AND MODEL THE PROBLEM

FIND POTENTIAL SOLUTIONS

SELECT PREFERRED SOLUTIONS

ANALYSE THE DESIGN

SOLUTION TO THE SUB-PROBLEM



Generic model of the quality-driven design space exploration

- The **quality-driven design space exploration** basically consists of the alternating phases of:
  - ***exploration of the space of abstract models of the required quality***

    and
  - ***exploration of the space of the more concrete issue's solutions*** obtained with the chosen quality models

FIND POT. SOLUTIONS

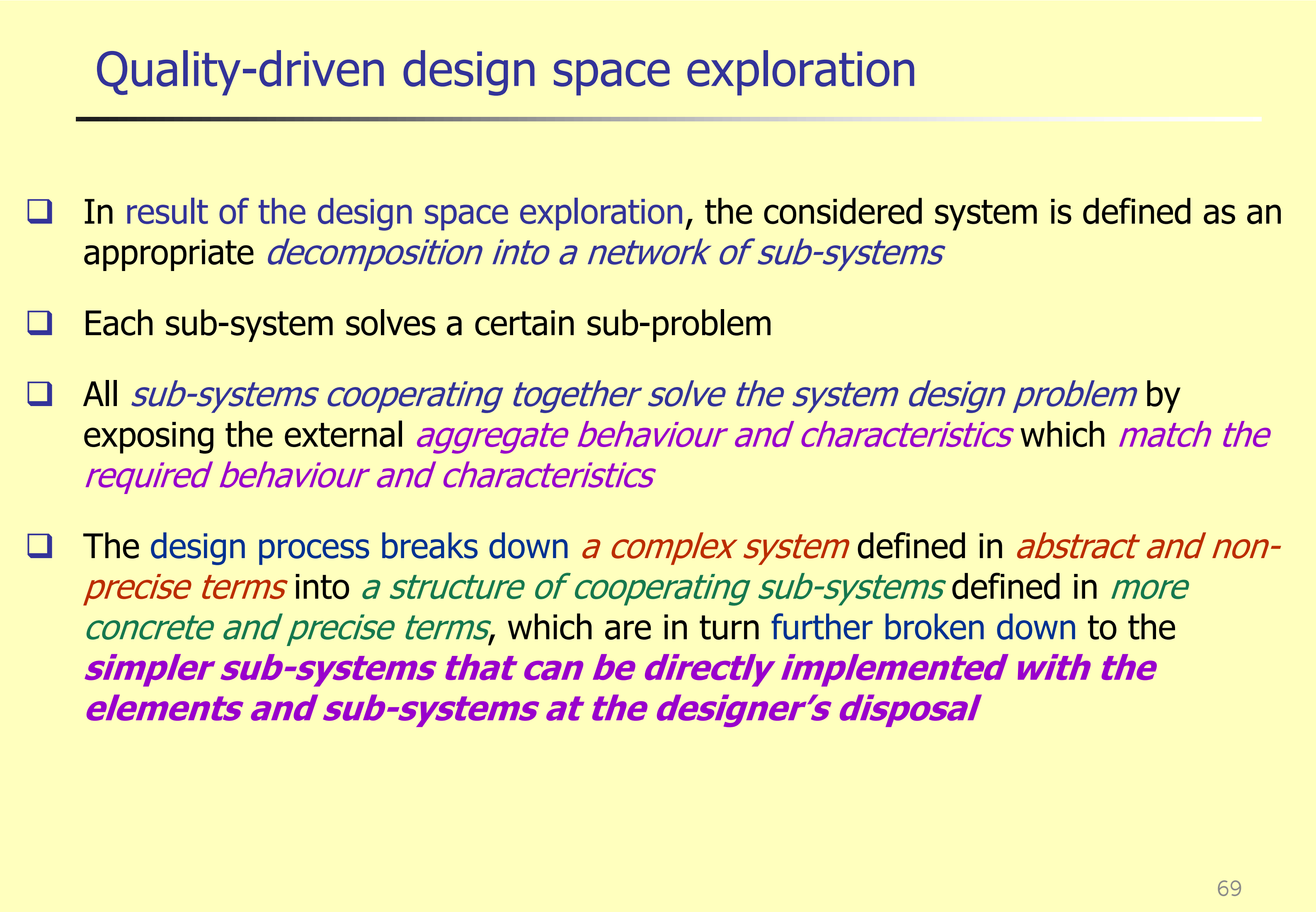
Frame solution opportunities

Construct potential solutions

Subproblems

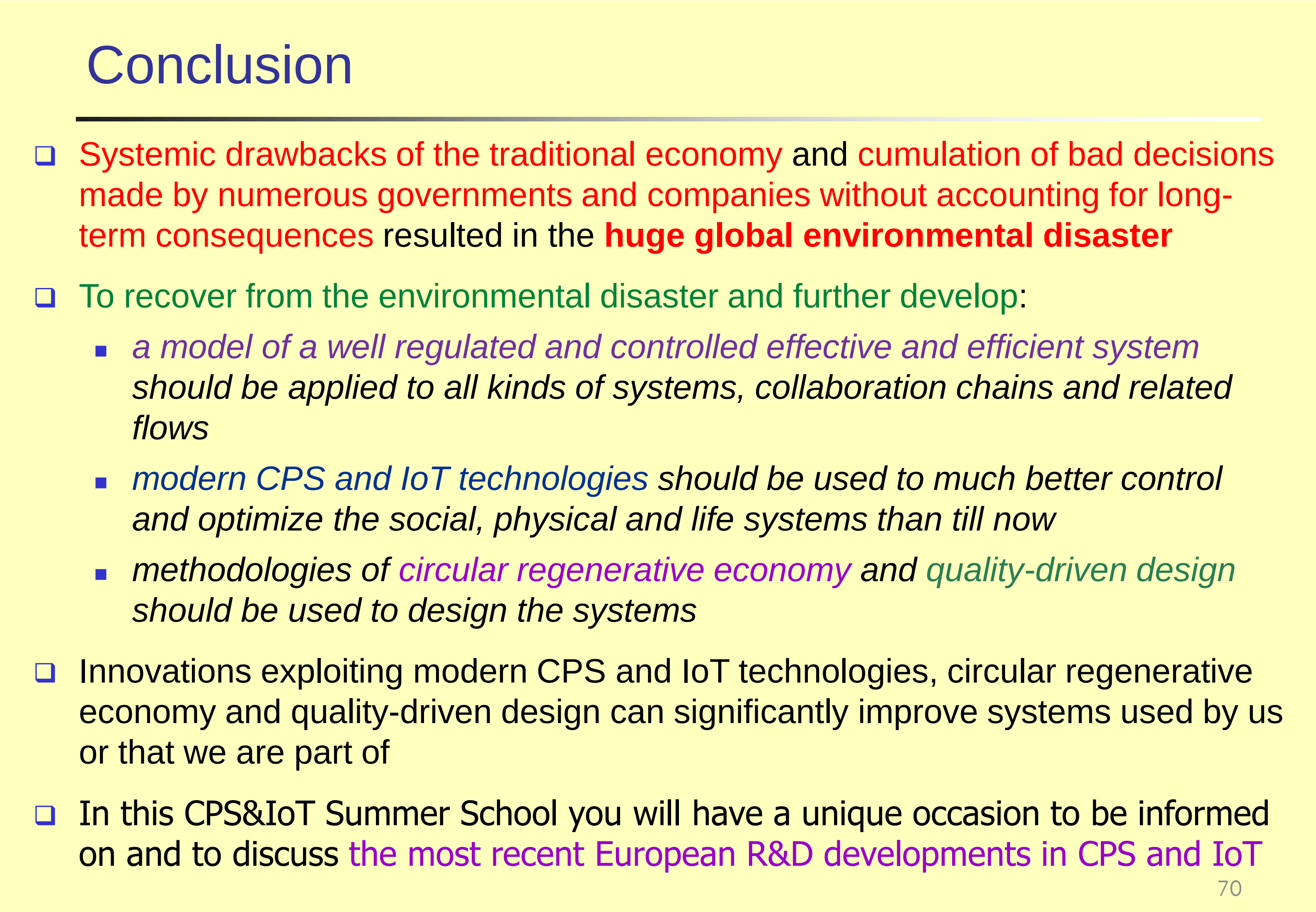
Subproblem solutions

68



Quality-driven design space exploration

- In result of the design space exploration, the considered system is defined as an appropriate *decomposition into a network of sub-systems*
- Each sub-system solves a certain sub-problem
- All *sub-systems cooperating together solve the system design problem* by exposing the external *aggregate behaviour and characteristics* which *match the required behaviour and characteristics*
- The design process breaks down *a complex system* defined in *abstract and non-precise terms* into *a structure of cooperating sub-systems* defined in *more concrete and precise terms*, which are in turn further broken down to the ***simpler sub-systems that can be directly implemented with the elements and sub-systems at the designer's disposal***



Conclusion

- Systemic drawbacks of the traditional economy and cumulation of bad decisions made by numerous governments and companies without accounting for long-term consequences resulted in the **huge global environmental disaster**
- To recover from the environmental disaster and further develop:
  - *a model of a well regulated and controlled effective and efficient system should be applied to all kinds of systems, collaboration chains and related flows*
  - *modern CPS and IoT technologies should be used to much better control and optimize the social, physical and life systems than till now*
  - *methodologies of circular regenerative economy and quality-driven design should be used to design the systems*
- Innovations exploiting modern CPS and IoT technologies, circular regenerative economy and quality-driven design can significantly improve systems used by us or that we are part of
- In this CPS&IoT Summer School you will have a unique occasion to be informed on and to discuss the most recent European R&D developments in CPS and IoT

70

EUROPEAN PROCESSOR INITIATIVE: Europe's Industrial HPC Processor Technology for the Exascale Era

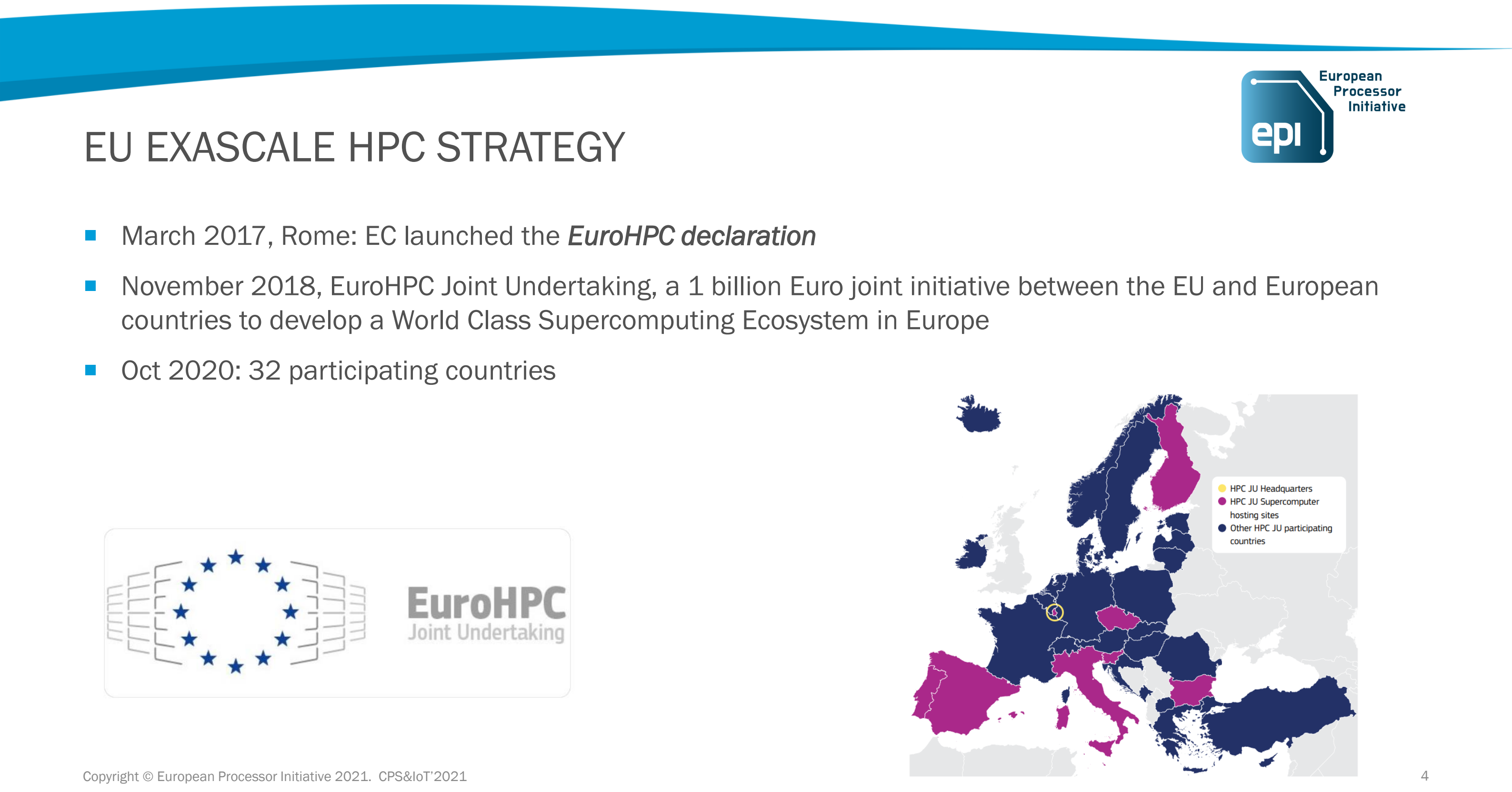
Mario Kovač, EPI Chief Communication Officer
mario.kovac@european-processor-initiative.eu; mario.kovac@fer.hr

THIS PROJECT HAS RECEIVED FUNDING FROM THE EUROPEAN UNION'S HORIZON 2020 RESEARCH AND INNOVATION PROGRAMME UNDER GRANT AGREEMENT NO 826647

1

Copyright © European Processor Initiative 2021. CPS&IoT'2021 2

THE STRATEGIC INTERPLAY



European Processor Initiative

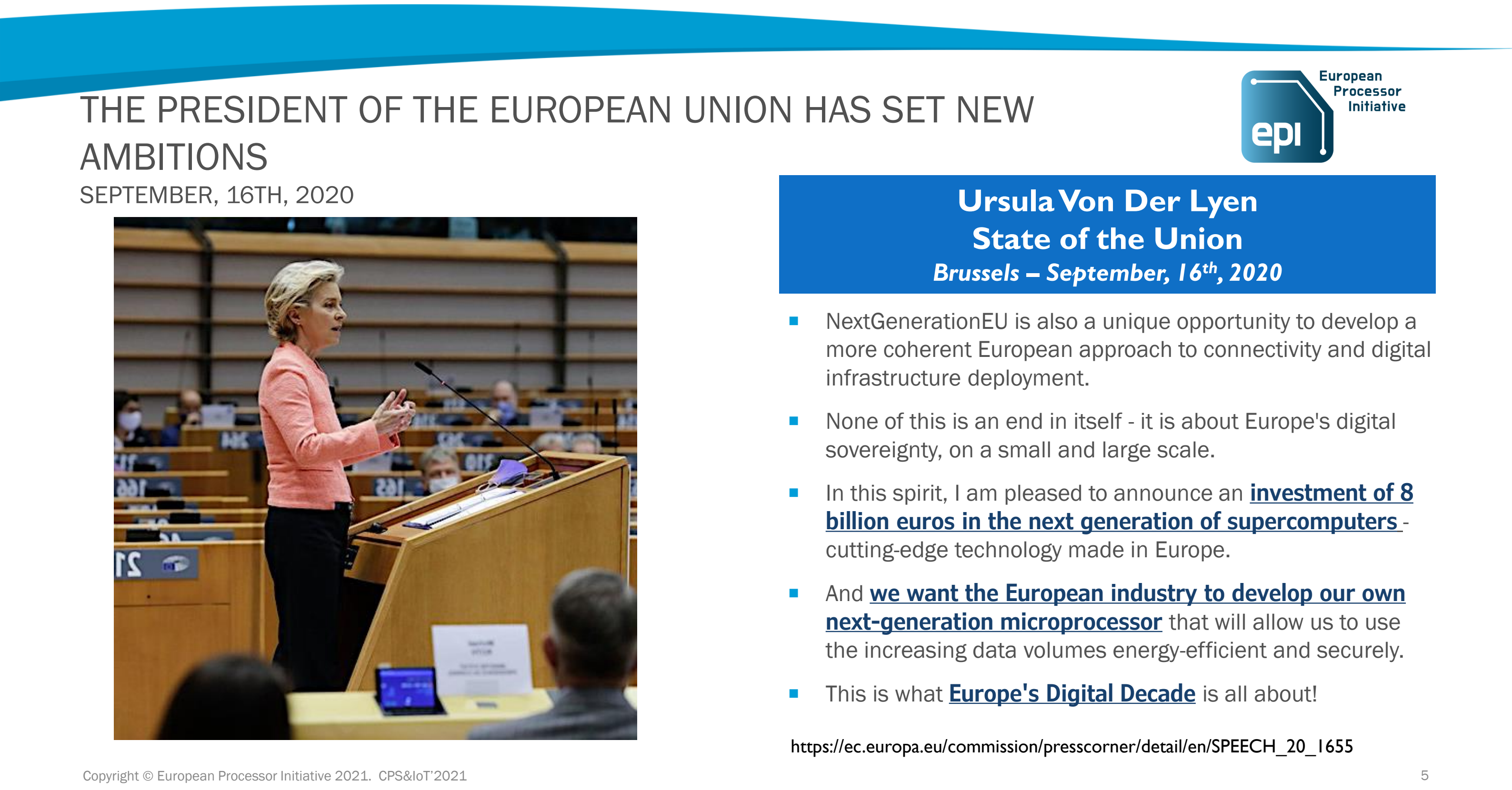
EU EXASCALE HPC STRATEGY

- March 2017, Rome: EC launched the ***EuroHPC declaration***
- November 2018, EuroHPC Joint Undertaking, a 1 billion Euro joint initiative between the EU and European countries to develop a World Class Supercomputing Ecosystem in Europe
- Oct 2020: 32 participating countries

EuroHPC Joint Undertaking

● HPC JU Headquarters
● HPC JU Supercomputer hosting sites
● Other HPC JU participating countries

4



THE PRESIDENT OF THE EUROPEAN UNION HAS SET NEW AMBITIONS

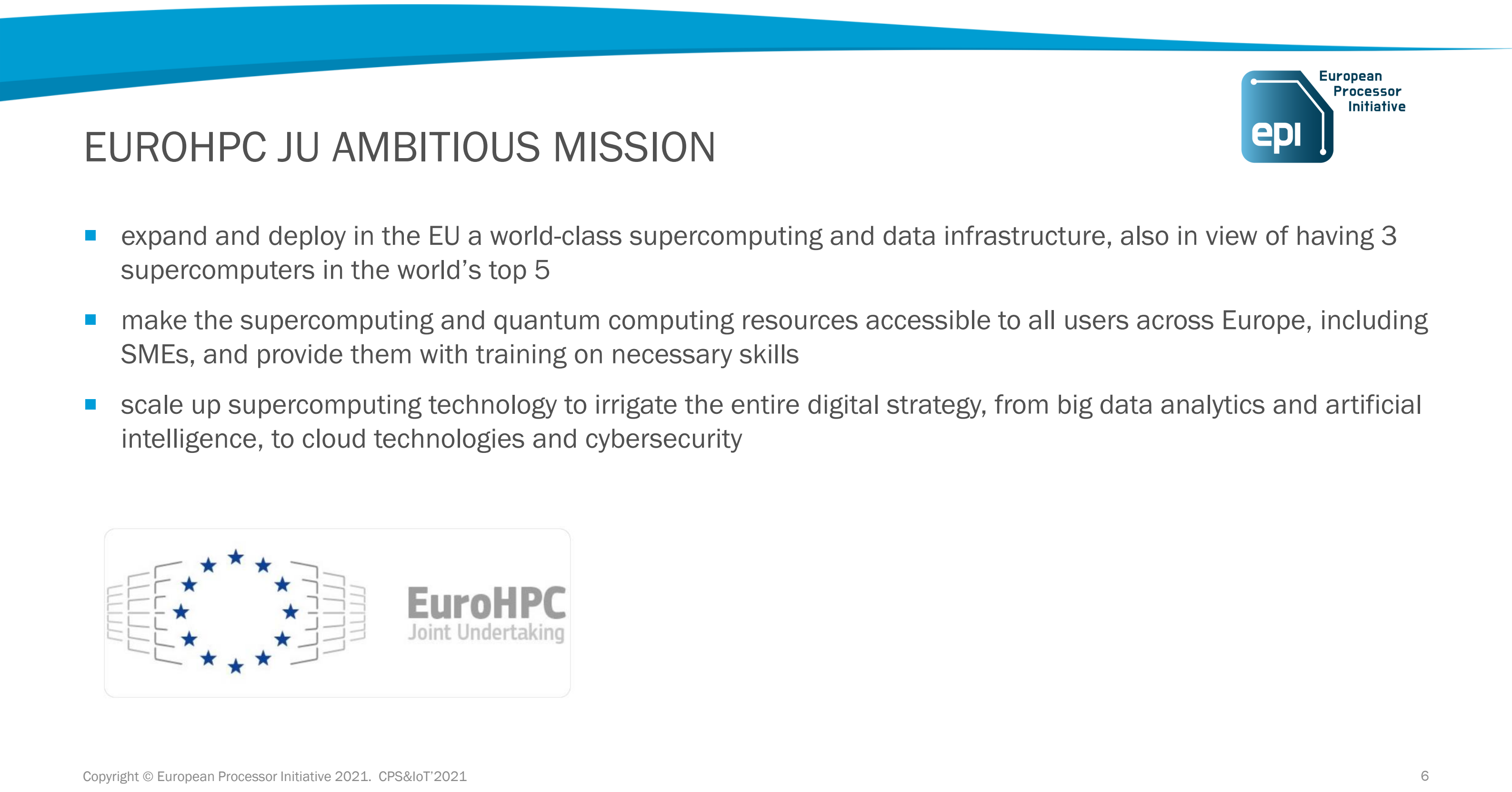
SEPTEMBER, 16TH, 2020

Ursula Von Der Lyen
State of the Union
Brussels – September, 16th, 2020

- NextGenerationEU is also a unique opportunity to develop a more coherent European approach to connectivity and digital infrastructure deployment.
- None of this is an end in itself - it is about Europe's digital sovereignty, on a small and large scale.
- In this spirit, I am pleased to announce an **investment of 8 billion euros in the next generation of supercomputers** - cutting-edge technology made in Europe.
- And **we want the European industry to develop our own next-generation microprocessor** that will allow us to use the increasing data volumes energy-efficient and securely.
- This is what **Europe's Digital Decade** is all about!

https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_20_1655

5



European
Processor
Initiative
epi

EUROHPC JU AMBITIOUS MISSION

- expand and deploy in the EU a world-class supercomputing and data infrastructure, also in view of having 3 supercomputers in the world's top 5
- make the supercomputing and quantum computing resources accessible to all users across Europe, including SMEs, and provide them with training on necessary skills
- scale up supercomputing technology to irrigate the entire digital strategy, from big data analytics and artificial intelligence, to cloud technologies and cybersecurity

6

Copyright © European Processor Initiative 2021. CPS&IoT'2021

7

DRIVERS OF THE EPI PROPOSAL

Societal challenges

- Climate change
- Cybersecurity
- Increasing energy needs
- Intensifying global competition
- Aging population
- Sovereignty (data, economical, embargo)

Image: https://www.compbiomed.eu/services/software-hub/

8

DRIVERS OF THE EPI PROPOSAL

- Connected mobility & *Autonomous Driving computing needs beyond 2023*
- Develop customized processors able to meet the performance needed for autonomous vehicles that would offer:
  - implementation of vehicle perception tasks in real-time in a fail-operational manner
  - increased computing performance, fail-operational, functional safety, cyber-security and real-time behaviour (RT)
  - compute resources with the same characteristics as their "big brothers" in exascale class supercomputers
- Sovereignty (data, economical, embargo)
- EU car manufacturing supremacy

European
Processor
Initiative

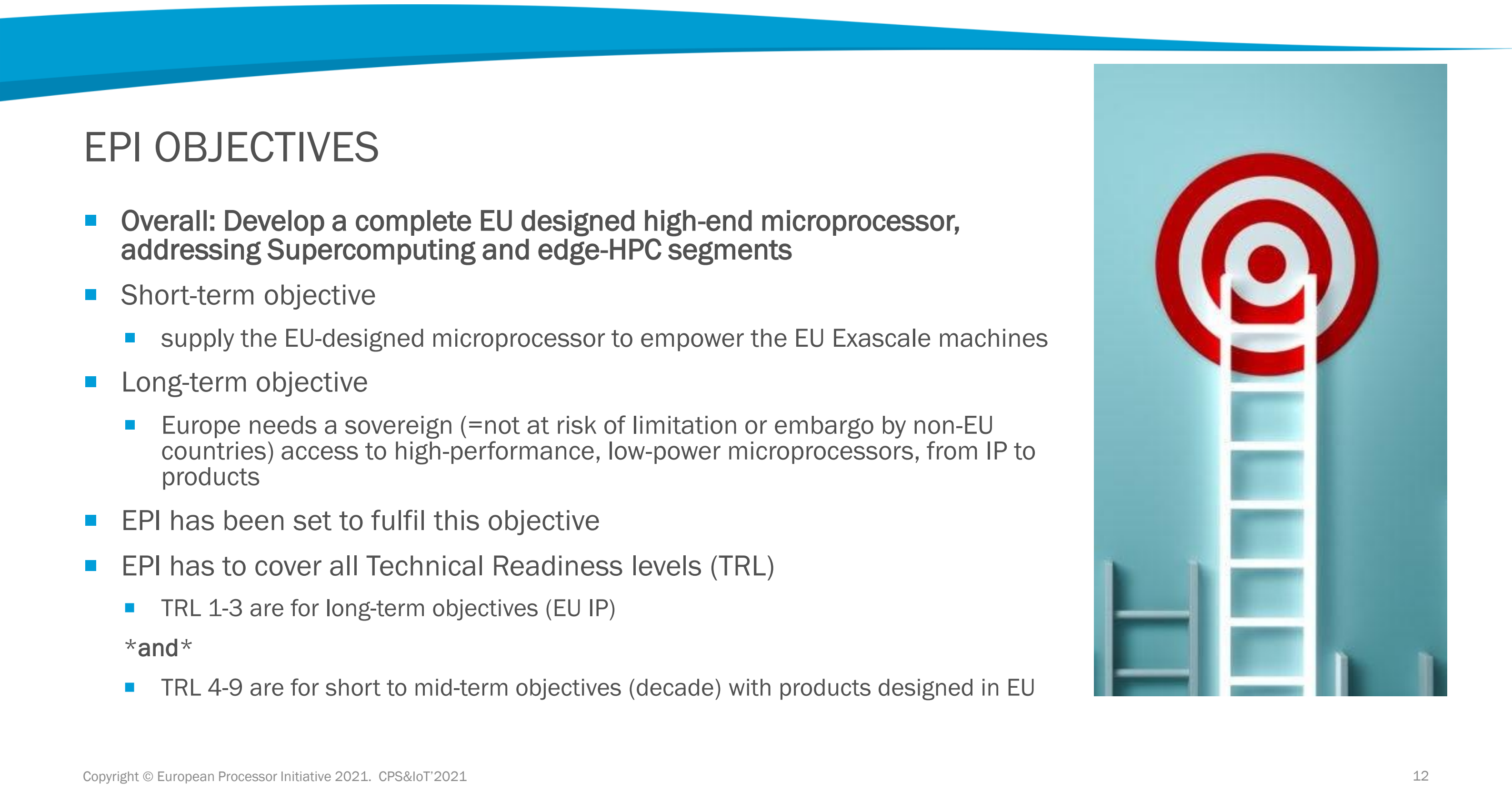
European
Processor
Initiative

10

28 PARTNERS FROM 10 EU COUNTRIES

European Processor Initiative
epi
BMW GROUP
MINI
Rolls-Royce Motor Cars Limited
Atos
infineon
BSC Barcelona Supercomputing Center Centro Nacional de Supercomputación
KERNKONZEPT
KALRAY
JÜLICH Forschungszentrum
semidynamics silicon design and verification services
TÉCNICO LISBOA
Fraunhofer
ALMA MATER STUDIORUM UNIVERSITÀ DI BOLOGNA
CHALMERS
UNIVERSITÀ DI PISA
FER University of Zagreb Faculty of Electrical Engineering and Computing
E4 COMPUTER ENGINEERING
CINECA
cea
SURF SARA
GENCI
FORTH INSTITUTE OF COMPUTER SCIENCE
ST
EXTOLL latency matters.
KIT Karlsruher Institut für Technologie
PROVE & RUN
ETH zürich
Elektrobit
menta
SIPEARL The Silicon Pearl

11



EPI OBJECTIVES

- **Overall: Develop a complete EU designed high-end microprocessor, addressing Supercomputing and edge-HPC segments**
- Short-term objective
  - supply the EU-designed microprocessor to empower the EU Exascale machines
- Long-term objective
  - Europe needs a sovereign (=not at risk of limitation or embargo by non-EU countries) access to high-performance, low-power microprocessors, from IP to products
- EPI has been set to fulfil this objective
- EPI has to cover all Technical Readiness levels (TRL)
  - TRL 1-3 are for long-term objectives (EU IP)

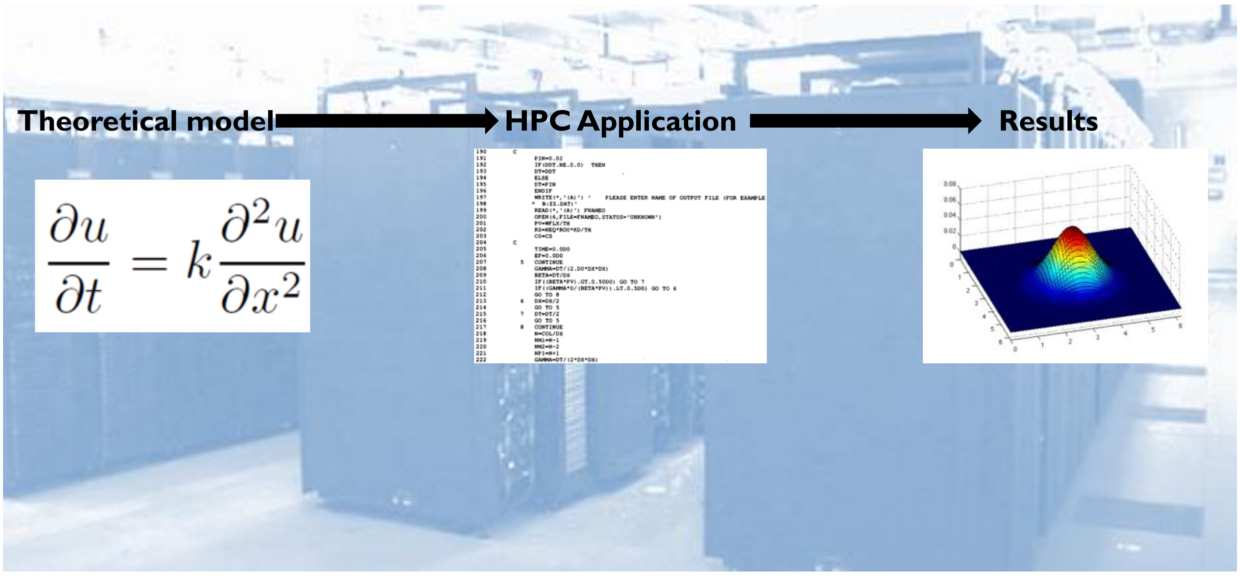
  and

  - TRL 4-9 are for short to mid-term objectives (decade) with products designed in EU

12

MERGE OF HPC AND AI

HPC BEFORE ARTIFICIAL INTELLIGENCE

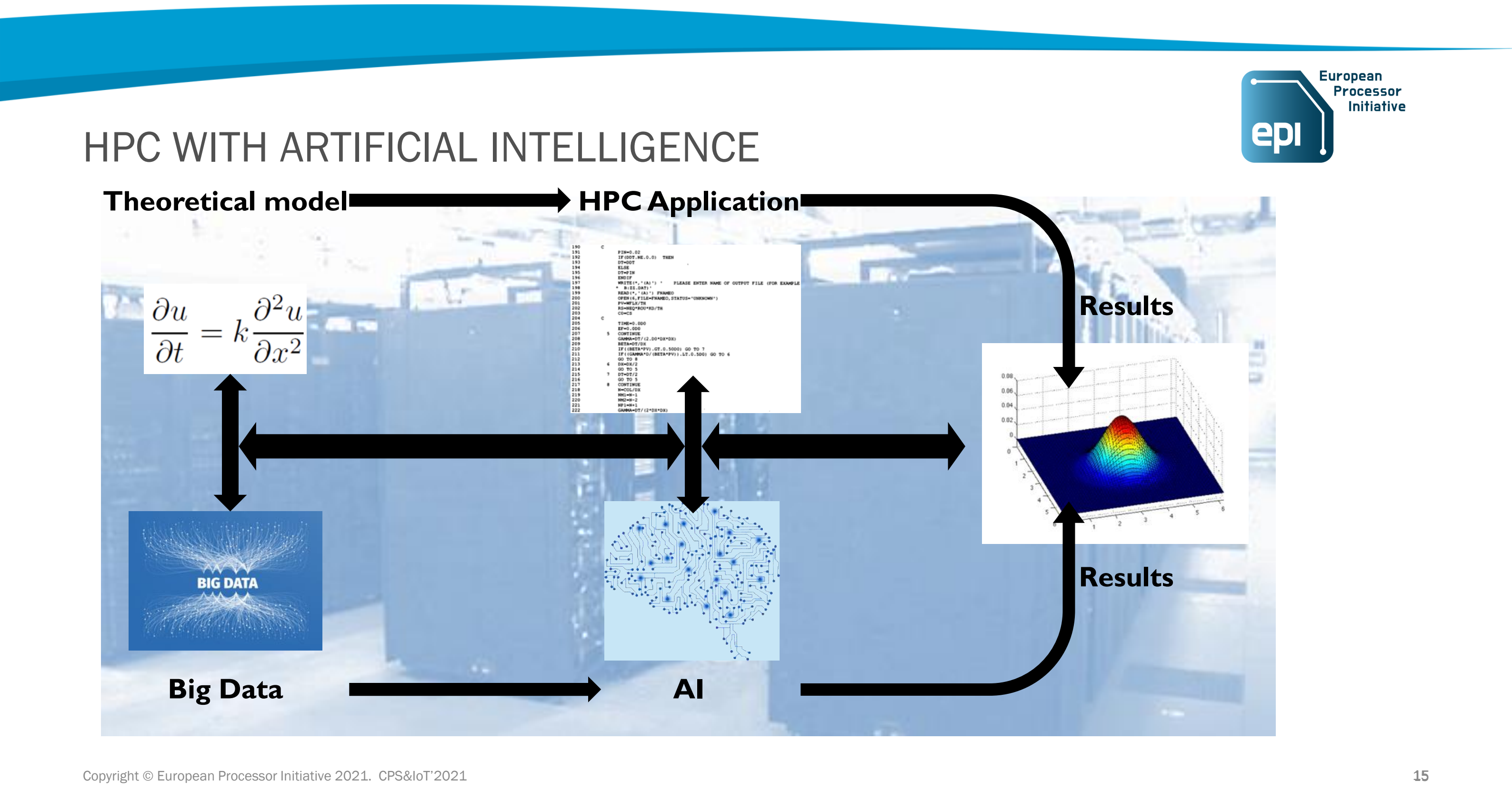


Theoretical model → HPC Application → Results

$$\frac{\partial u}{\partial t} = k\frac{\partial^2 u}{\partial x^2}$$

```
C
      PIN=0.02
      IF(DDT.NE.0.0)  THEN
      DT=DDT
      ELSE
      DT=PIN
      ENDIF
      WRITE(*,'(A)') '    PLEASE ENTER NAME OF OUTPUT FILE (FOR EXAMPLE
     *  B:ZZ.DAT)'
      READ(*,'(A)') FNAMEO
      OPEN(6,FILE=FNAMEO,STATUS='UNKNOWN')
      PV=WFLX/TH
      RS=NEQ*ROU*KD/TH
      CO=CS
C
      TIME=0.0D0
      EF=0.0D0
    5 CONTINUE
      GAMMA=DT/(2.D0*DX*DX)
      BETA=DT/DX
      IF((BETA*PV).GT.0.50D0) GO TO 7
      IF((GAMMA*D/(BETA*PV)).LT.0.5D0) GO TO 6
      GO TO 8
    6 DX=DX/2
      GO TO 5
    7 DT=DT/2
      GO TO 5
    8 CONTINUE
      N=COL/DX
      NM1=N-1
      NM2=N-2
      NP1=N+1
      GAMMA=DT/(2*DX*DX)
```

Copyright © European Processor Initiative 2021. CPS&IoT’2021



HPC WITH ARTIFICIAL INTELLIGENCE

Theoretical model

HPC Application

$$\frac{\partial u}{\partial t} = k\frac{\partial^2 u}{\partial x^2}$$

```
      C
            PIN=0.02
            IF(DDT.NE.0.0)  THEN
            DT=DDT
            ELSE
            DT=PIN
            ENDIF
            WRITE(*,'(A)') '    PLEASE ENTER NAME OF OUTPUT FILE (FOR EXAMPLE
           *  B:ZZ.DAT)'
            READ(*,'(A)') FNAMEO
            OPEN(6,FILE=FNAMEO,STATUS='UNKNOWN')
            PV=WFLX/TH
            RS=NEQ*ROU*KD/TH
            CO=CS
      C
            TIME=0.0D0
            EF=0.0D0
        5   CONTINUE
            GAMMA=DT/(2.D0*DX*DX)
            BETA=DT/DX
            IF((BETA*PV).GT.0.50D0) GO TO 7
            IF((GAMMA*D/(BETA*PV)).LT.0.5D0) GO TO 6
            GO TO 8
        6   DX=DX/2
            GO TO 5
        7   DT=DT/2
            GO TO 5
        8   CONTINUE
            N=COL/DX
            NM1=N-1
            NM2=N-2
            NP1=N+1
            GAMMA=DT/(2*DX*DX)
```

Results

Results

Big Data

AI

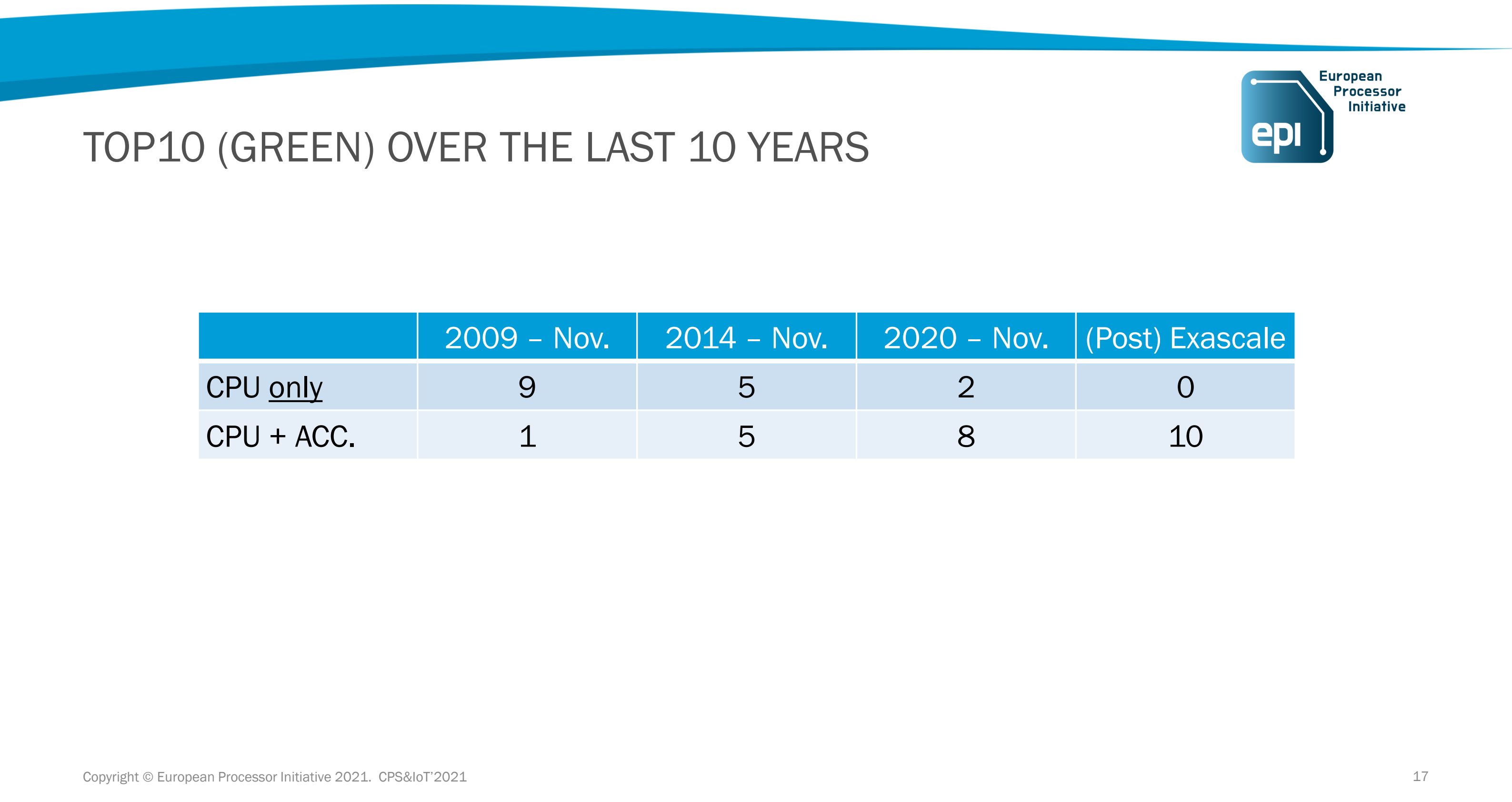
Copyright © European Processor Initiative 2021. CPS&IoT'2021

15

©MECO.net

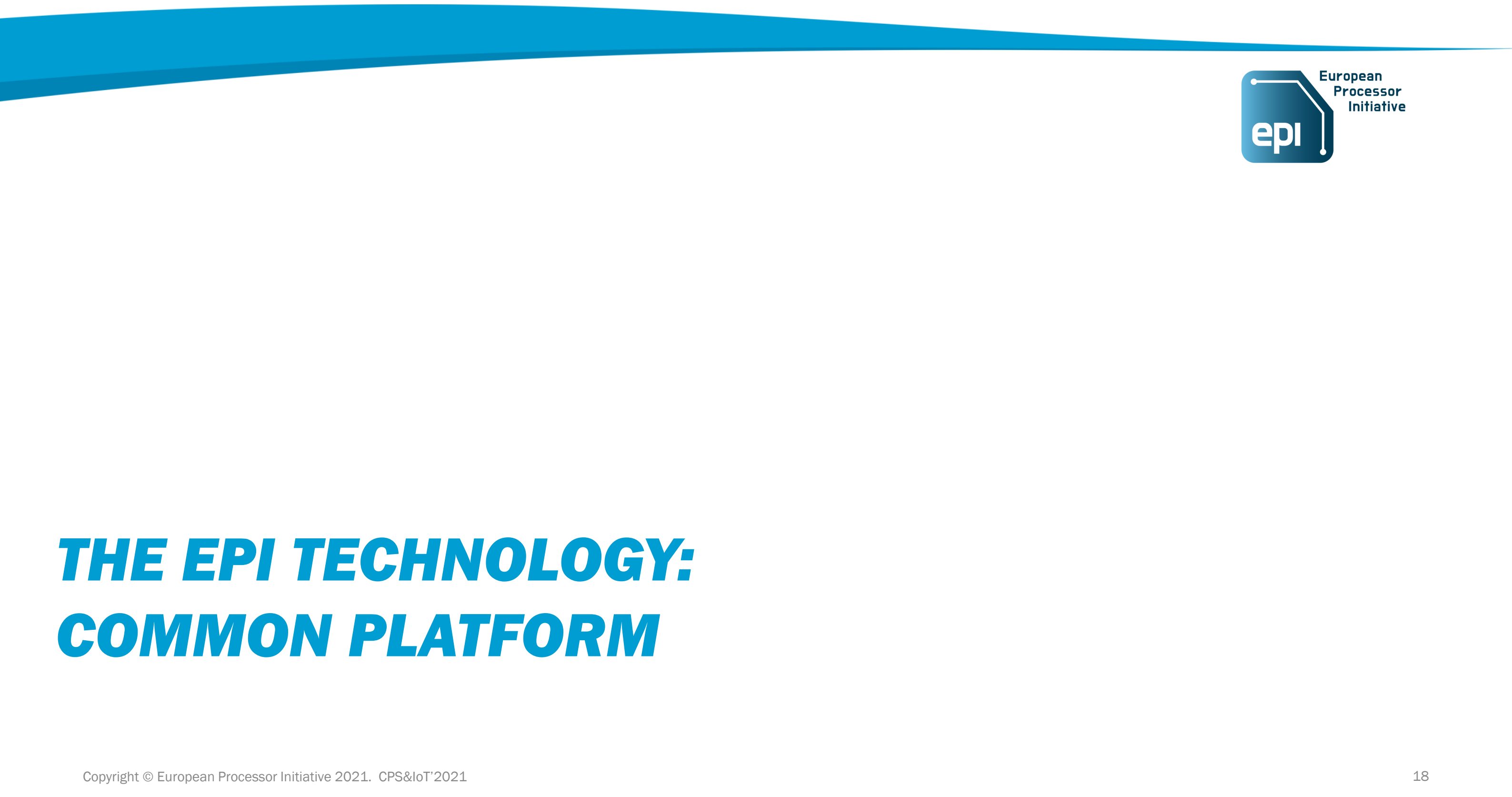
Cambrian explosion
Achieving performance through specialization

Courtesy Steve Scott
Cray CTO



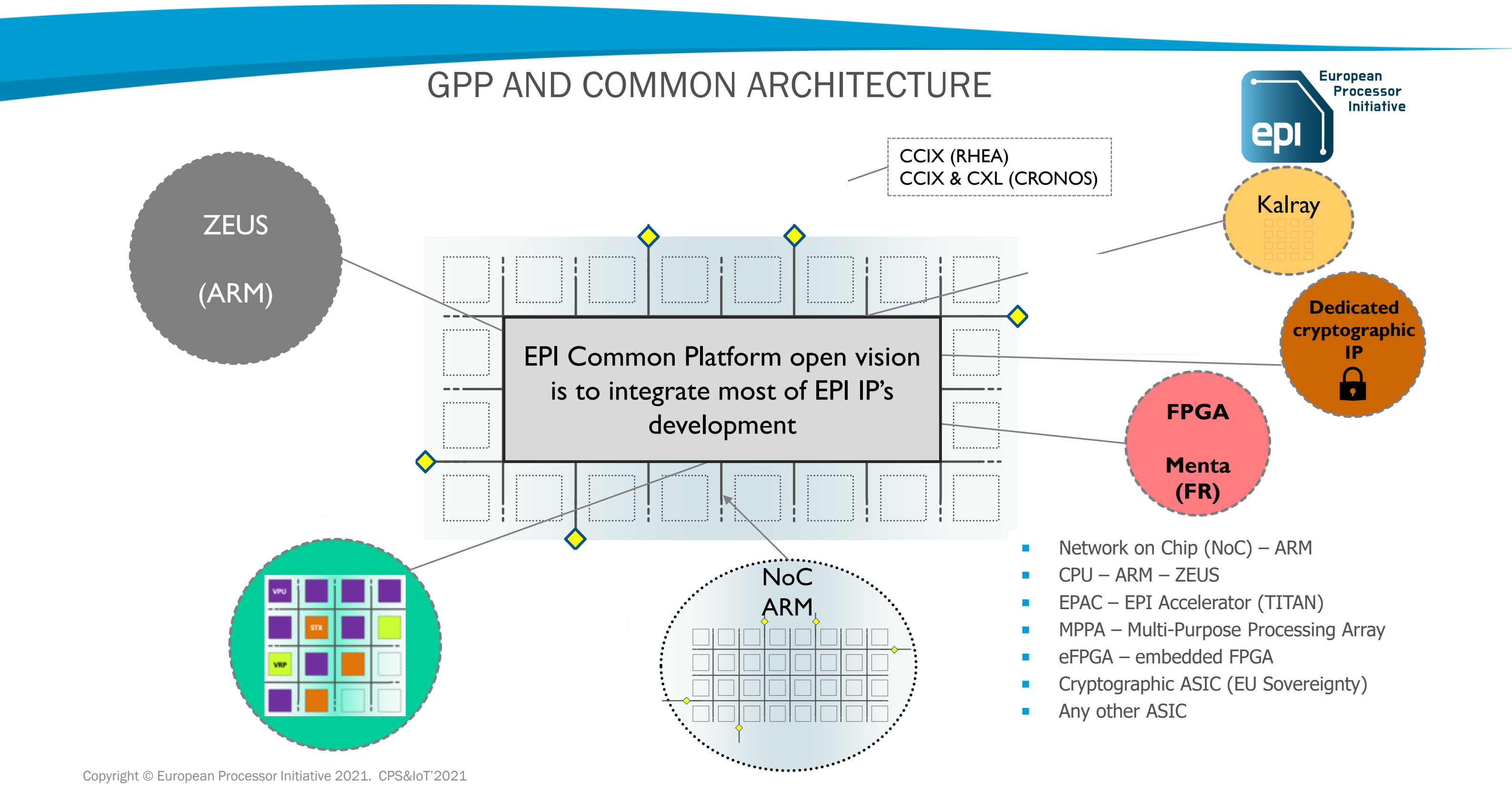
TOP10 (GREEN) OVER THE LAST 10 YEARS

	2009 – Nov.	2014 – Nov.	2020 – Nov.	(Post) Exascale
CPU only	9	5	2	0
CPU + ACC.	1	5	8	10



European Processor Initiative
epi

THE EPI TECHNOLOGY: COMMON PLATFORM



GPP AND COMMON ARCHITECTURE

European Processor Initiative

epi

CCIX (RHEA)
CCIX & CXL (CRONOS)

ZEUS

(ARM)

EPI Common Platform open vision is to integrate most of EPI IP's development

Kalray

Dedicated cryptographic IP

FPGA

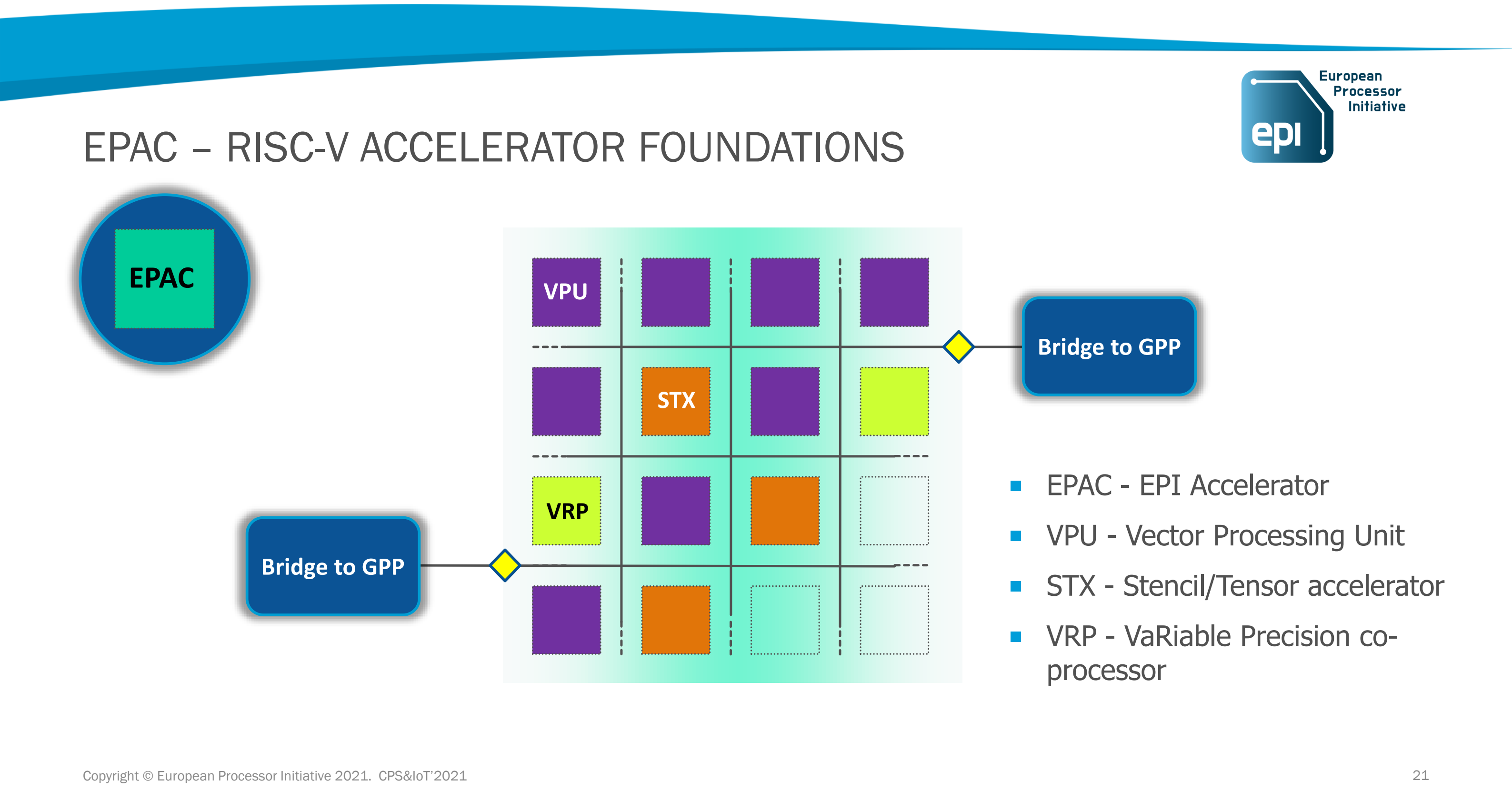
Menta (FR)

NoC
ARM

- Network on Chip (NoC) – ARM
- CPU – ARM – ZEUS
- EPAC – EPI Accelerator (TITAN)
- MPPA – Multi-Purpose Processing Array
- eFPGA – embedded FPGA
- Cryptographic ASIC (EU Sovereignty)
- Any other ASIC

European Processor Initiative

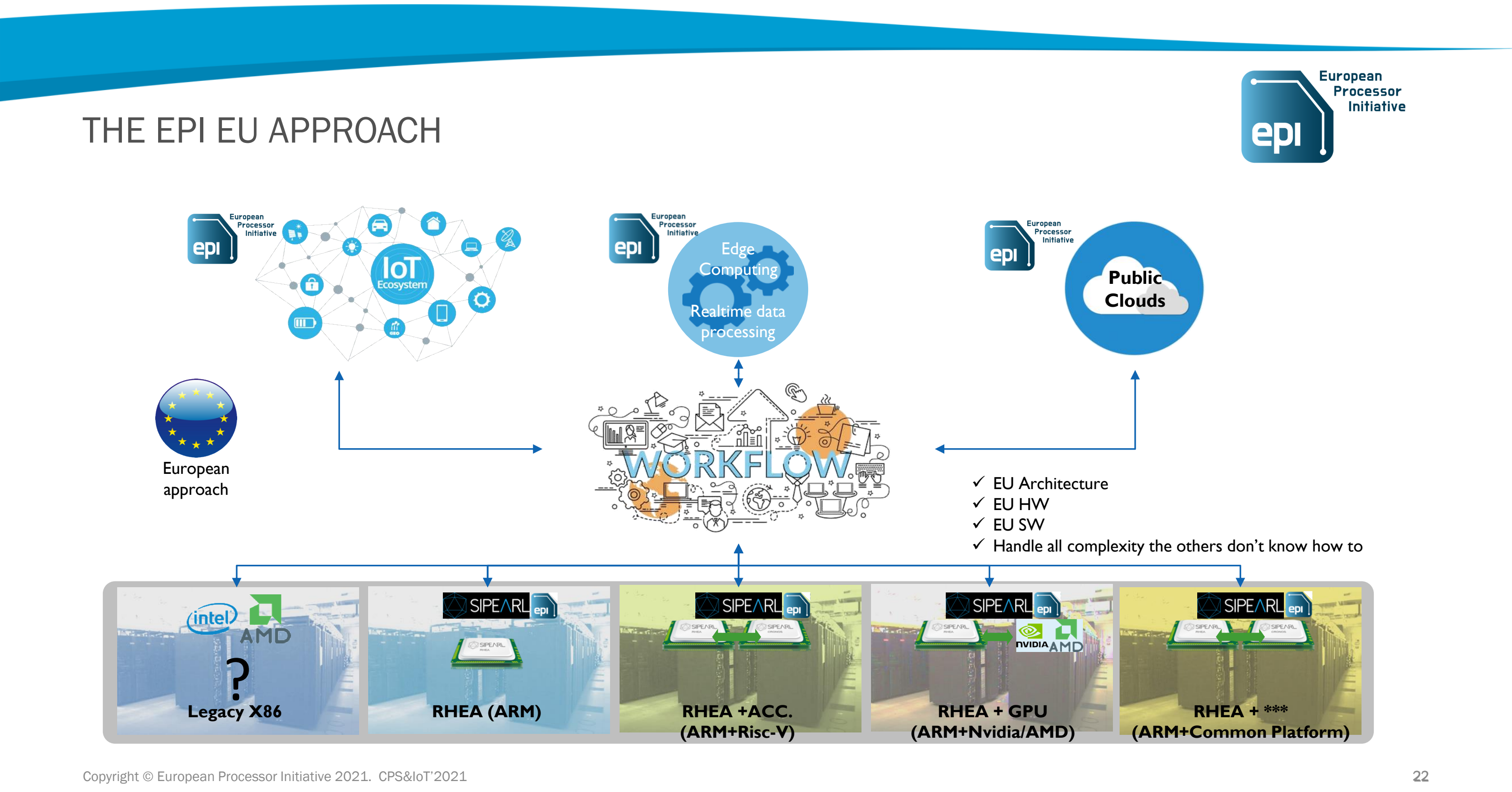
THE EPI TECHNOLOGY: ACCELERATORS



EPAC – RISC-V ACCELERATOR FOUNDATIONS

- EPAC - EPI Accelerator
- VPU - Vector Processing Unit
- STX - Stencil/Tensor accelerator
- VRP - VaRiable Precision co-processor

21



THE EPI EU APPROACH

European approach

- ✓ EU Architecture
- ✓ EU HW
- ✓ EU SW
- ✓ Handle all complexity the others don't know how to

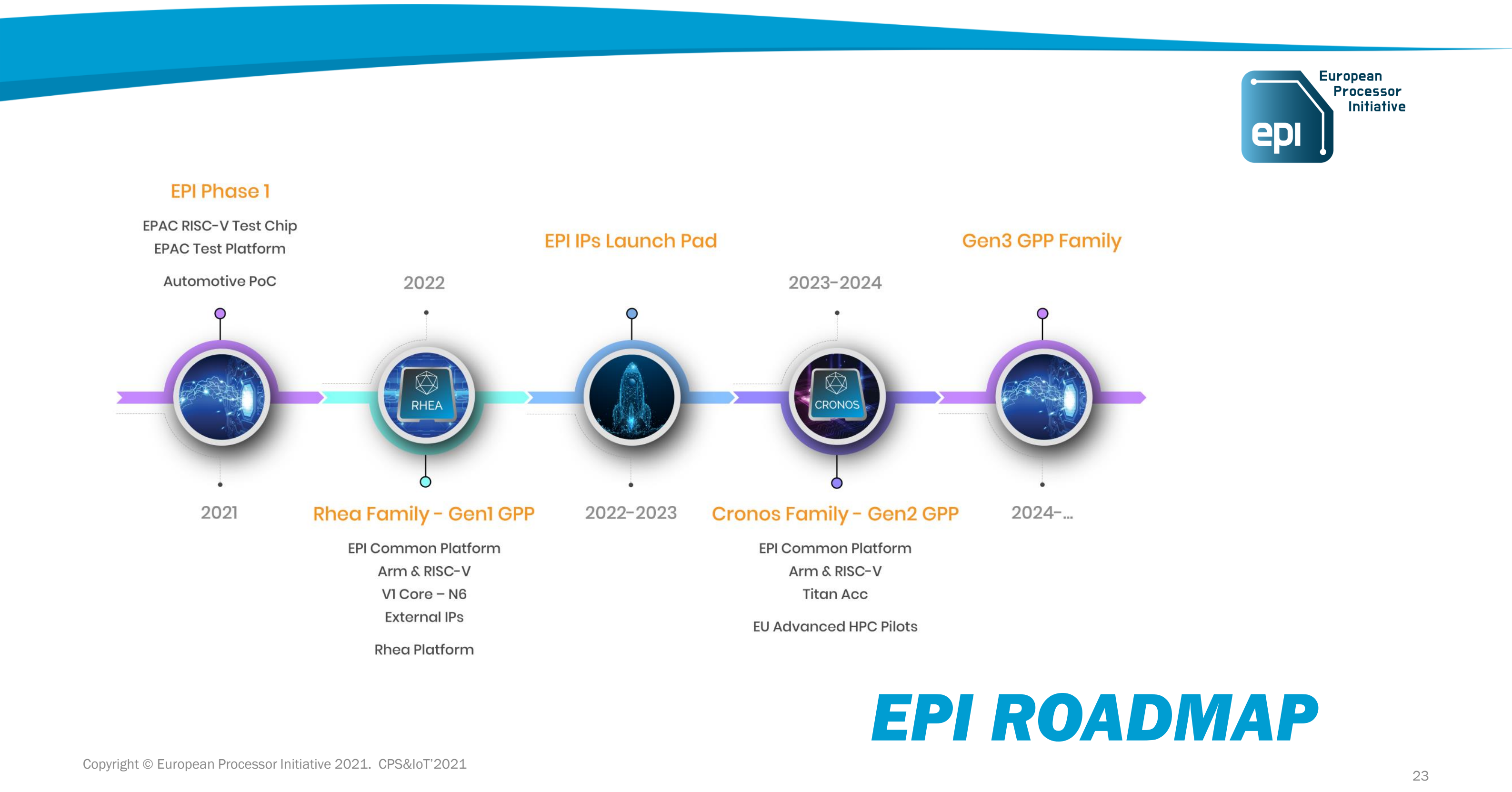
Legacy X86

RHEA (ARM)

RHEA +ACC. (ARM+Risc-V)

RHEA + GPU (ARM+Nvidia/AMD)

RHEA + *** (ARM+Common Platform)



European Processor Initiative

EPI Phase 1

EPAC RISC-V Test Chip
EPAC Test Platform

Automotive PoC

2021

2022

Rhea Family - Gen1 GPP

EPI Common Platform
Arm & RISC-V
V1 Core – N6
External IPs

Rhea Platform

EPI IPs Launch Pad

2022-2023

2023-2024

Cronos Family - Gen2 GPP

EPI Common Platform
Arm & RISC-V
Titan Acc

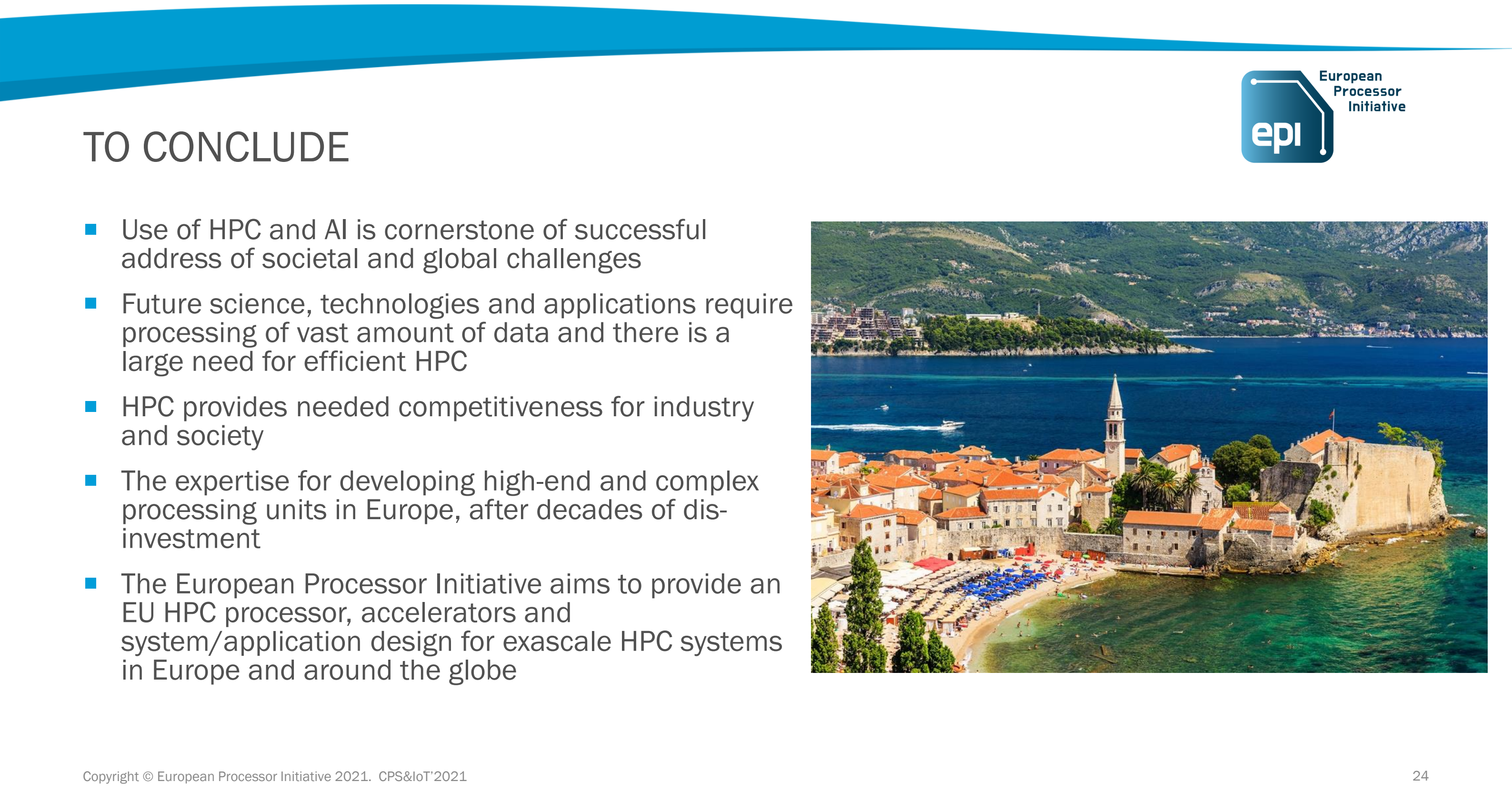
EU Advanced HPC Pilots

Gen3 GPP Family

2024-...

EPI ROADMAP

23



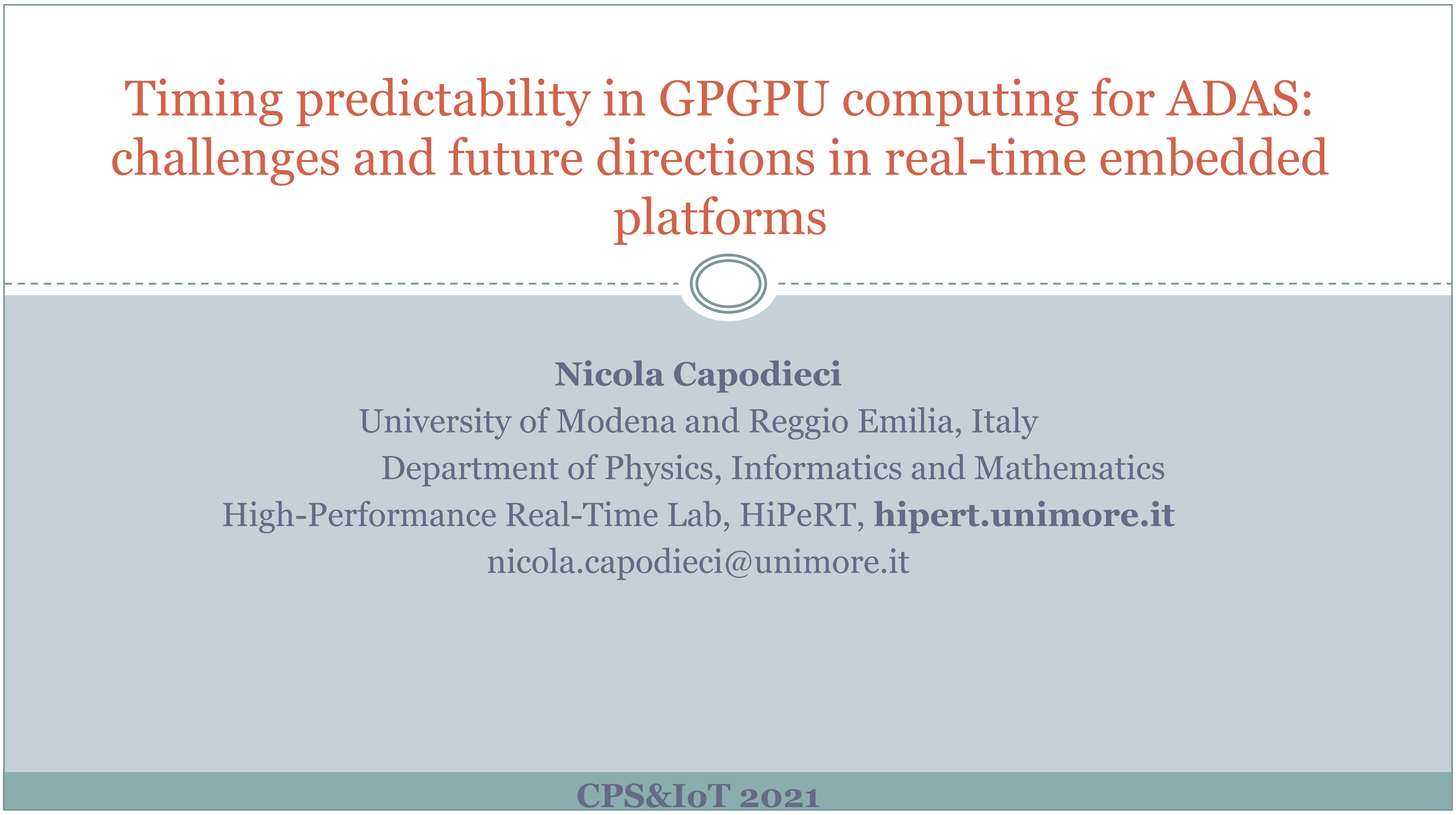
TO CONCLUDE

- Use of HPC and AI is cornerstone of successful address of societal and global challenges
- Future science, technologies and applications require processing of vast amount of data and there is a large need for efficient HPC
- HPC provides needed competitiveness for industry and society
- The expertise for developing high-end and complex processing units in Europe, after decades of dis-investment
- The European Processor Initiative aims to provide an EU HPC processor, accelerators and system/application design for exascale HPC systems in Europe and around the globe

THANK YOU FOR YOUR ATTENTION

- w www.european-processor-initiative.eu
- @EuProcessor
- in European Processor Initiative
- European Processor Initiative

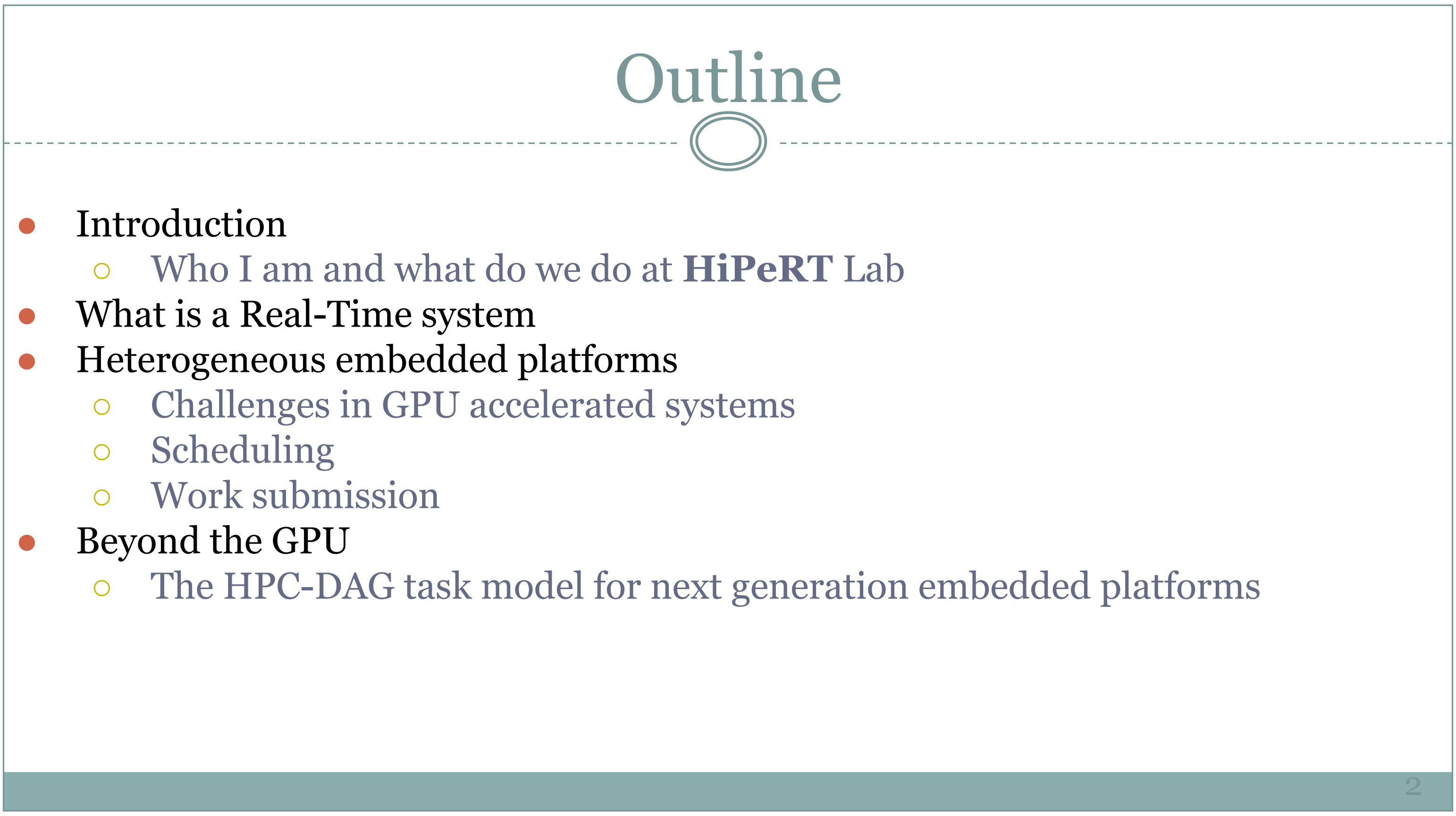
25



Timing predictability in GPGPU computing for ADAS: challenges and future directions in real-time embedded platforms

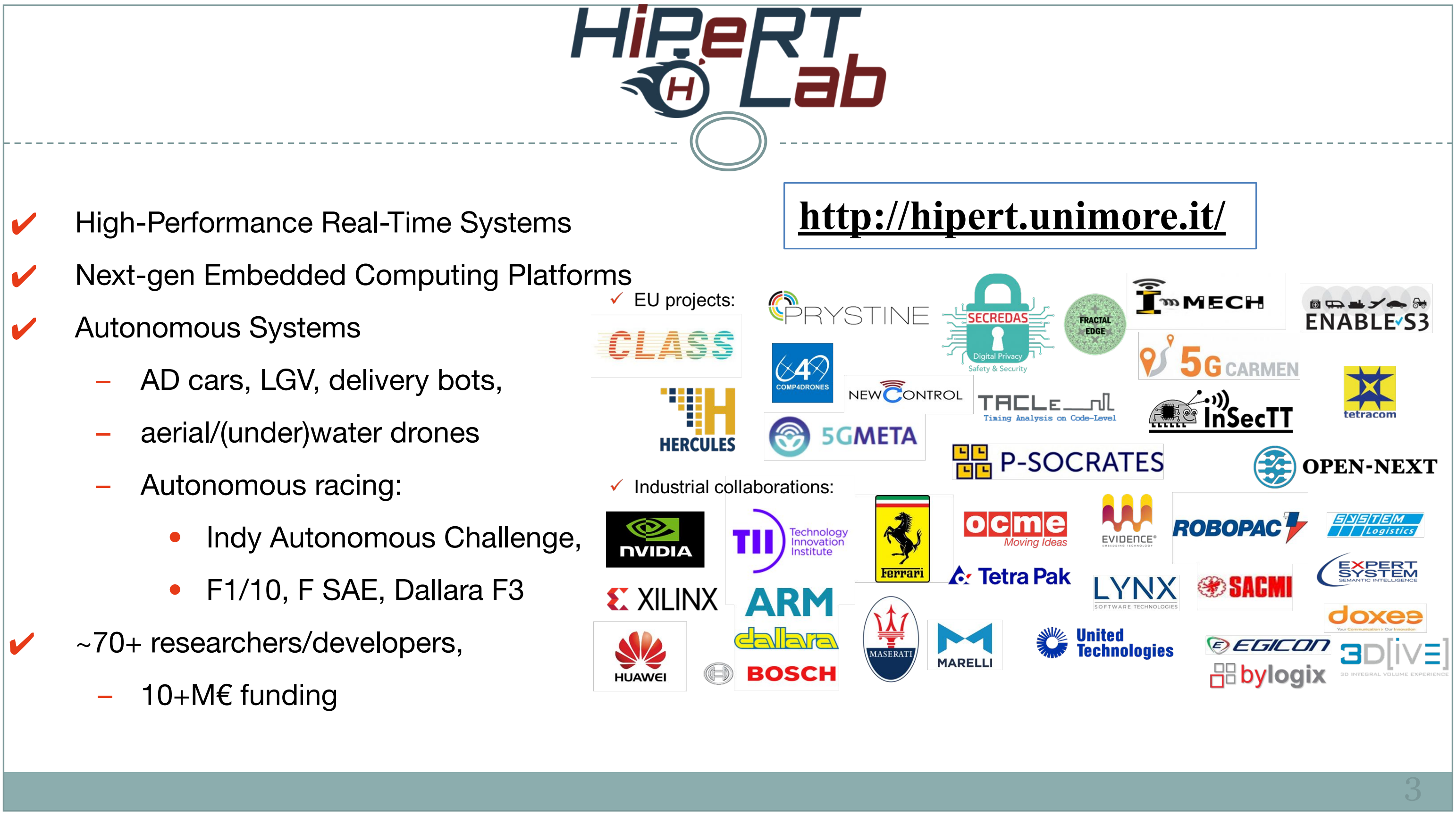
Nicola Capodieci
University of Modena and Reggio Emilia, Italy
Department of Physics, Informatics and Mathematics
High-Performance Real-Time Lab, HiPeRT, **hipert.unimore.it**
nicola.capodieci@unimore.it

CPS&IoT 2021



Outline

- Introduction
  - Who I am and what do we do at **HiPeRT** Lab
- What is a Real-Time system
- Heterogeneous embedded platforms
  - Challenges in GPU accelerated systems
  - Scheduling
  - Work submission
- Beyond the GPU
  - The HPC-DAG task model for next generation embedded platforms



HiPeRT Lab

- ✔ High-Performance Real-Time Systems
- ✔ Next-gen Embedded Computing Platforms
- ✔ Autonomous Systems
  - AD cars, LGV, delivery bots,
  - aerial/(under)water drones
  - Autonomous racing:
    - Indy Autonomous Challenge,
    - F1/10, F SAE, Dallara F3
- ✔ ~70+ researchers/developers,
  - 10+M€ funding

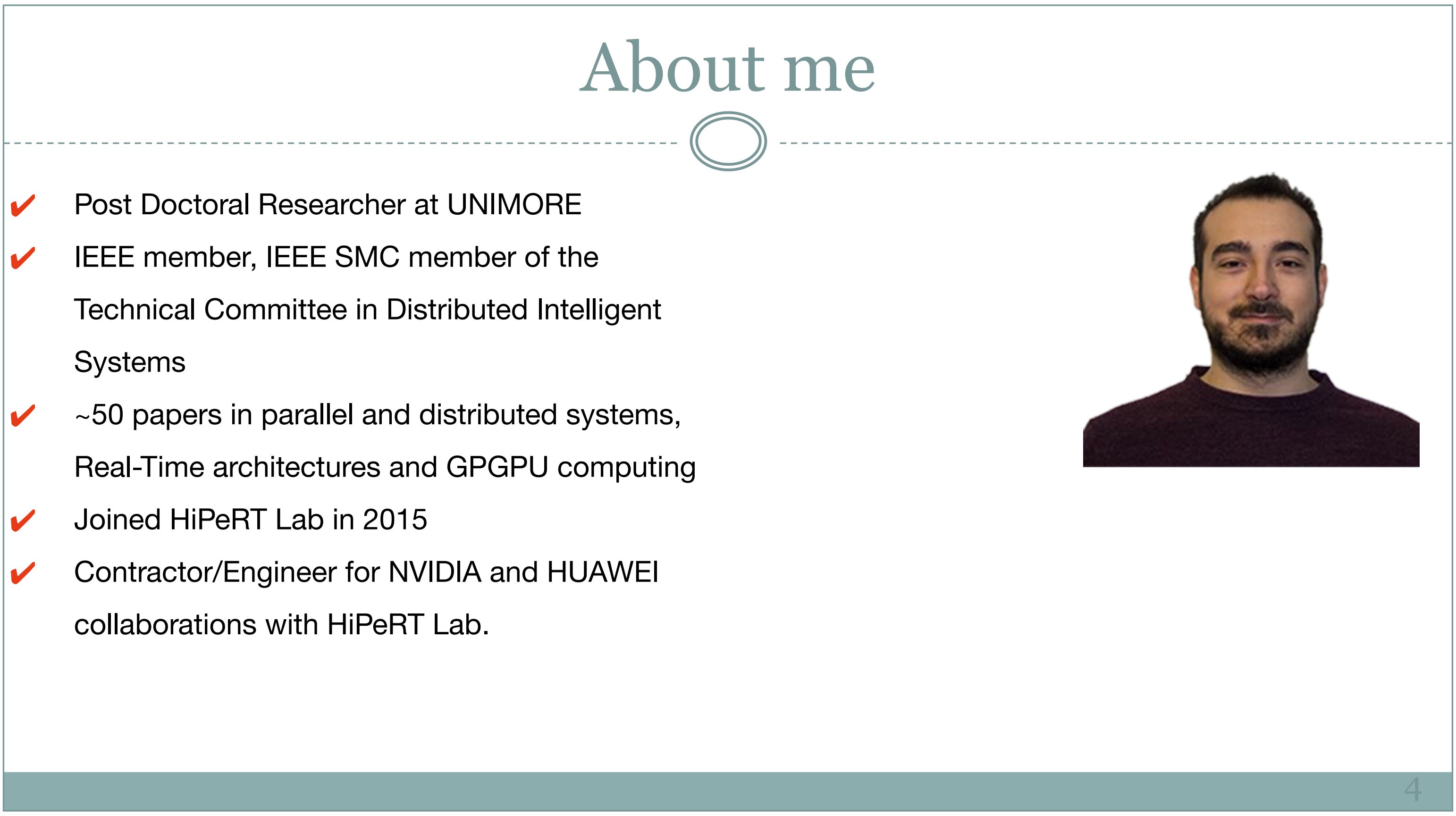
http://hipert.unimore.it/

✓ EU projects:

✓ Industrial collaborations:

CLASS
PRYSTINE
SECREDAS
FRACTAL EDGE
I-MECH
ENABLE-S3
COMP4DRONES
NEWCONTROL
TACLe
5G CARMEN
HERCULES
5GMETA
InSecTT
tetracom
P-SOCRATES
OPEN-NEXT
NVIDIA
Technology Innovation Institute
Ferrari
ocme
EVIDENCE
ROBOPAC
SYSTEM Logistics
XILINX
ARM
Tetra Pak
LYNX
SACMI
EXPERT SYSTEM
dallara
doxee
HUAWEI
BOSCH
MASERATI
MARELLI
United Technologies
EGICON
bylogix
3D[IVE]
3

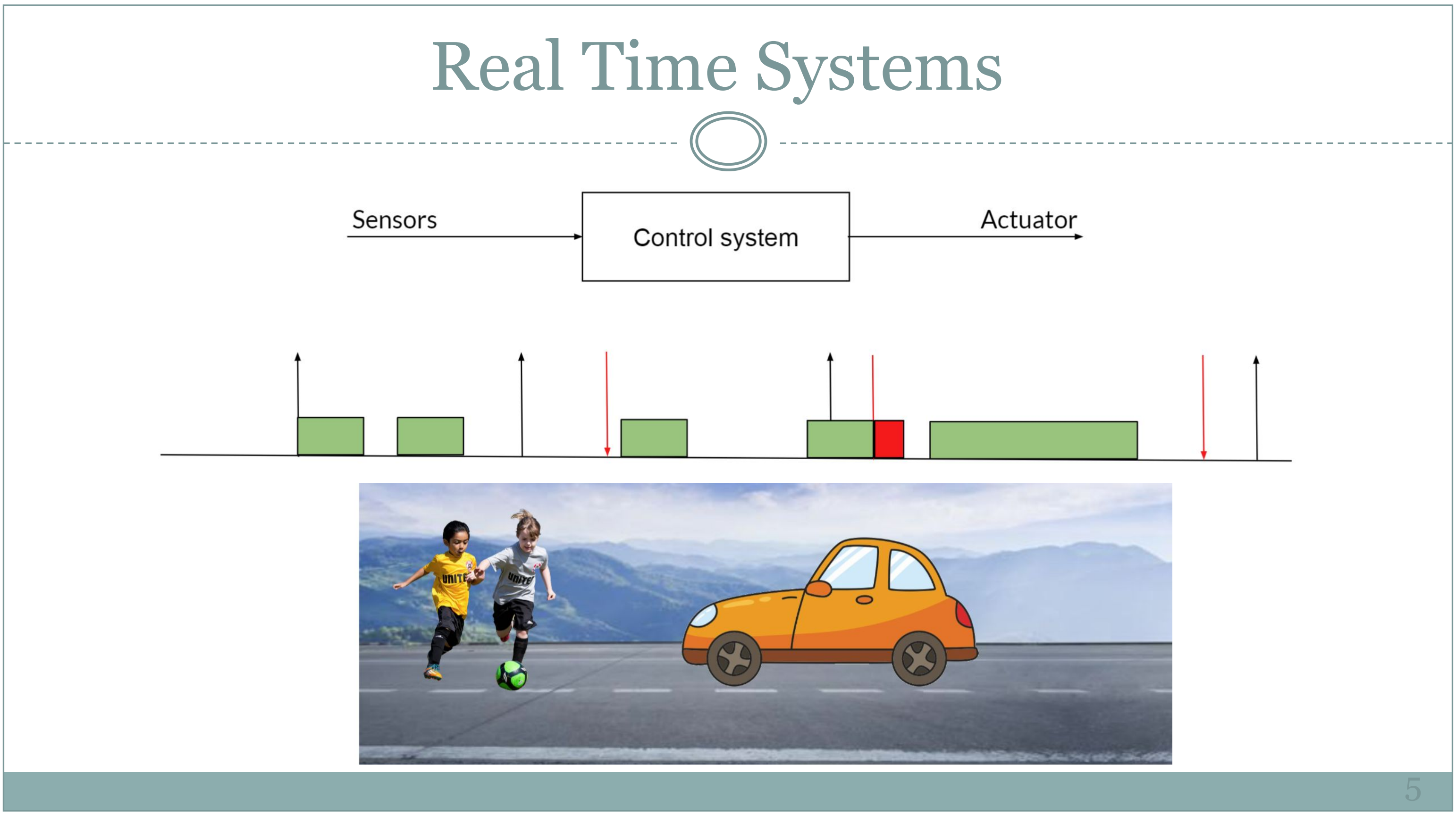
©MECO.net



About me

- ✔ Post Doctoral Researcher at UNIMORE
- ✔ IEEE member, IEEE SMC member of the Technical Committee in Distributed Intelligent Systems
- ✔ ~50 papers in parallel and distributed systems, Real-Time architectures and GPGPU computing
- ✔ Joined HiPeRT Lab in 2015
- ✔ Contractor/Engineer for NVIDIA and HUAWEI collaborations with HiPeRT Lab.

4



Real Time Systems

Sensors

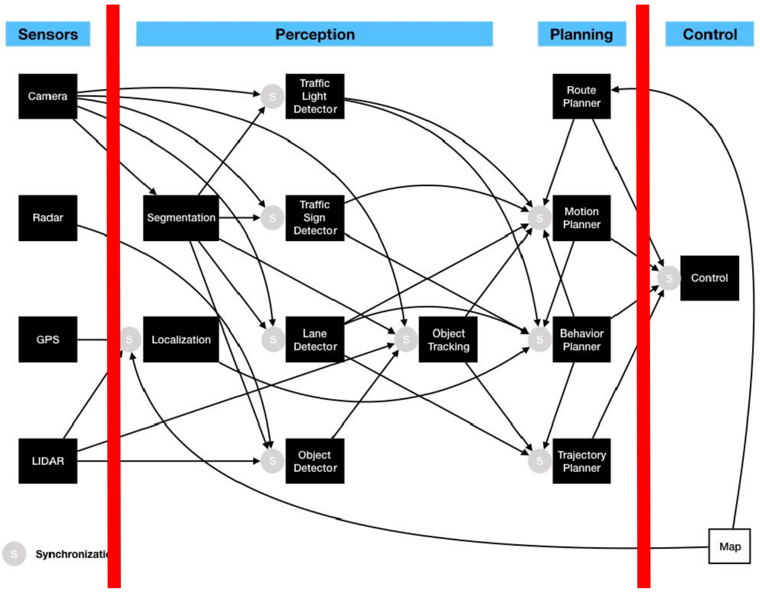
Control system

Actuator

5

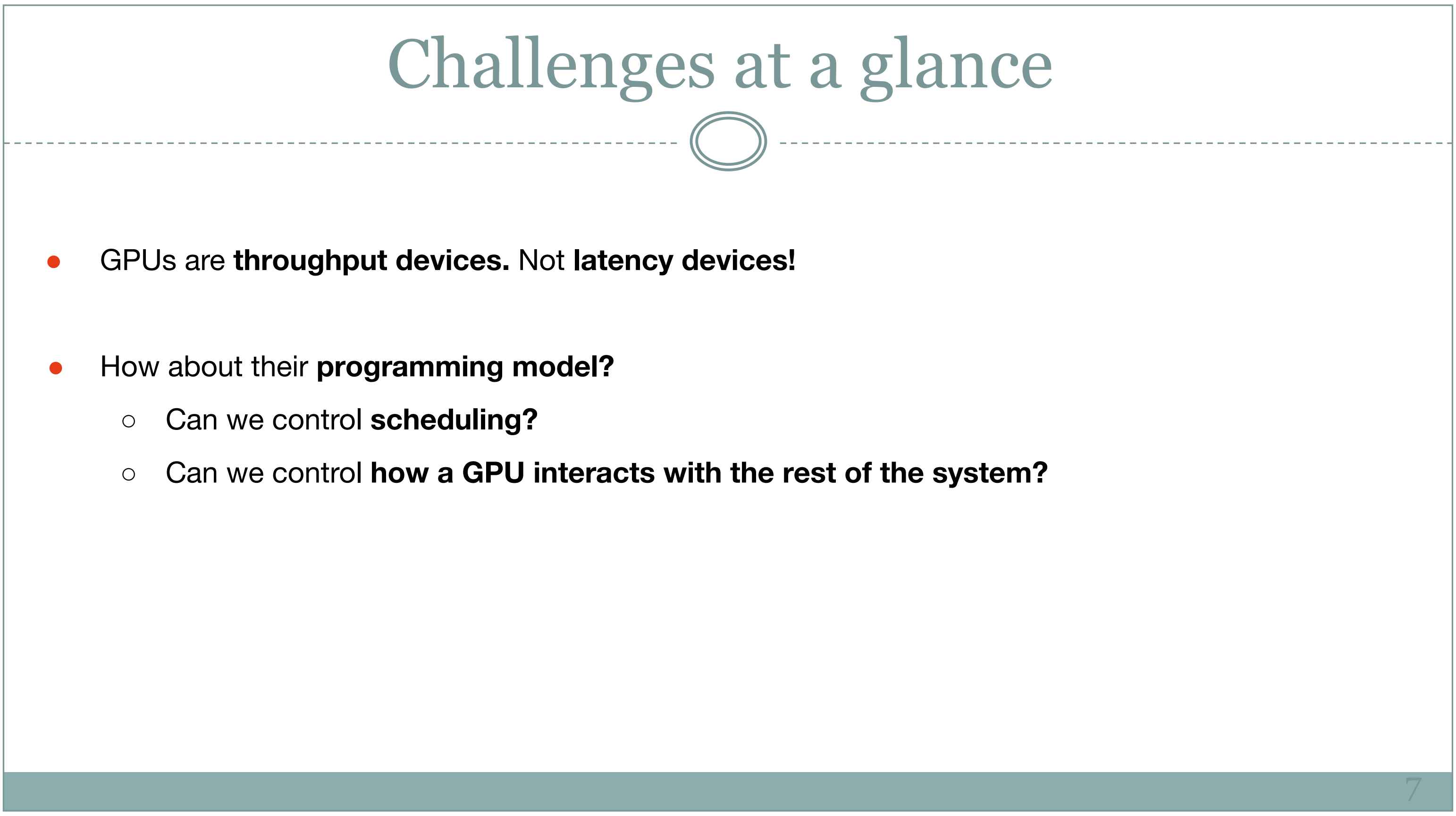
Real-Time in GPU in ADAS

- ✔ Modern ADAS applications integrate massively parallel workloads with strong safety requirements and latency-critical **Hard Real Time** tasks
- ✔ GPUs are massively parallel accelerators able to provide the necessary performance-per-watt for ADAS applications
- ✔ **...but how suitable are they for latency critical tasks?**



Sensors
Perception
Planning
Control
Camera
Radar
GPS
LIDAR
Segmentation
Localization
Traffic Light Detector
Traffic Sign Detector
Lane Detector
Object Tracking
Object Detector
Route Planner
Motion Planner
Behavior Planner
Trajectory Planner
Control
Map
S Synchronizati

6

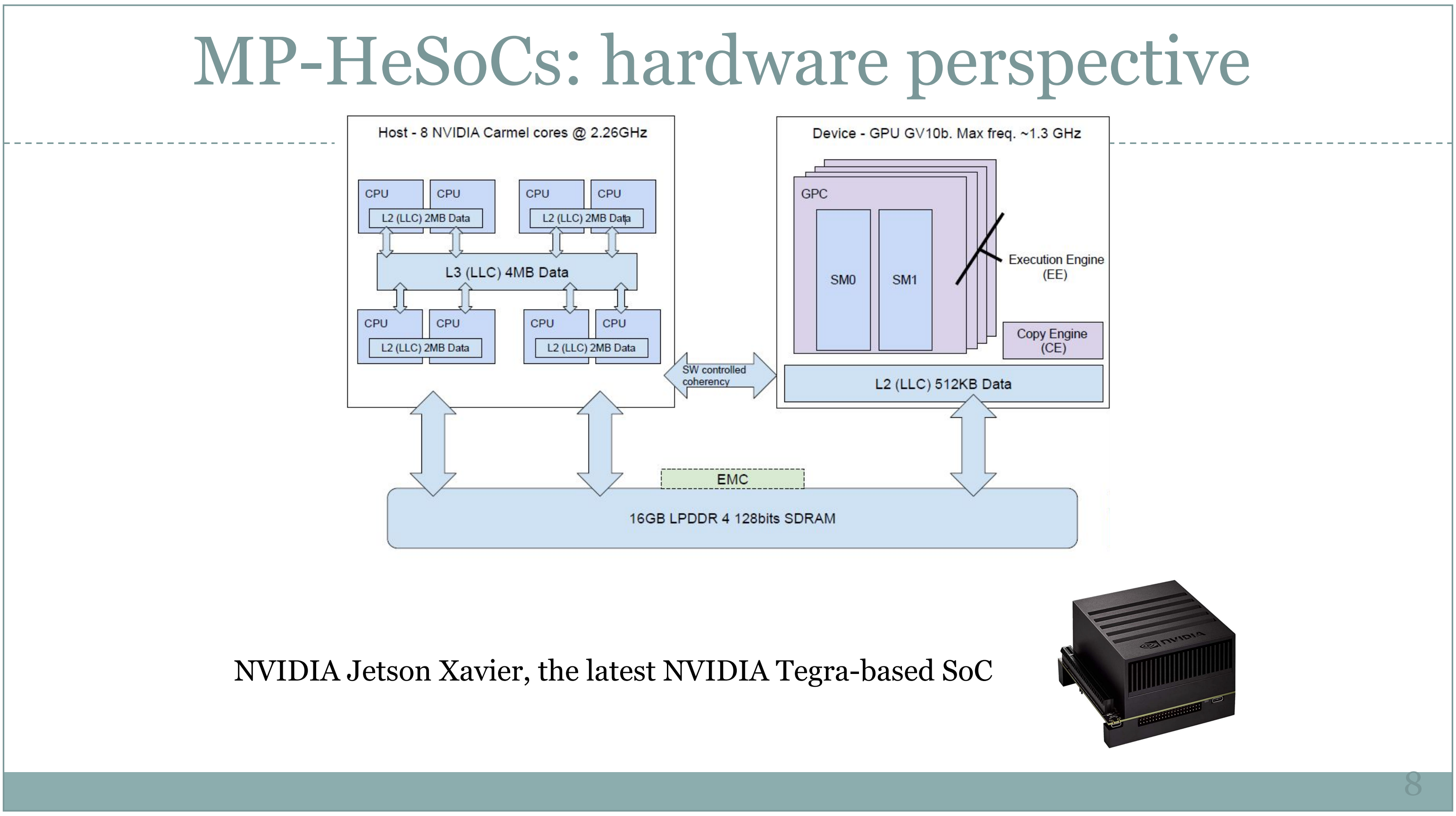


Challenges at a glance

- GPUs are **throughput devices.** Not **latency devices!**

- How about their **programming model?**
  - Can we control **scheduling?**
  - Can we control **how a GPU interacts with the rest of the system?**

7



MP-HeSoCs: hardware perspective

Host - 8 NVIDIA Carmel cores @ 2.26GHz

CPU CPU L2 (LLC) 2MB Data

CPU CPU L2 (LLC) 2MB Data

L3 (LLC) 4MB Data

CPU CPU L2 (LLC) 2MB Data

CPU CPU L2 (LLC) 2MB Data

SW controlled coherency

Device - GPU GV10b. Max freq. ~1.3 GHz

GPC

SM0

SM1

Execution Engine (EE)

Copy Engine (CE)

L2 (LLC) 512KB Data

EMC

16GB LPDDR 4 128bits SDRAM

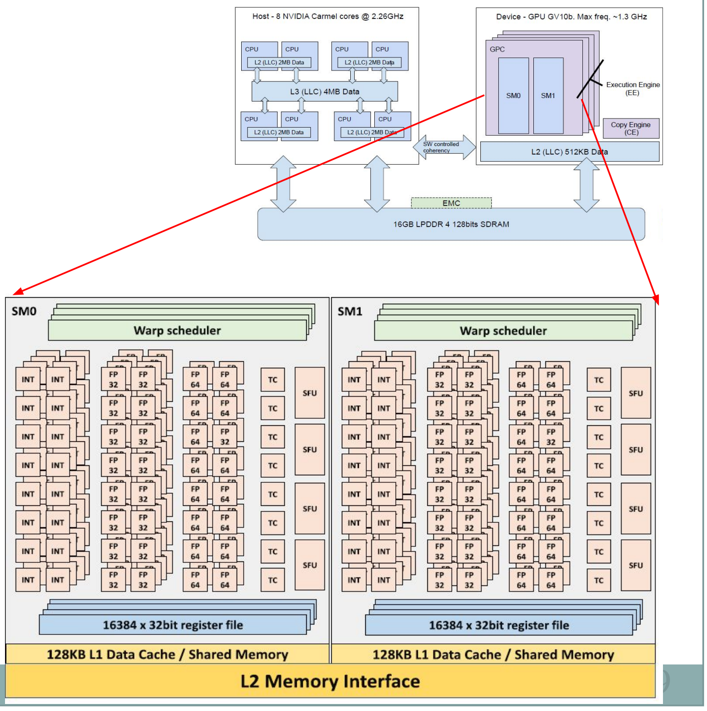
NVIDIA Jetson Xavier, the latest NVIDIA Tegra-based SoC

8

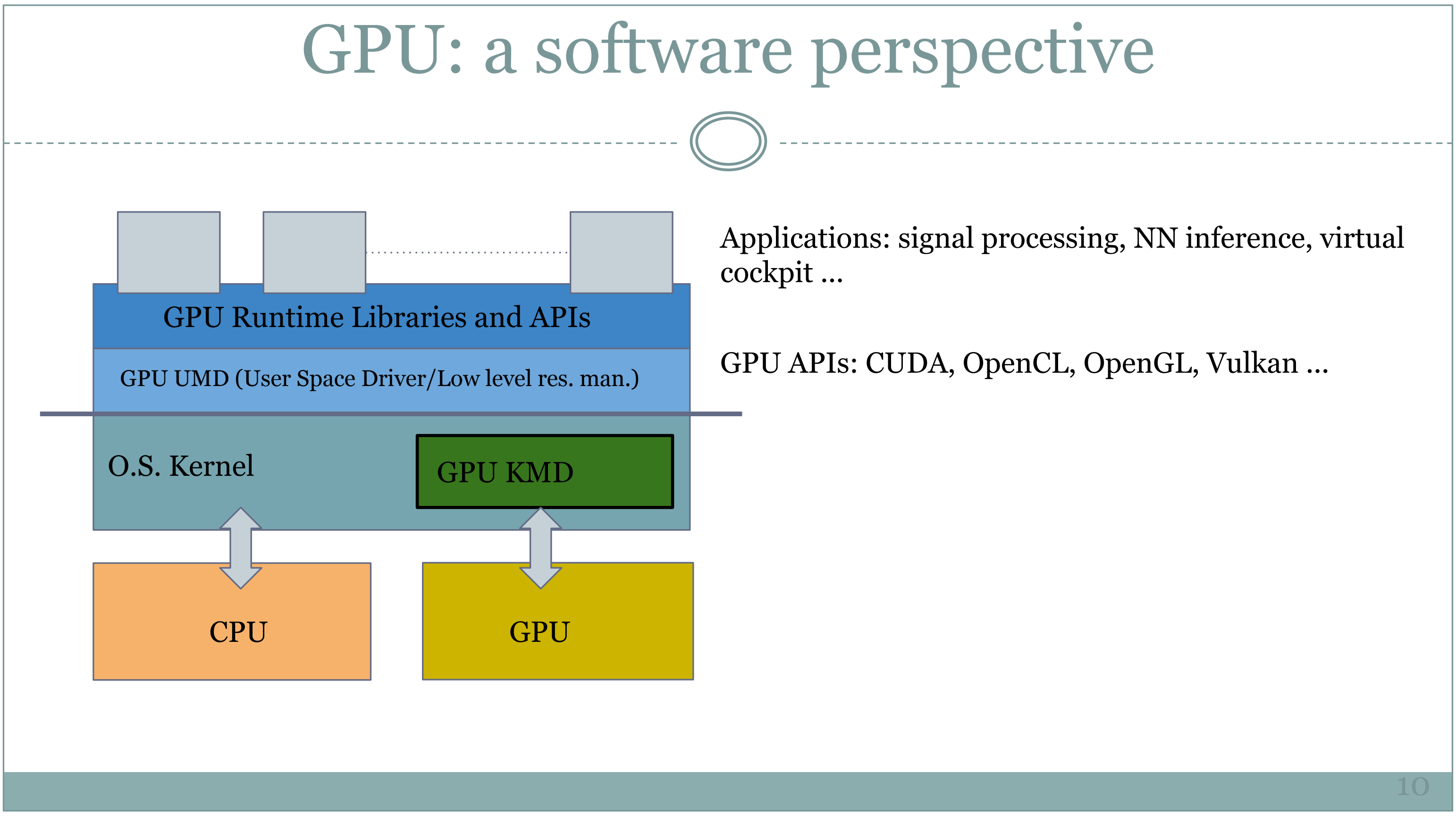
©MECO.net

The NVIDA tegra iGPU

- Xavier – Volta microarchitecture
  - Copy engine
- Execution Engine
  - 8 Streaming multiprocessors (SMs)
  - 64 CUDA cores per SM
  - 4 warp schedulers
- SMs are grouped into graphic processing clusters (GPCs)



©MECO.net



GPU: a software perspective

GPU Runtime Libraries and APIs

GPU UMD (User Space Driver/Low level res. man.)

O.S. Kernel

GPU KMD

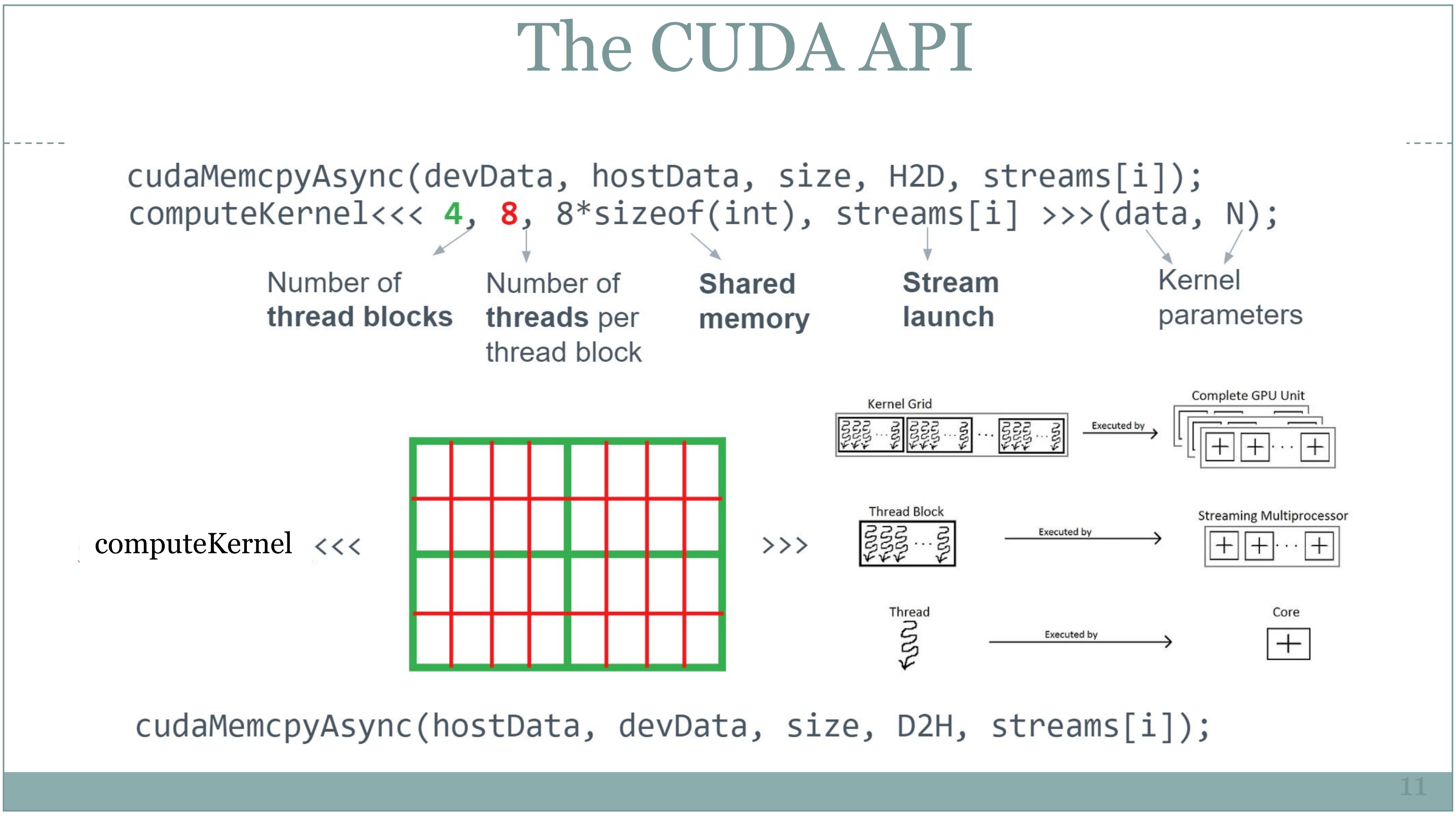
CPU

GPU

Applications: signal processing, NN inference, virtual cockpit ...

GPU APIs: CUDA, OpenCL, OpenGL, Vulkan ...

10



The CUDA API

```
cudaMemcpyAsync(devData, hostData, size, H2D, streams[i]);
computeKernel<<< 4, 8, 8*sizeof(int), streams[i] >>>(data, N);
```

Number of **thread blocks**

Number of **threads** per thread block

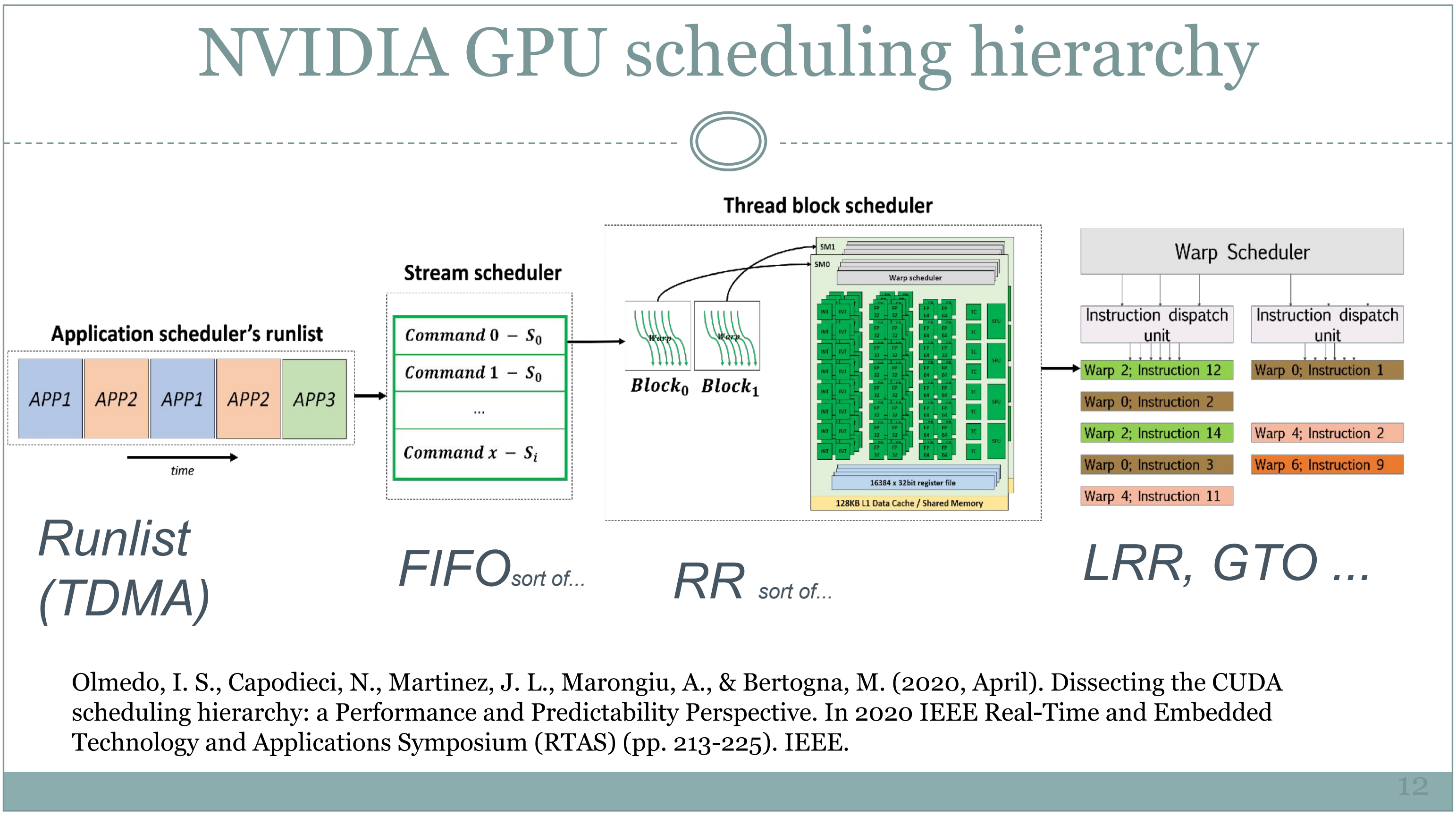
Shared memory

Stream launch

Kernel parameters

computeKernel <<< >>>

```
cudaMemcpyAsync(hostData, devData, size, D2H, streams[i]);
```



NVIDIA GPU scheduling hierarchy

Application scheduler's runlist

APP1 | APP2 | APP1 | APP2 | APP3

time

Stream scheduler

$Command\ 0 - S_0$

$Command\ 1 - S_0$

...

$Command\ x - S_i$

Thread block scheduler

$Block_0$ $Block_1$

Warp

SM1

SM0

Warp scheduler

16384 x 32bit register file

128KB L1 Data Cache / Shared Memory

Warp Scheduler

Instruction dispatch unit

Instruction dispatch unit

Warp 2; Instruction 12

Warp 0; Instruction 2

Warp 2; Instruction 14

Warp 0; Instruction 3

Warp 4; Instruction 11

Warp 0; Instruction 1

Warp 4; Instruction 2

Warp 6; Instruction 9

Runlist (TDMA)

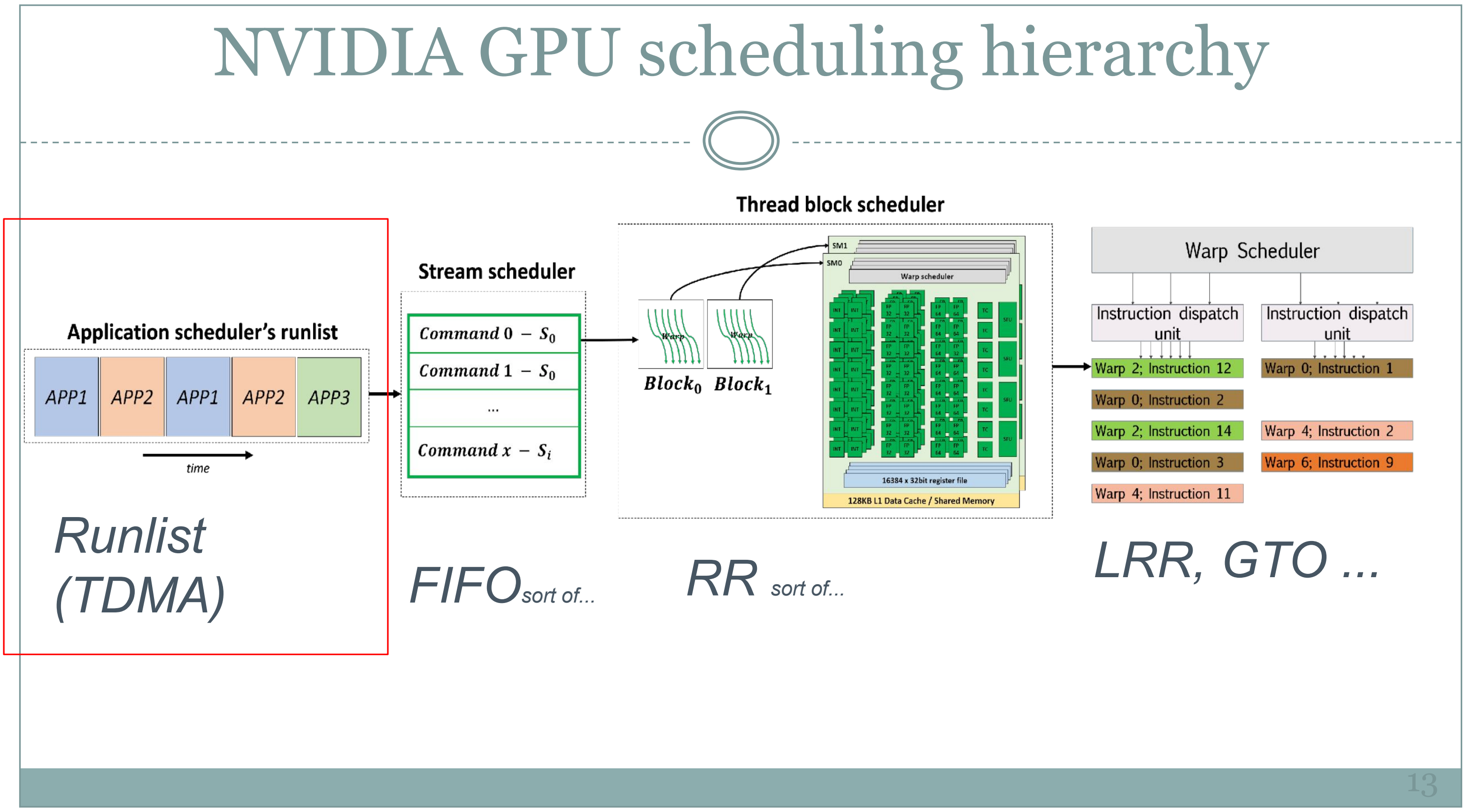
FIFO sort of...

RR sort of...

LRR, GTO ...

Olmedo, I. S., Capodieci, N., Martinez, J. L., Marongiu, A., & Bertogna, M. (2020, April). Dissecting the CUDA scheduling hierarchy: a Performance and Predictability Perspective. In 2020 IEEE Real-Time and Embedded Technology and Applications Symposium (RTAS) (pp. 213-225). IEEE.

12



NVIDIA GPU scheduling hierarchy

Application scheduler's runlist

APP1 APP2 APP1 APP2 APP3

time

Runlist (TDMA)

Stream scheduler

Command 0 – S_0

Command 1 – S_0

...

Command x – S_i

FIFO sort of...

Thread block scheduler

$Block_0$ $Block_1$

Warp
Warp
SM1
SM0
Warp scheduler
16384 x 32bit register file
128KB L1 Data Cache / Shared Memory

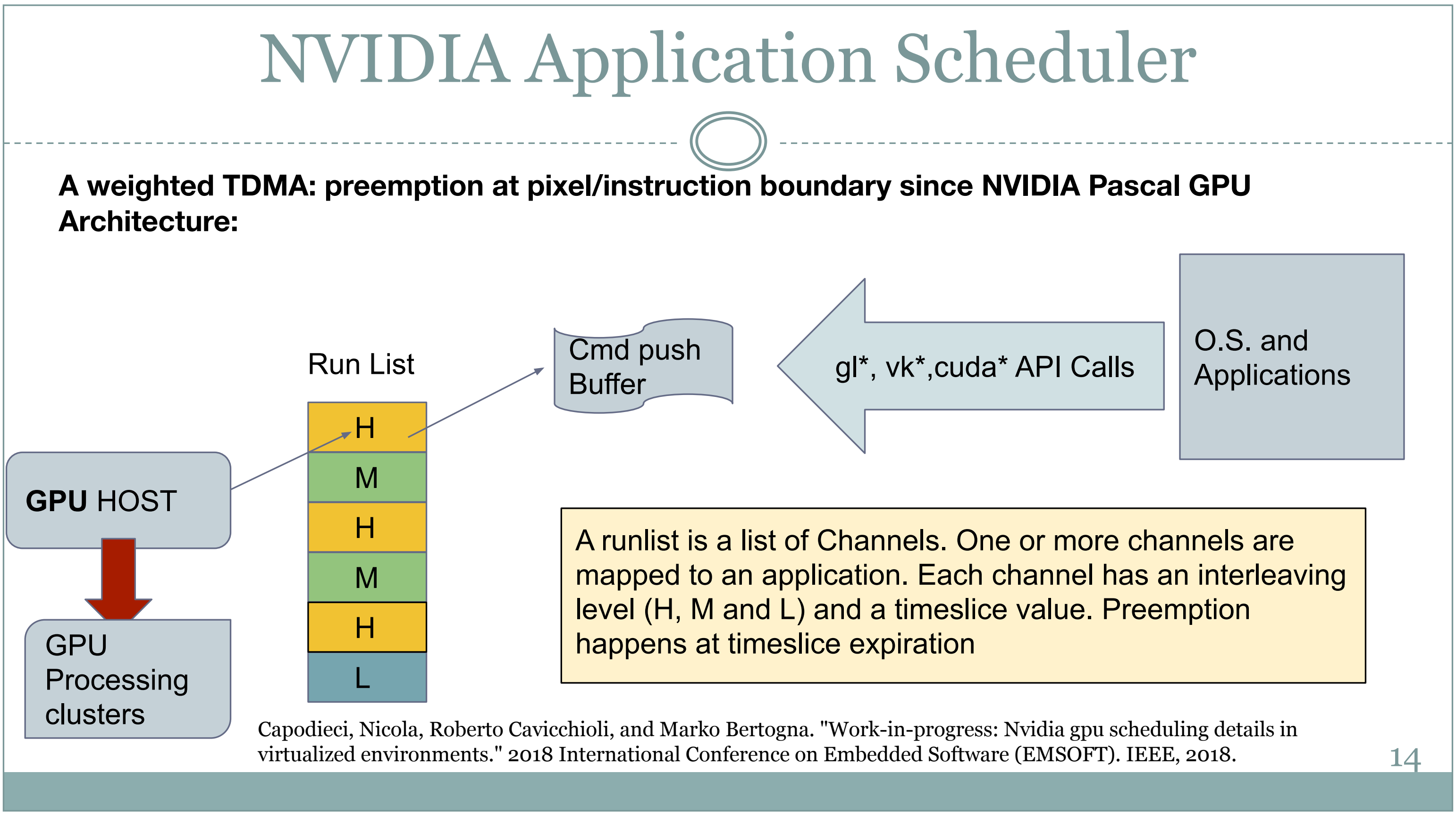
RR sort of...

Warp Scheduler

Instruction dispatch unit	Instruction dispatch unit
Warp 2; Instruction 12	Warp 0; Instruction 1
Warp 0; Instruction 2	
Warp 2; Instruction 14	Warp 4; Instruction 2
Warp 0; Instruction 3	Warp 6; Instruction 9
Warp 4; Instruction 11	

LRR, GTO ...

13



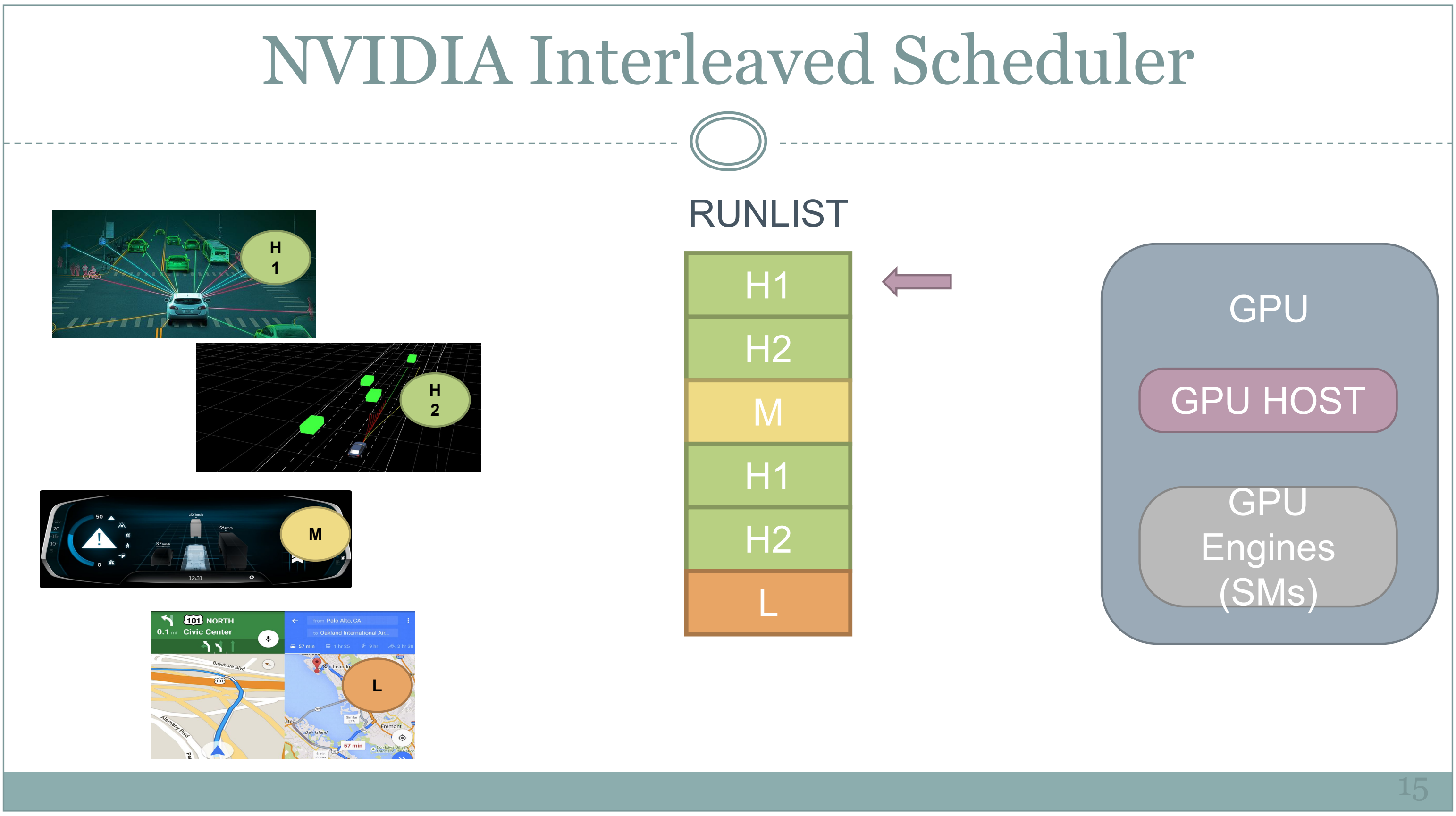
NVIDIA Application Scheduler

A weighted TDMA: preemption at pixel/instruction boundary since NVIDIA Pascal GPU Architecture:

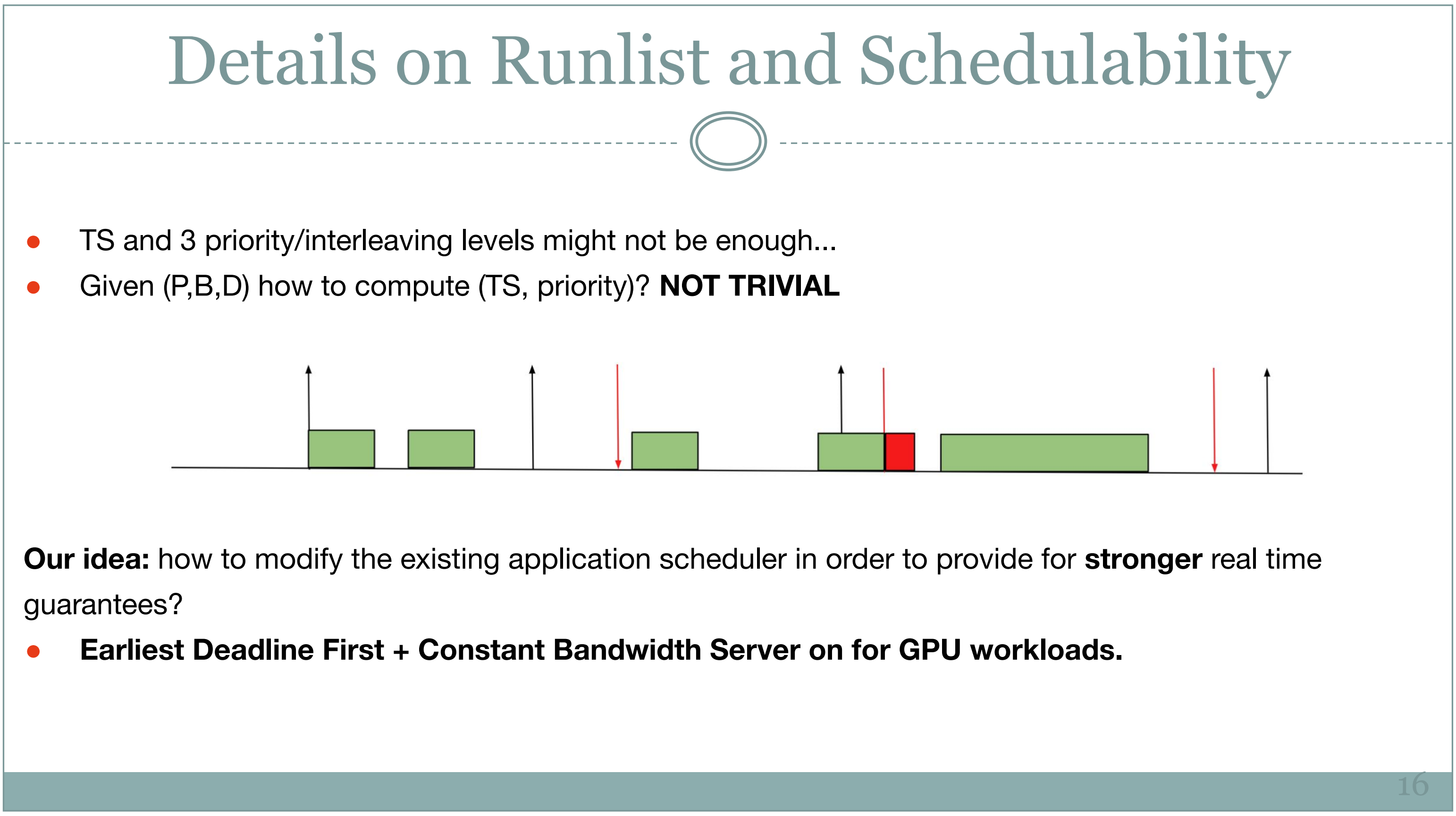
A runlist is a list of Channels. One or more channels are mapped to an application. Each channel has an interleaving level (H, M and L) and a timeslice value. Preemption happens at timeslice expiration

Capodieci, Nicola, Roberto Cavicchioli, and Marko Bertogna. "Work-in-progress: Nvidia gpu scheduling details in virtualized environments." 2018 International Conference on Embedded Software (EMSOFT). IEEE, 2018.

14



NVIDIA Interleaved Scheduler

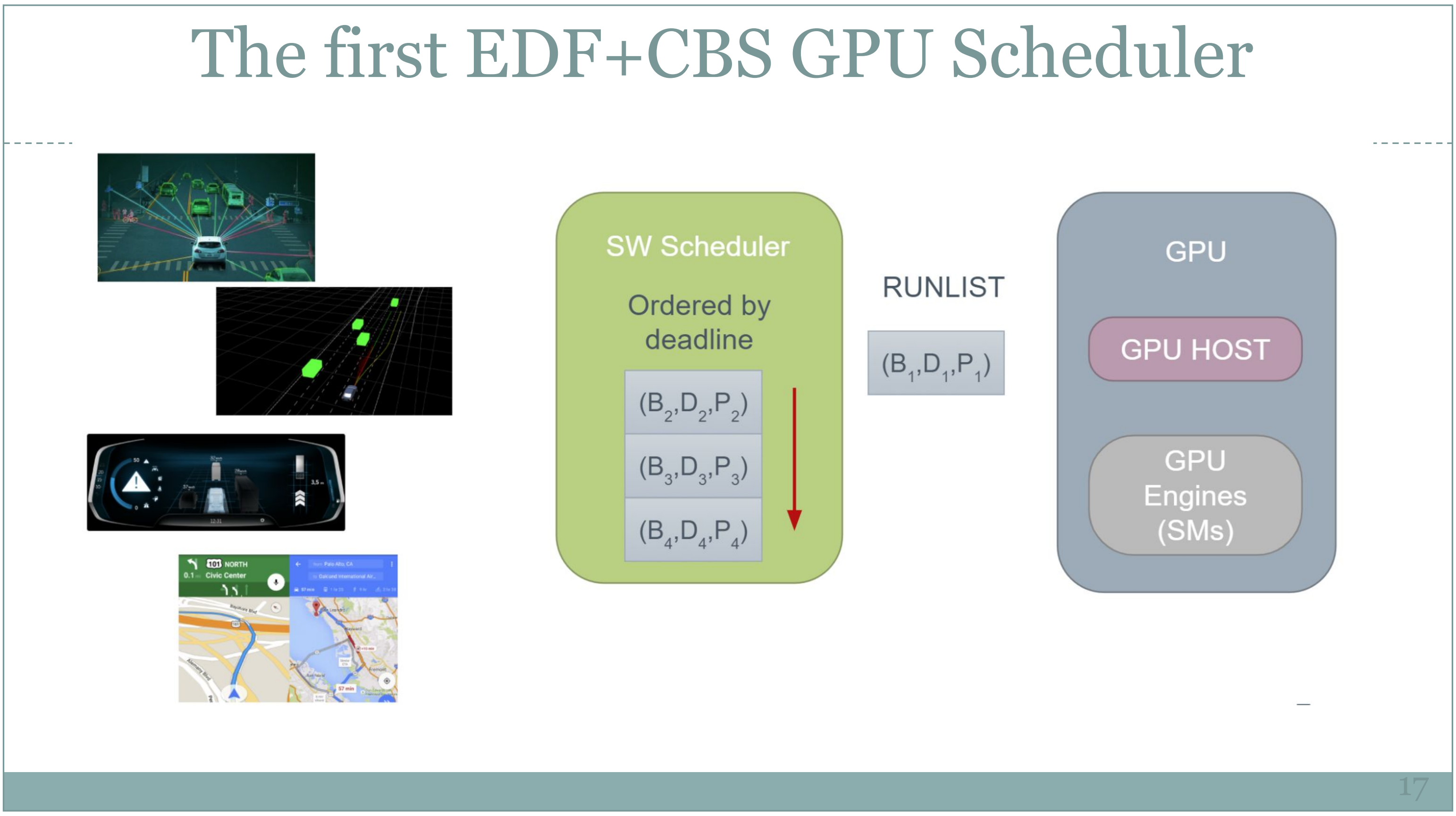


Details on Runlist and Schedulability

- TS and 3 priority/interleaving levels might not be enough...
- Given (P,B,D) how to compute (TS, priority)? **NOT TRIVIAL**

Our idea: how to modify the existing application scheduler in order to provide for **stronger** real time guarantees?

- **Earliest Deadline First + Constant Bandwidth Server on for GPU workloads.**



The first EDF+CBS GPU Scheduler

SW Scheduler

Ordered by deadline

(B_2,D_2,P_2)

(B_3,D_3,P_3)

(B_4,D_4,P_4)

RUNLIST

(B_1,D_1,P_1)

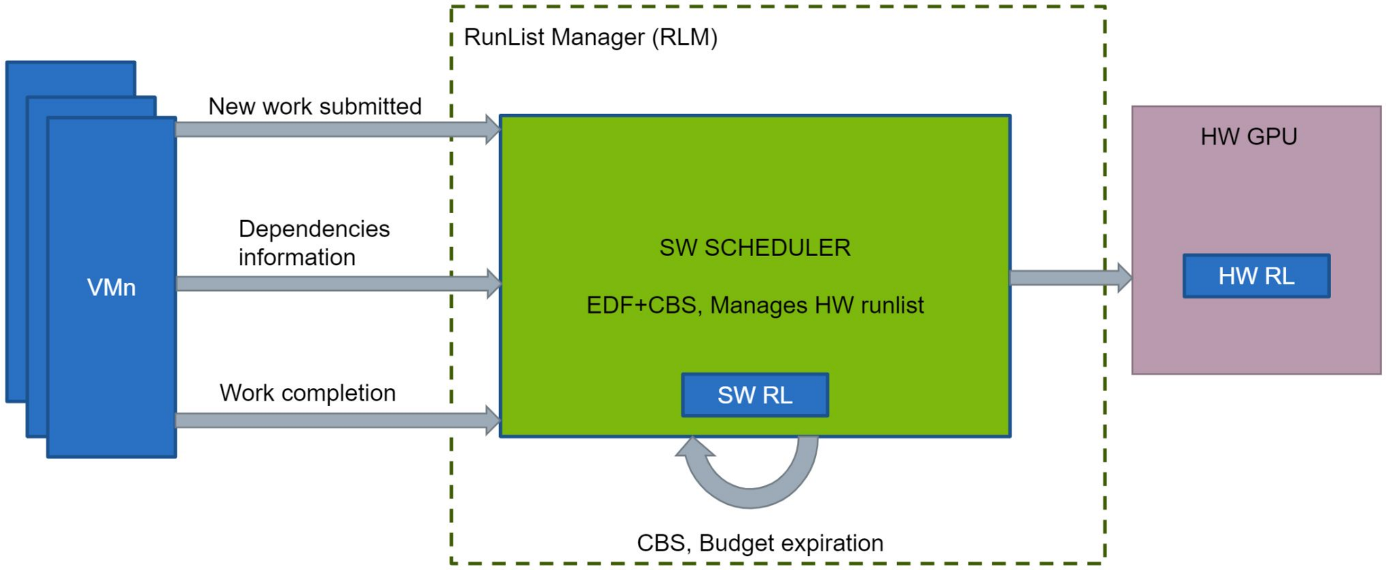
GPU

GPU HOST

GPU Engines (SMs)

17

Scheduler Prototype Design



RunList Manager (RLM)

New work submitted

Dependencies information

Work completion

VMn

SW SCHEDULER

EDF+CBS, Manages HW runlist

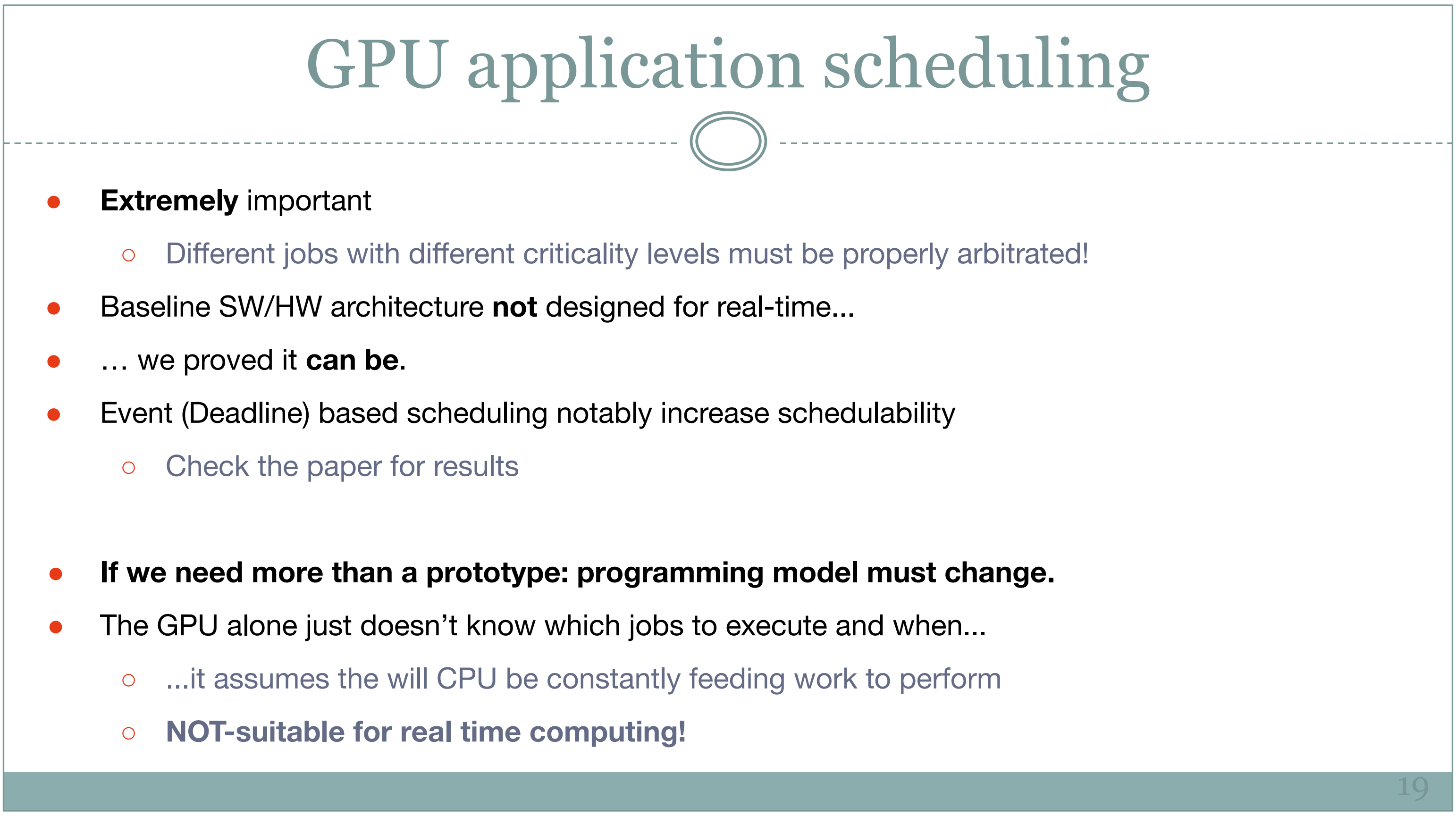
SW RL

CBS, Budget expiration

HW GPU

HW RL

Capodieci, N., Cavicchioli, R., Bertogna, M., & Paramakuru, A. (2018, December). Deadline-based scheduling for gpu with preemption support. In *2018 IEEE Real-Time Systems Symposium (RTSS)* (pp. 119-130). IEEE.

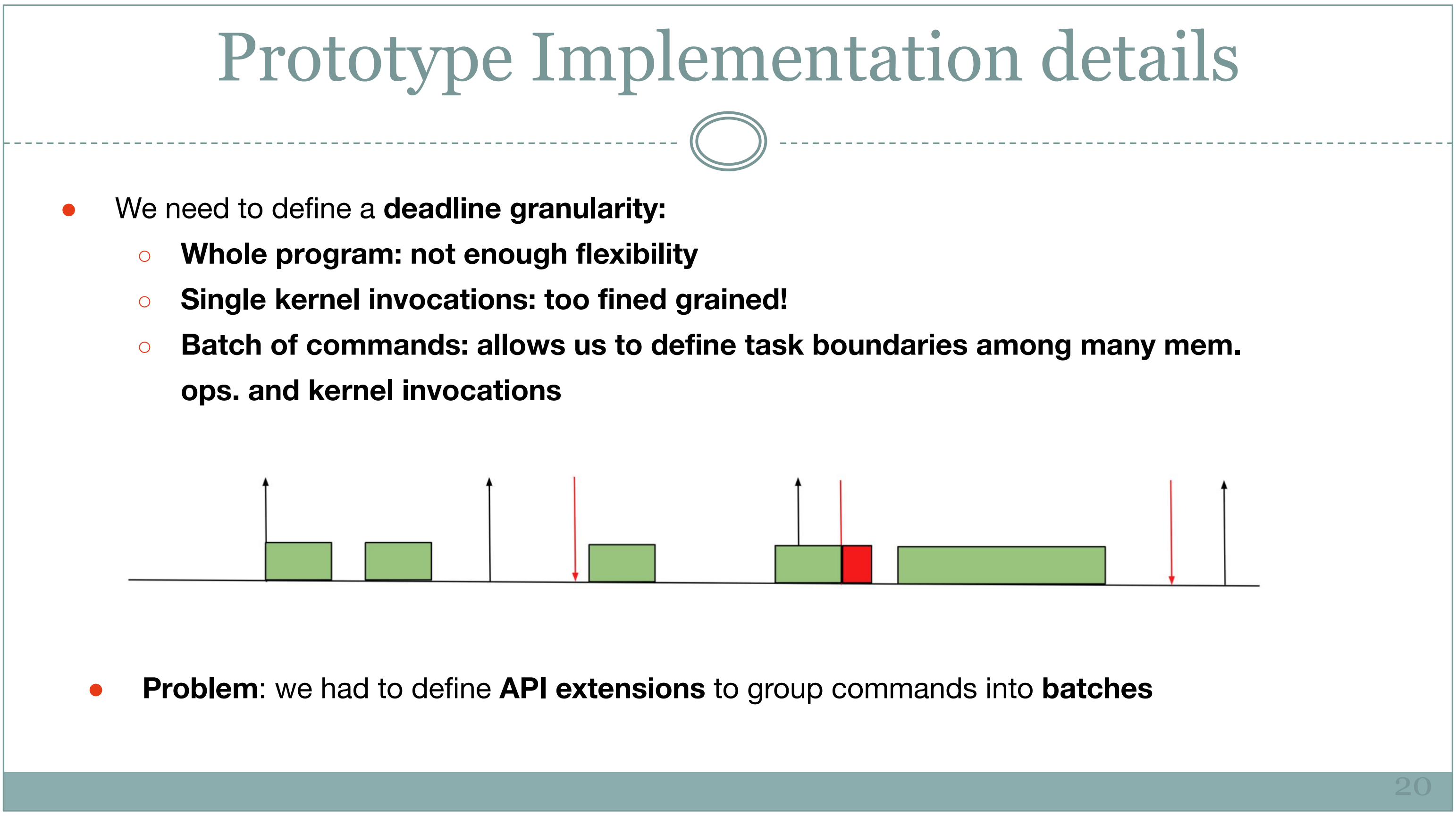


GPU application scheduling

- **Extremely** important
  - ○ Different jobs with different criticality levels must be properly arbitrated!
- Baseline SW/HW architecture **not** designed for real-time...
- … we proved it **can be**.
- Event (Deadline) based scheduling notably increase schedulability
  - ○ Check the paper for results

- **If we need more than a prototype: programming model must change.**
- The GPU alone just doesn't know which jobs to execute and when...
  - ○ ...it assumes the will CPU be constantly feeding work to perform
  - ○ **NOT-suitable for real time computing!**

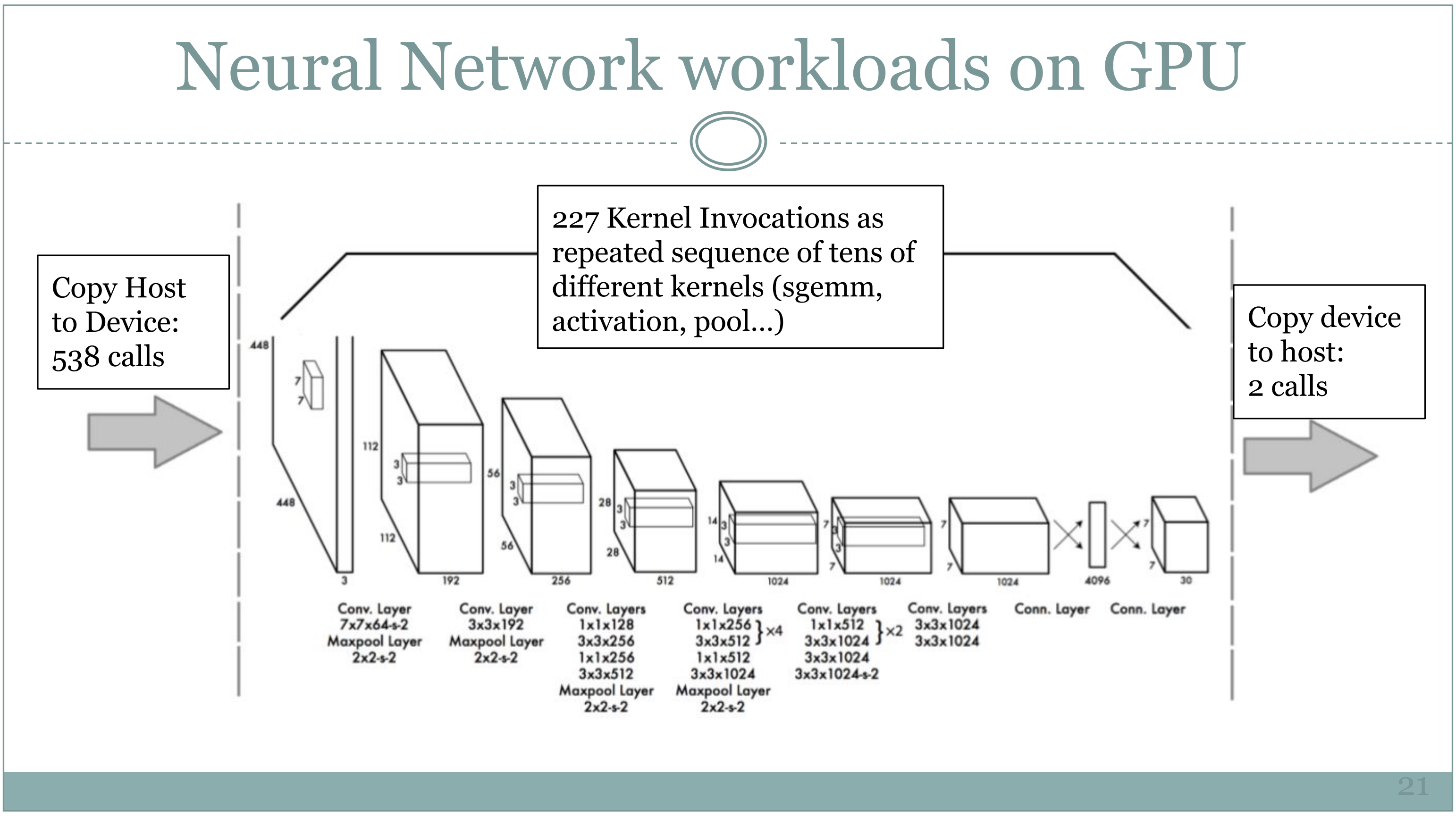
19



Prototype Implementation details

- We need to define a **deadline granularity:**
  - **Whole program: not enough flexibility**
  - **Single kernel invocations: too fined grained!**
  - **Batch of commands: allows us to define task boundaries among many mem. ops. and kernel invocations**

- **Problem**: we had to define **API extensions** to group commands into **batches**



Neural Network workloads on GPU

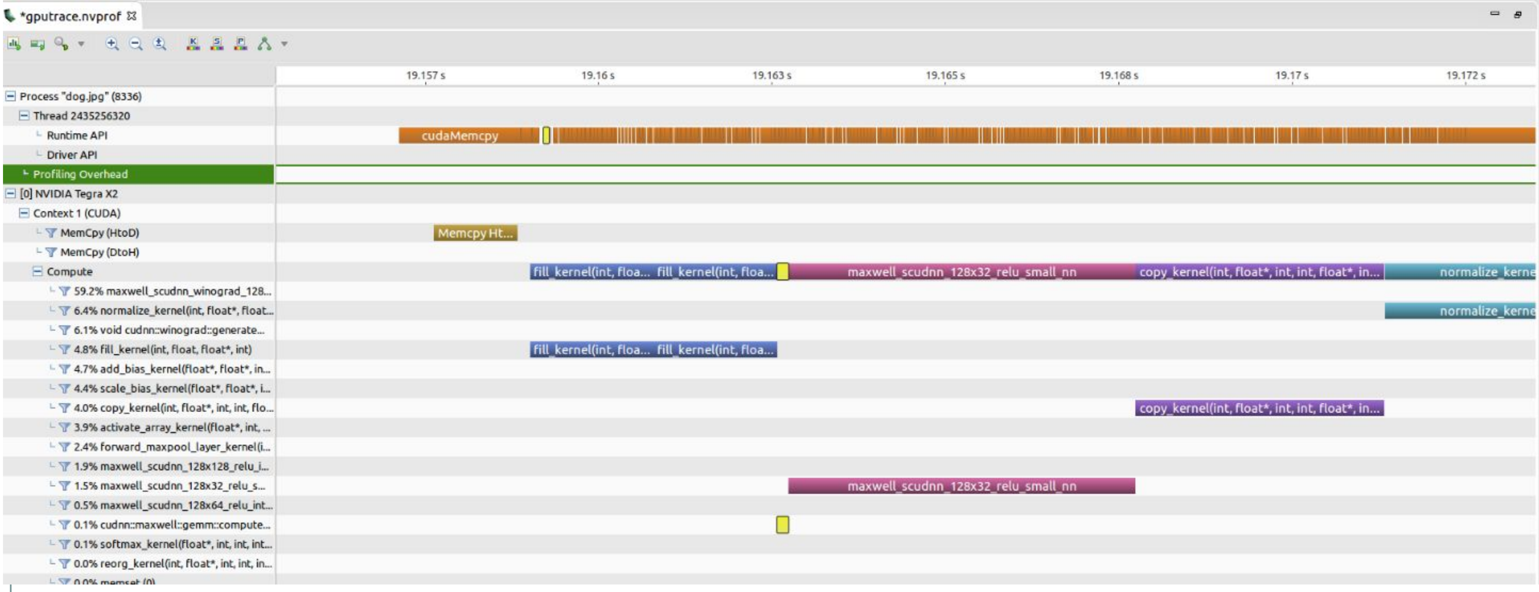
Copy Host to Device: 538 calls

227 Kernel Invocations as repeated sequence of tens of different kernels (sgemm, activation, pool…)

Copy device to host: 2 calls

21

Nvprof trace (YOLOv3)

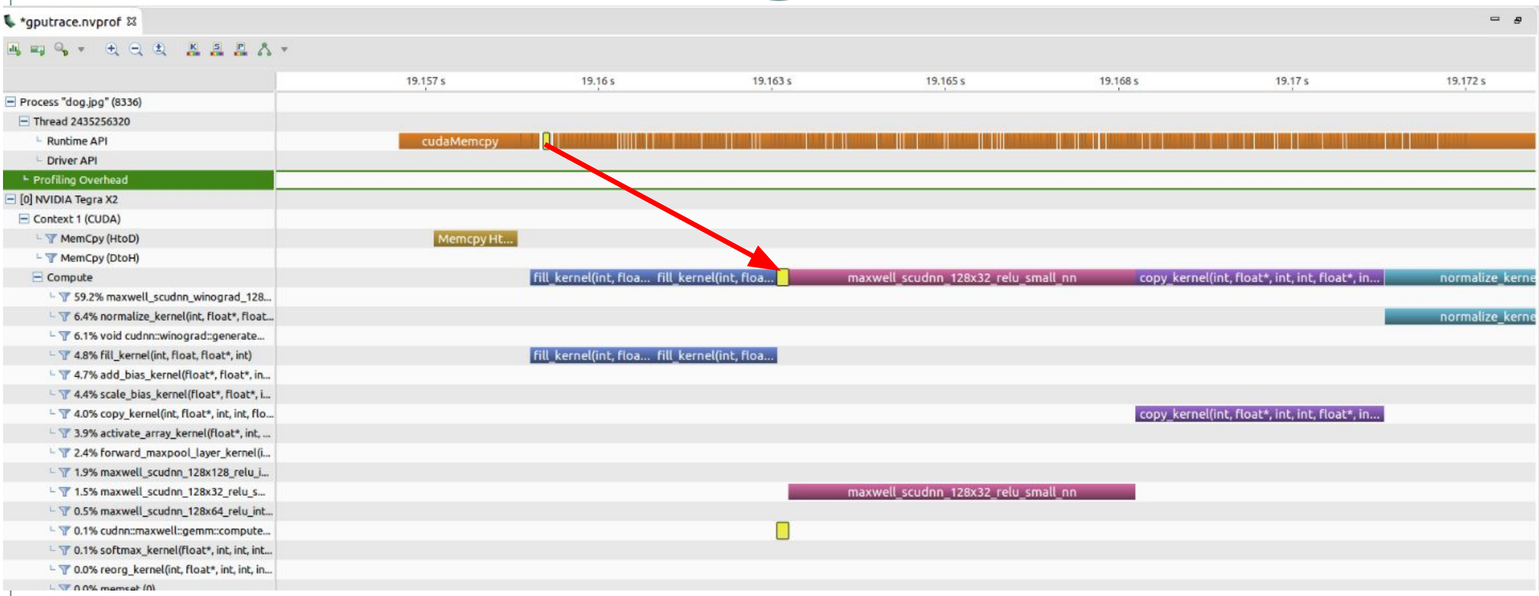


*gputrace.nvprof

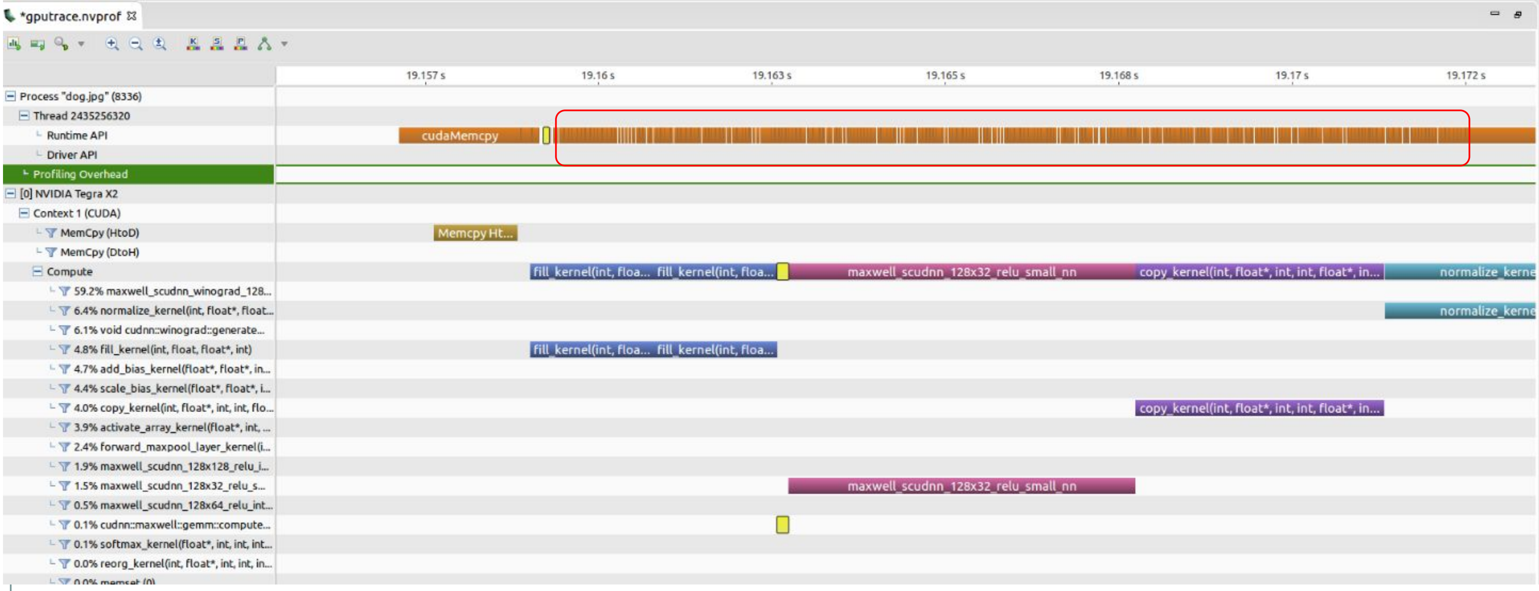
```
Process "dog.jpg" (8336)
  Thread 2435256320
    Runtime API
    Driver API
  Profiling Overhead
[0] NVIDIA Tegra X2
  Context 1 (CUDA)
    MemCpy (HtoD)
    MemCpy (DtoH)
    Compute
      59.2% maxwell_scudnn_winograd_128...
      6.4% normalize_kernel(int, float*, float...
      6.1% void cudnn::winograd::generate...
      4.8% fill_kernel(int, float, float*, int)
      4.7% add_bias_kernel(float*, float*, in...
      4.4% scale_bias_kernel(float*, float*, i...
      4.0% copy_kernel(int, float*, int, int, flo...
      3.9% activate_array_kernel(float*, int, ...
      2.4% forward_maxpool_layer_kernel(i...
      1.9% maxwell_scudnn_128x128_relu_i...
      1.5% maxwell_scudnn_128x32_relu_s...
      0.5% maxwell_scudnn_128x64_relu_int...
      0.1% cudnn::maxwell::gemm::compute...
      0.1% softmax_kernel(float*, int, int, int...
      0.0% reorg_kernel(int, float*, int, int, in...
      0.0% memset (0)
```

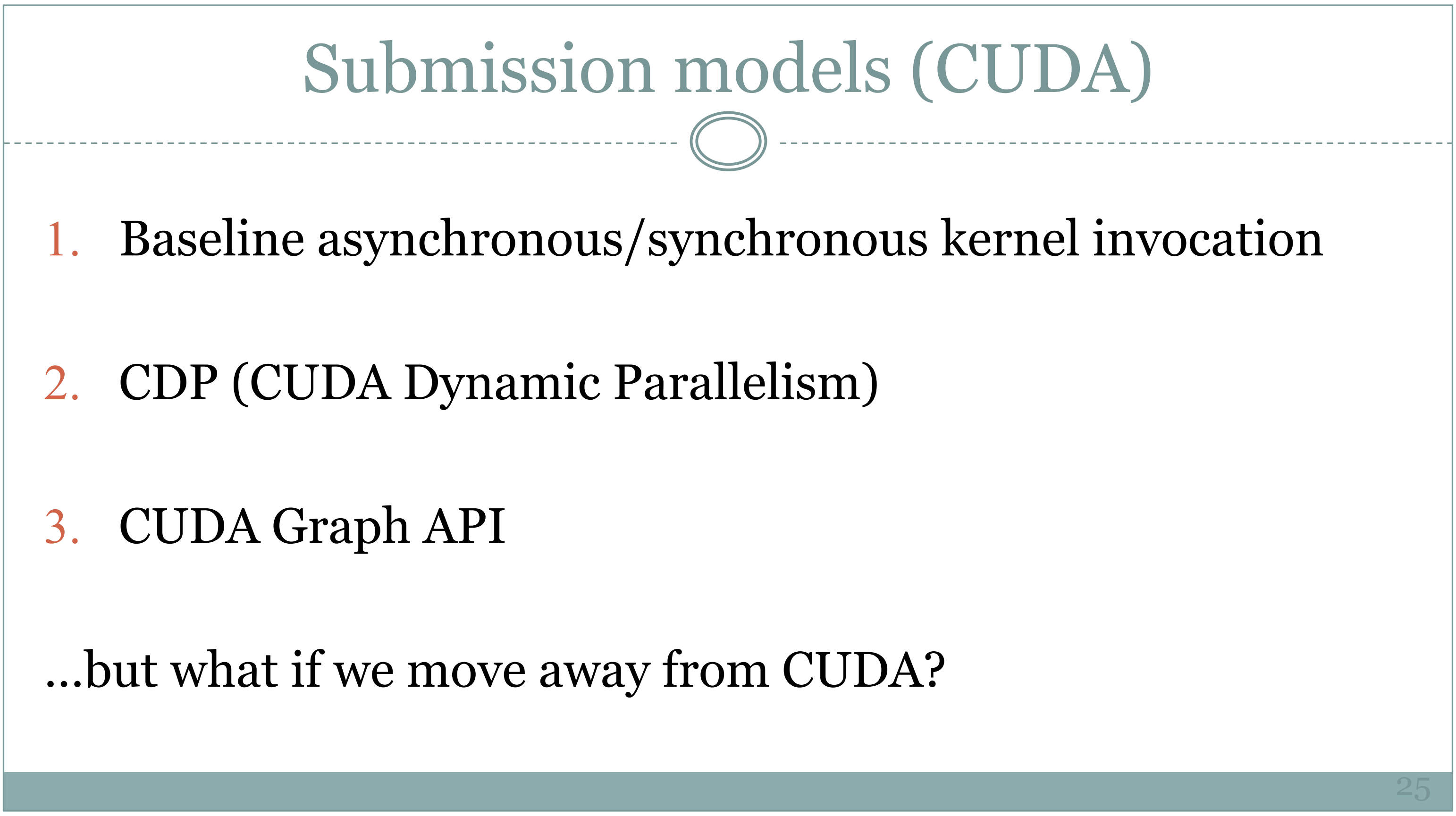
©MECO.net

Nvprof trace (CPU submits to GPU)


*gputrace.nvprof
19.157 s
19.16 s
19.163 s
19.165 s
19.168 s
19.17 s
19.172 s
Process "dog.jpg" (8336)
Thread 2435256320
Runtime API
Driver API
Profiling Overhead
[0] NVIDIA Tegra X2
Context 1 (CUDA)
MemCpy (HtoD)
MemCpy (DtoH)
Compute
59.2% maxwell_scudnn_winograd_128...
6.4% normalize_kernel(int, float*, float...
6.1% void cudnn::winograd::generate...
4.8% fill_kernel(int, float, float*, int)
4.7% add_bias_kernel(float*, float*, in...
4.4% scale_bias_kernel(float*, float*, i...
4.0% copy_kernel(int, float*, int, int, flo...
3.9% activate_array_kernel(float*, int, ...
2.4% forward_maxpool_layer_kernel(i...
1.9% maxwell_scudnn_128x128_relu_i...
1.5% maxwell_scudnn_128x32_relu_s...
0.5% maxwell_scudnn_128x64_relu_int...
0.1% cudnn::maxwell::gemm::compute...
0.1% softmax_kernel(float*, int, int, int...
0.0% reorg_kernel(int, float*, int, int, in...
0.0% memset (0)
cudaMemcpy
Memcpy Ht...
fill_kernel(int, floa...
fill_kernel(int, floa...
maxwell_scudnn_128x32_relu_small_nn
copy_kernel(int, float*, int, int, float*, in...
normalize_kerne

Nvprof trace (Busy CPU with lots of submissions)


*gputrace.nvprof
19.157 s
19.16 s
19.163 s
19.165 s
19.168 s
19.17 s
19.172 s
Process "dog.jpg" (8336)
Thread 2435256320
Runtime API
Driver API
Profiling Overhead
[0] NVIDIA Tegra X2
Context 1 (CUDA)
MemCpy (HtoD)
MemCpy (DtoH)
Compute
59.2% maxwell_scudnn_winograd_128...
6.4% normalize_kernel(int, float*, float...
6.1% void cudnn::winograd::generate...
4.8% fill_kernel(int, float, float*, int)
4.7% add_bias_kernel(float*, float*, in...
4.4% scale_bias_kernel(float*, float*, i...
4.0% copy_kernel(int, float*, int, int, flo...
3.9% activate_array_kernel(float*, int, ...
2.4% forward_maxpool_layer_kernel(i...
1.9% maxwell_scudnn_128x128_relu_i...
1.5% maxwell_scudnn_128x32_relu_s...
0.5% maxwell_scudnn_128x64_relu_int...
0.1% cudnn::maxwell::gemm::compute...
0.1% softmax_kernel(float*, int, int, int...
0.0% reorg_kernel(int, float*, int, int, in...
0.0% memset (0)
cudaMemcpy
Memcpy Ht...
fill_kernel(int, floa...
fill_kernel(int, floa...
maxwell_scudnn_128x32_relu_small_nn
copy_kernel(int, float*, int, int, float*, in...
normalize_kerne

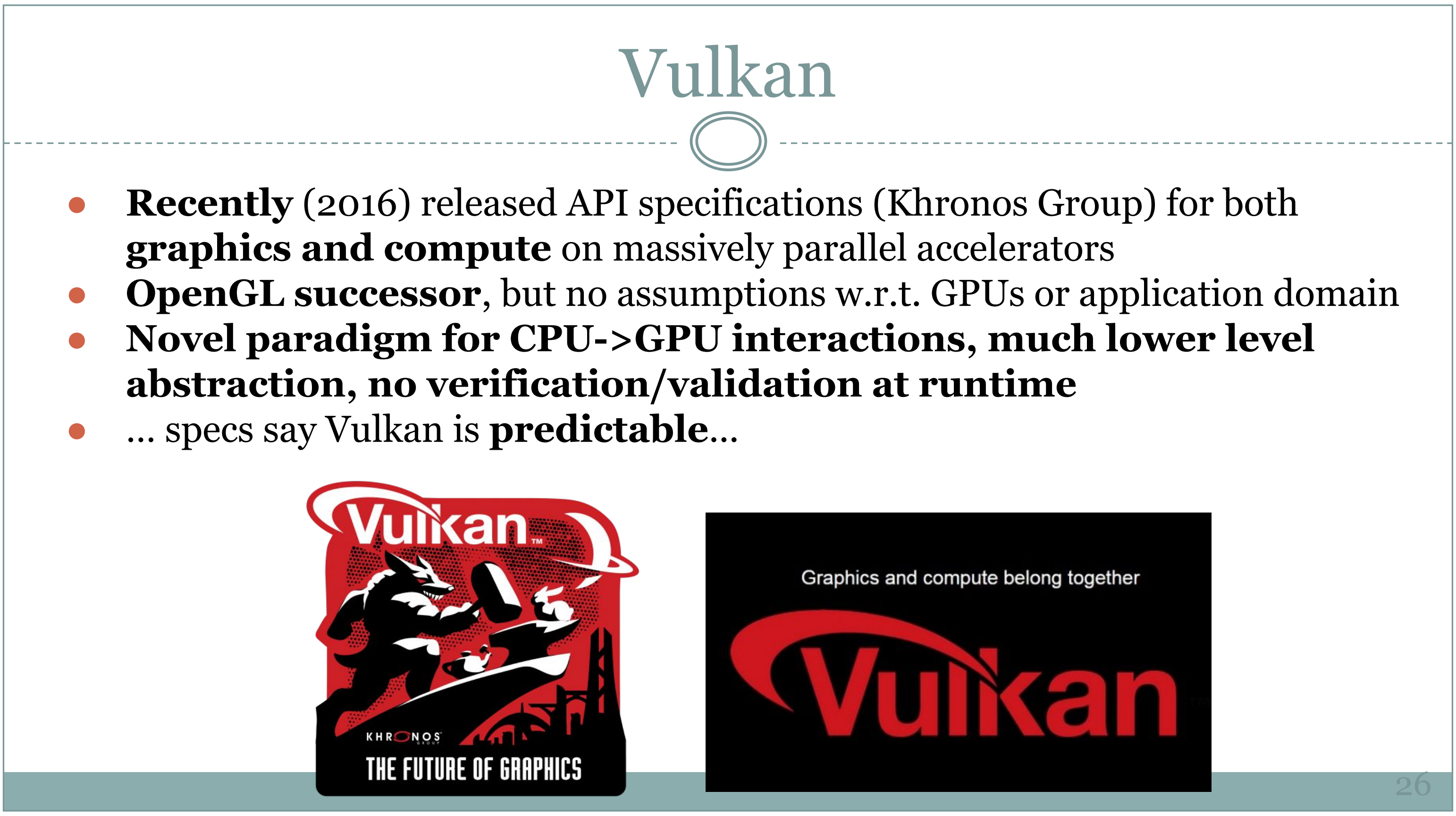


Submission models (CUDA)

1. Baseline asynchronous/synchronous kernel invocation
2. CDP (CUDA Dynamic Parallelism)
3. CUDA Graph API

...but what if we move away from CUDA?

25

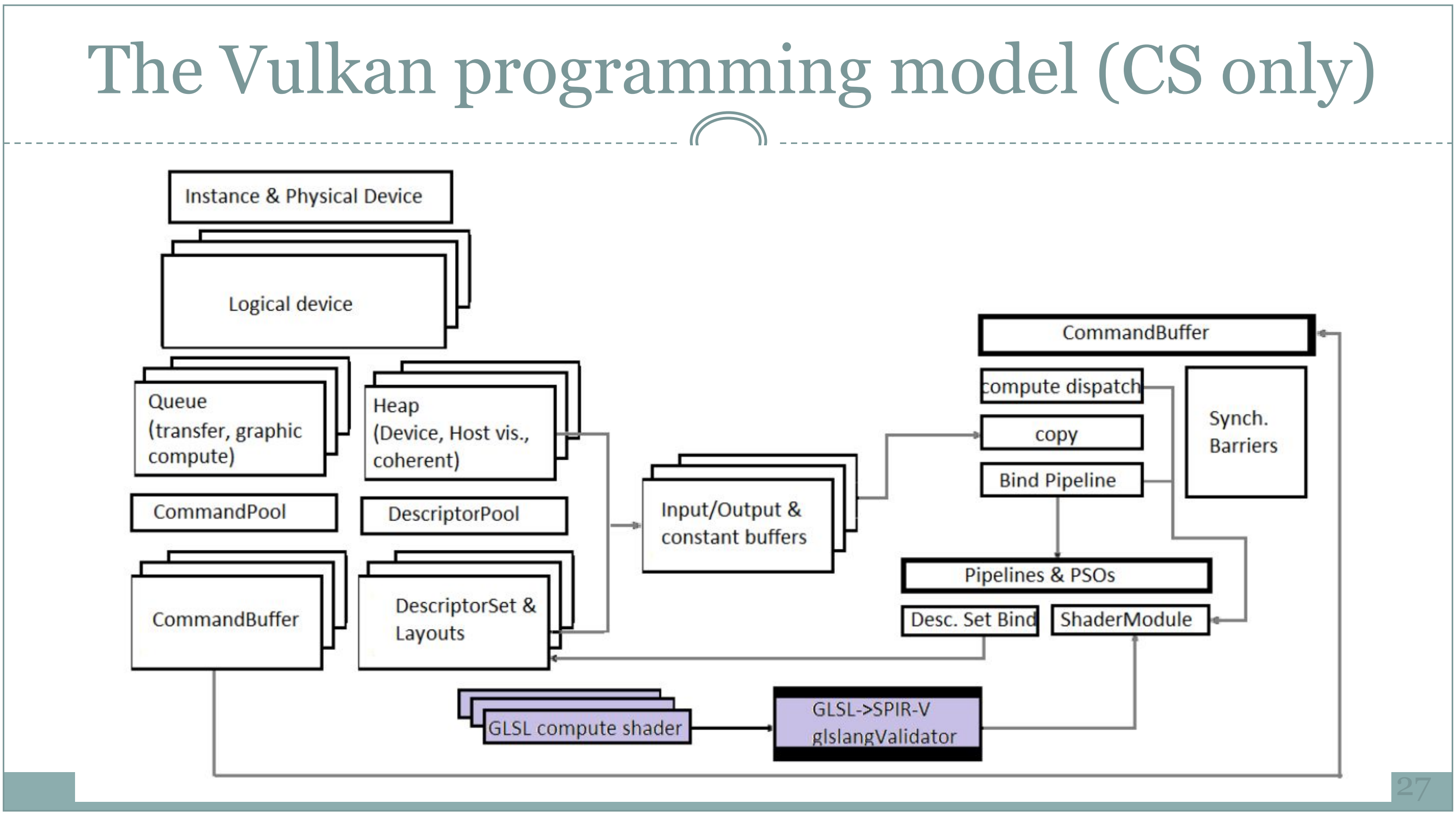


Vulkan

- **Recently** (2016) released API specifications (Khronos Group) for both **graphics and compute** on massively parallel accelerators
- **OpenGL successor**, but no assumptions w.r.t. GPUs or application domain
- **Novel paradigm for CPU->GPU interactions, much lower level abstraction, no verification/validation at runtime**
- ... specs say Vulkan is **predictable**...

Vulkan™
KHRONOS
THE FUTURE OF GRAPHICS
Graphics and compute belong together
Vulkan

26



The Vulkan programming model (CS only)

Instance & Physical Device

Logical device

Queue (transfer, graphic compute)

Heap (Device, Host vis., coherent)

CommandPool

DescriptorPool

CommandBuffer

DescriptorSet & Layouts

Input/Output & constant buffers

GLSL compute shader

GLSL->SPIR-V glslangValidator

CommandBuffer

compute dispatch

copy

Bind Pipeline

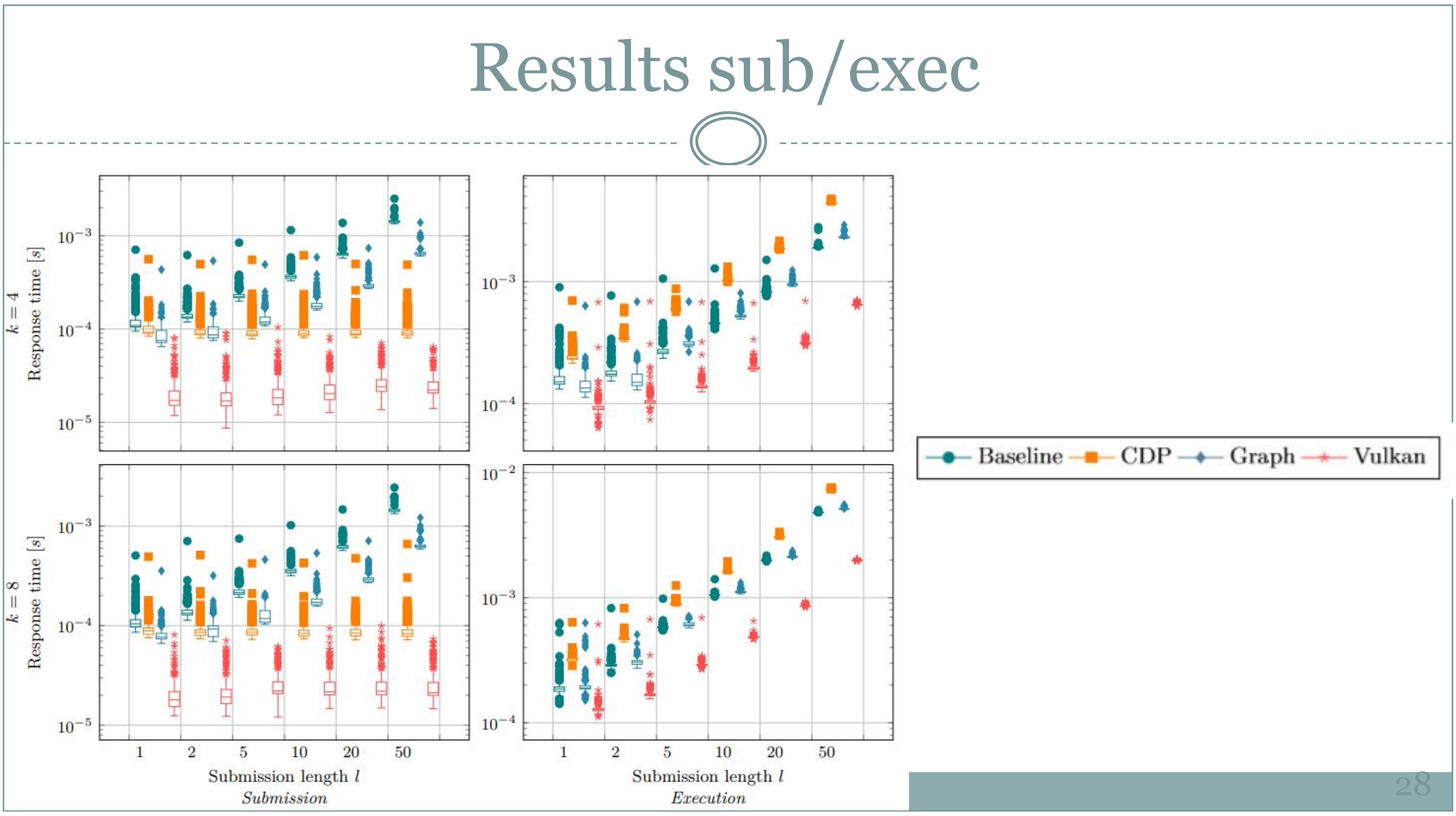
Synch. Barriers

Pipelines & PSOs

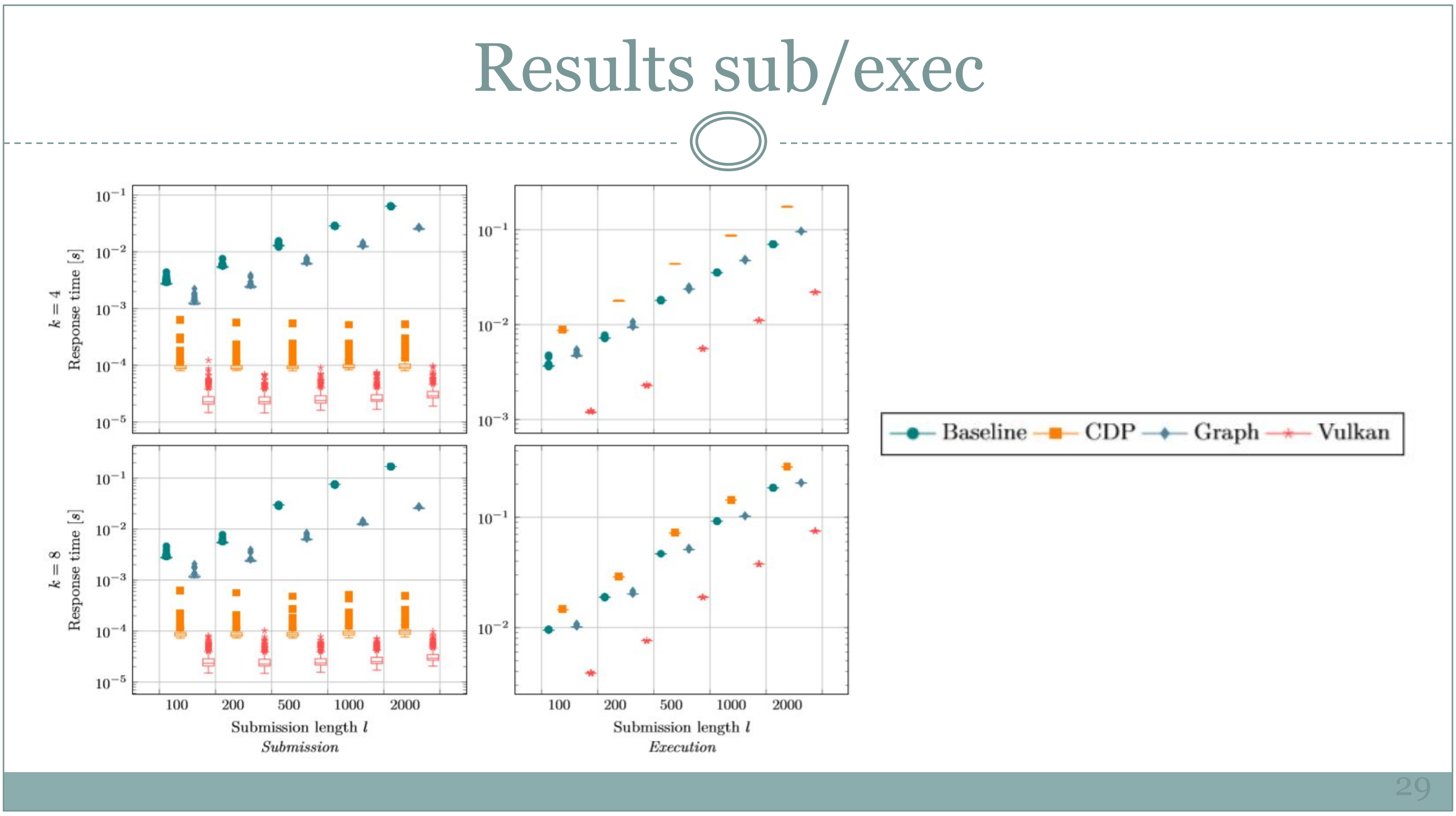
Desc. Set Bind

ShaderModule

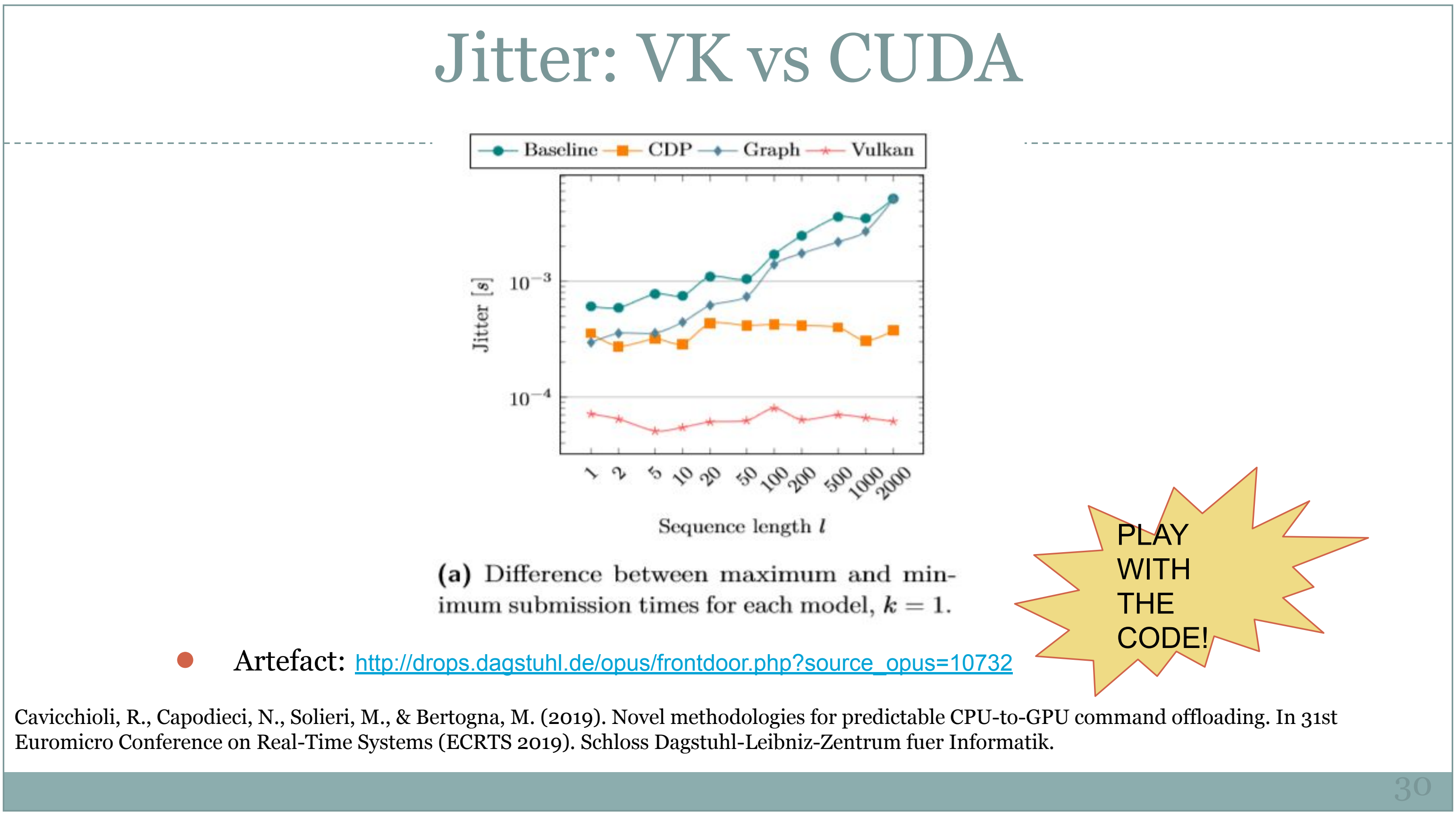
27



Results sub/exec



Results sub/exec



Jitter: VK vs CUDA

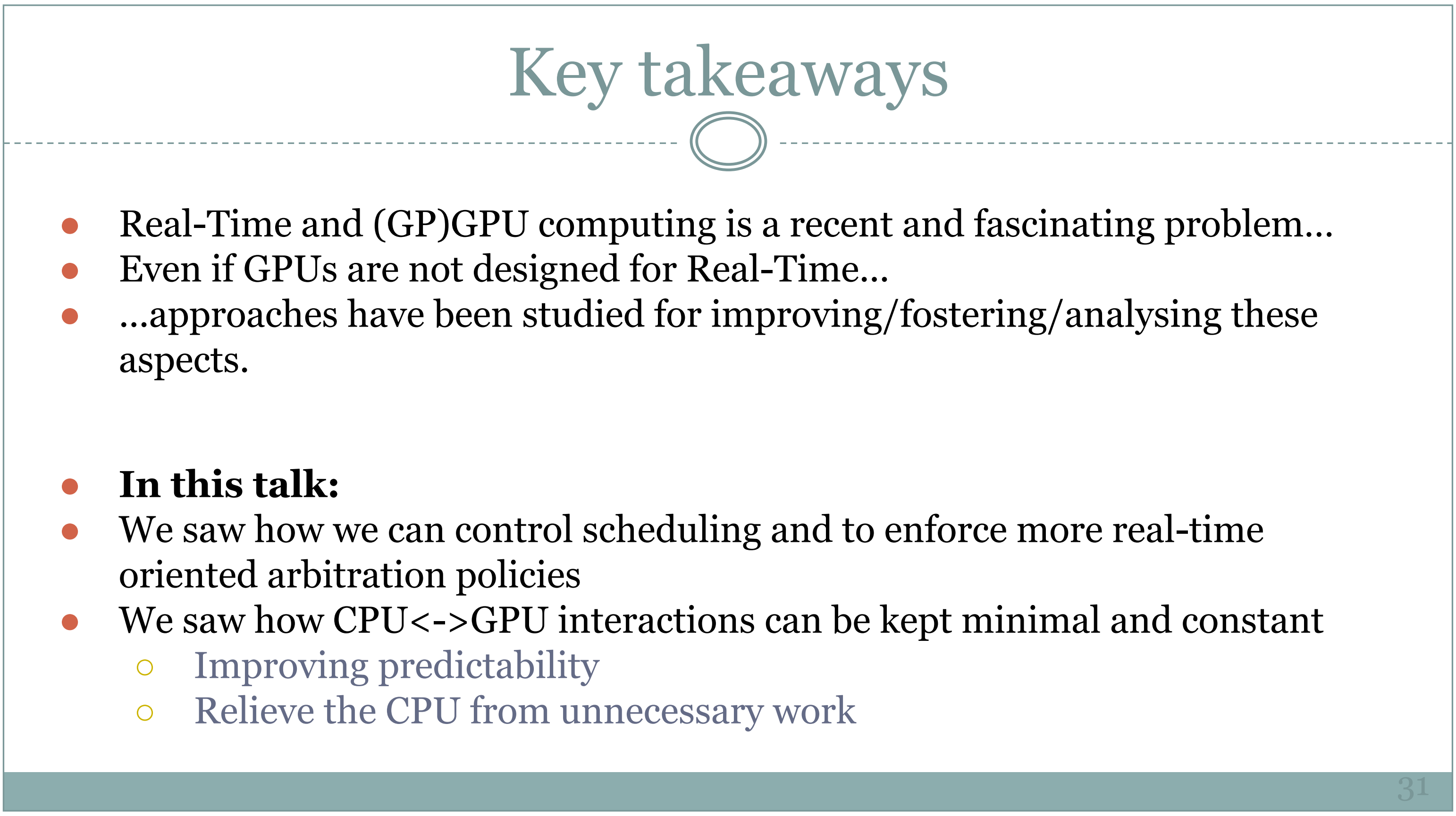
(a) Difference between maximum and minimum submission times for each model, $k = 1$.

- Artefact: http://drops.dagstuhl.de/opus/frontdoor.php?source_opus=10732

PLAY WITH THE CODE!

Cavicchioli, R., Capodieci, N., Solieri, M., & Bertogna, M. (2019). Novel methodologies for predictable CPU-to-GPU command offloading. In 31st Euromicro Conference on Real-Time Systems (ECRTS 2019). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

30

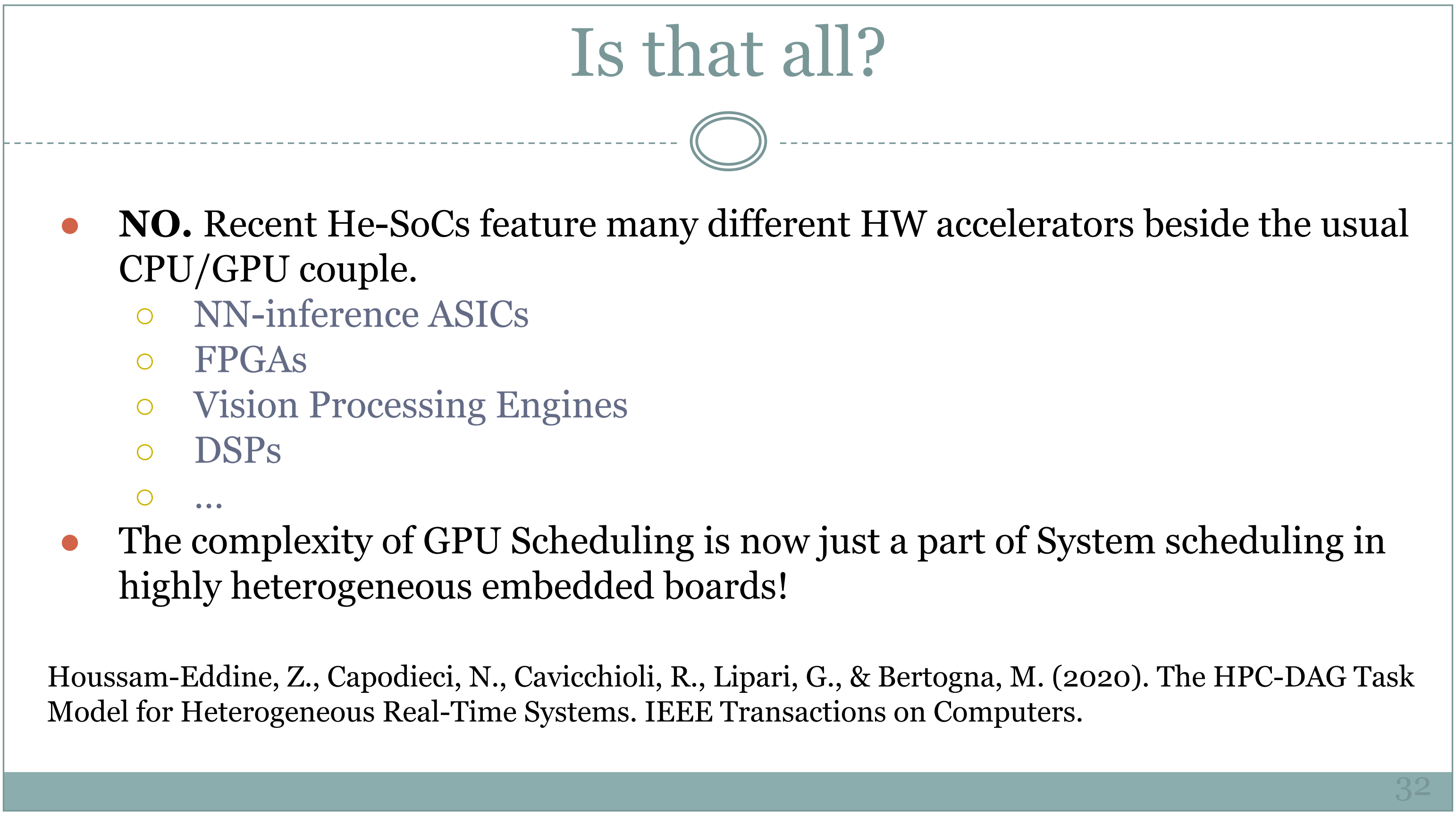


Key takeaways

- Real-Time and (GP)GPU computing is a recent and fascinating problem…
- Even if GPUs are not designed for Real-Time…
- …approaches have been studied for improving/fostering/analysing these aspects.

- **In this talk:**
- We saw how we can control scheduling and to enforce more real-time oriented arbitration policies
- We saw how CPU<->GPU interactions can be kept minimal and constant
  - ○ Improving predictability
  - ○ Relieve the CPU from unnecessary work

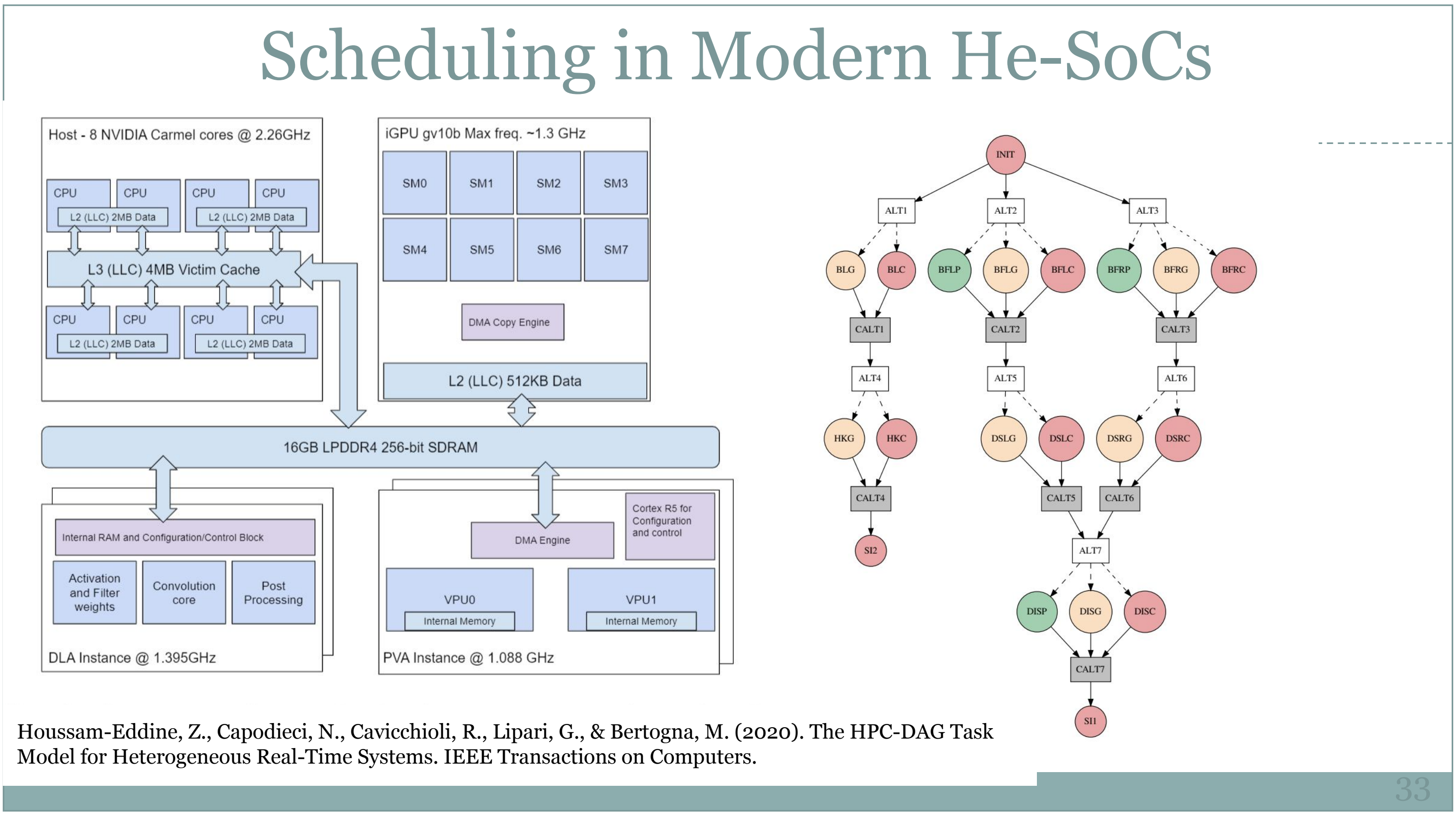
31



Is that all?

- **NO.** Recent He-SoCs feature many different HW accelerators beside the usual CPU/GPU couple.
  - NN-inference ASICs
  - FPGAs
  - Vision Processing Engines
  - DSPs
  - …
- The complexity of GPU Scheduling is now just a part of System scheduling in highly heterogeneous embedded boards!

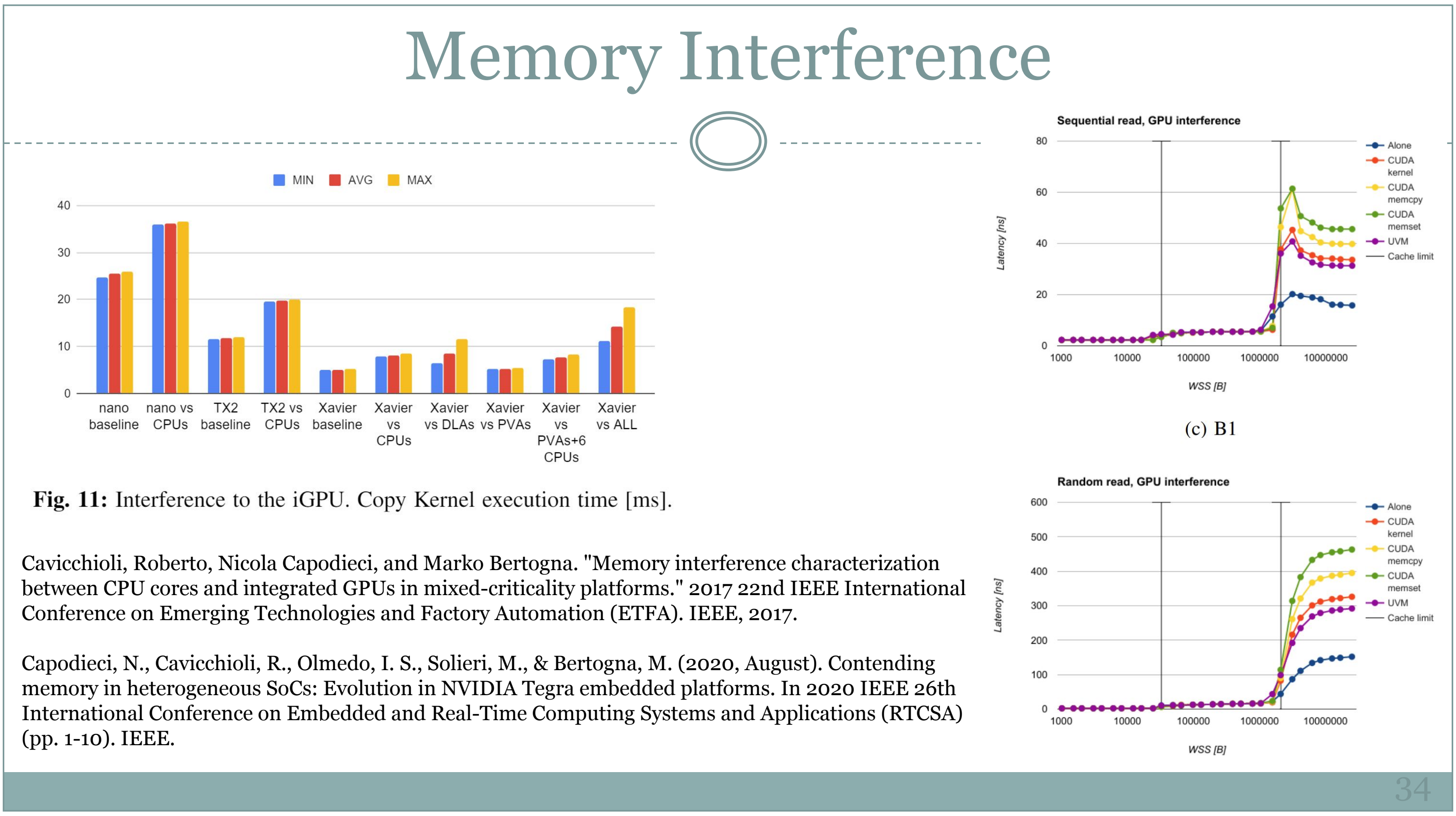
Houssam-Eddine, Z., Capodieci, N., Cavicchioli, R., Lipari, G., & Bertogna, M. (2020). The HPC-DAG Task Model for Heterogeneous Real-Time Systems. IEEE Transactions on Computers.



Scheduling in Modern He-SoCs

Houssam-Eddine, Z., Capodieci, N., Cavicchioli, R., Lipari, G., & Bertogna, M. (2020). The HPC-DAG Task Model for Heterogeneous Real-Time Systems. IEEE Transactions on Computers.

33



Memory Interference

Fig. 11: Interference to the iGPU. Copy Kernel execution time [ms].

Cavicchioli, Roberto, Nicola Capodieci, and Marko Bertogna. "Memory interference characterization between CPU cores and integrated GPUs in mixed-criticality platforms." 2017 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA). IEEE, 2017.

Capodieci, N., Cavicchioli, R., Olmedo, I. S., Solieri, M., & Bertogna, M. (2020, August). Contending memory in heterogeneous SoCs: Evolution in NVIDIA Tegra embedded platforms. In 2020 IEEE 26th International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA) (pp. 1-10). IEEE.

(c) B1

Thank you!

Questions?

https://hipert.unimore.it/

nicola.capodieci@unimore.it

35

Engineering a Manycore Processor for Edge Computing

Benoît Dupont de Dinechin
Kalray S.A. France
Email: benoit.dinechin@gmail.com
URL: https://sites.google.com/site/benoitdinechin/

Abstract – **Edge computing applications such as autonomous driving systems (ADS) and 5G radio access network (RAN) require significant computing capabilities and predictable response times, while being constrained by size, weight and power (SWaP). Such applications significantly benefit from computing platforms based on manycore processors. We first expose the differences between multi-core architectures and many-core architectures, currently mainly represented by GPGPU processors. Then, by using the MPPA3 processor from Kalray as an illustration, we present some of the challenges and the choices involved by engineering an edge processing computing platform based on a manycore architecture. On the local architecture, energy efficiency and time predictability can be leveraged from a Fisher-style VLIW architecture. Accelerating deep learning inference is achieved by tightly coupling a tensor coprocessor. On the global architecture, the cache coherence domains are preferably localized to the compute units. These compute units are connected by a network-on-chip capable of multi-casting, where deadlock-free routing requires some care. The computing platform is completed by providing standard and open programming environments. Among these, OpenCL, OpenVX and OpenMP appear as the most relevant for compute-intensive edge applications, once these environments are enabled to efficiently exploit the compute unit local memories of the manycore architecture.**

About the author

Benoît Dupont de Dinechin *is the Chief Technology Officer of Kalray. He is the main architect of the Kalray VLIW core including its deep learning coprocessor, and the co-architect of the Kalray Multi-Purpose Processing Array (MPPA) family of processors. Benoît also defined the Kalray software roadmap and still contributes to its production compilers. Before joining Kalray, Benoît was managing Research and Development of the STMicroelectronics Software, Tools, Services division, and was promoted to STMicroelectronics Fellow in 2008. Prior to STMicroelectronics, Benoît worked at the Cray Research park (Minnesota, USA), where he designed and developed the software pipeliner of the Cray T3E production compilers.*

Benoît earned an engineering degree in Radar and Telecommunications from the Ecole Nationale Supérieure de l'Aéronautique et de l'Espace (Toulouse, France), and a doctoral degree in computer systems from the University Pierre et Marie Curie (Paris) under the direction of Prof. P. Feautrier. He completed his post-doctoral studies at the McGill University (Montreal, Canada) at the ACAPS laboratory led by Prof. G.R. Gao. Benoît authored 16 patents in the area of computer architecture, and published over 60 conference papers, journal articles and book chapters in the areas of parallel computing, compiler design and operations research..

Hearables: From in-ear Recording of Vital Signs and Neural Function to Doctorless Hospitals

Danilo P. Mandić
Imperial College London, UK
Email: d.mandic@imperial.ac.uk
URL: http://www.commsp.ee.ic.ac.uk/~mandic/

Abstract – **Future health systems require the means to assess and track the neural and physiological function of a user over long periods of time, and in the community. Human body responses are manifested through multiple, interacting modalities – the mechanical, electrical and chemical; yet, current physiological monitors (e.g. actigraphy, heart rate) largely lack in cross-modal ability, are inconvenient and/or stigmatizing. We address these challenges through an inconspicuous earpiece, which benefits from the relatively stable position of the ear canal with respect to vital organs. Equipped with miniature multimodal sensors, it robustly measures the brain, cardiac and respiratory functions. Comprehensive experiments validate each modality within the proposed earpiece, while its potential in wearable health monitoring is illustrated through case studies spanning these three functions. We further demonstrate how combining data from multiple sensors within such an integrated wearable device improves both the accuracy of measurements and the ability to deal with artifacts in real-world scenarios. This framework opens up the avenues for a subsequent use of a number of machine learning paradigms, from lifelong learning to Big Data, to be used in a real world application of utmost importance – new generation health systems.**

Keywords – Health systems, Multimodal sensors, Health monitoring, Big data

About the author

Danilo P. Mandic *is a Professor in signal processing with Imperial College London, UK, and has been working in the areas of adaptive signal processing and bioengineering. He is a Fellow of the IEEE and member of the Board of Governors of International Neural Networks Society (INNS). He has received five best paper awards in Brain Computer Interface, runs the Smart Environments Lab at Imperial, and has more than 300 publications in journals and conferences. Prof Mandic has received the 2019 Dennis Gabor Award by the International Neural Networks Society (for outstanding achievements in neural engineering), and the President Award for Excellence in Postgraduate Supervision at Imperial. His work on Hearables appeared in IEEE Spectrum, MIT Technology Review and has led to several granted patents in this area.*

Learning, Analysis, Synthesis and Optimization of CPS

Kim G Larsen & Marius Mikucionis

Aalborg University, DENMARK

AALBORG UNIVERSITET

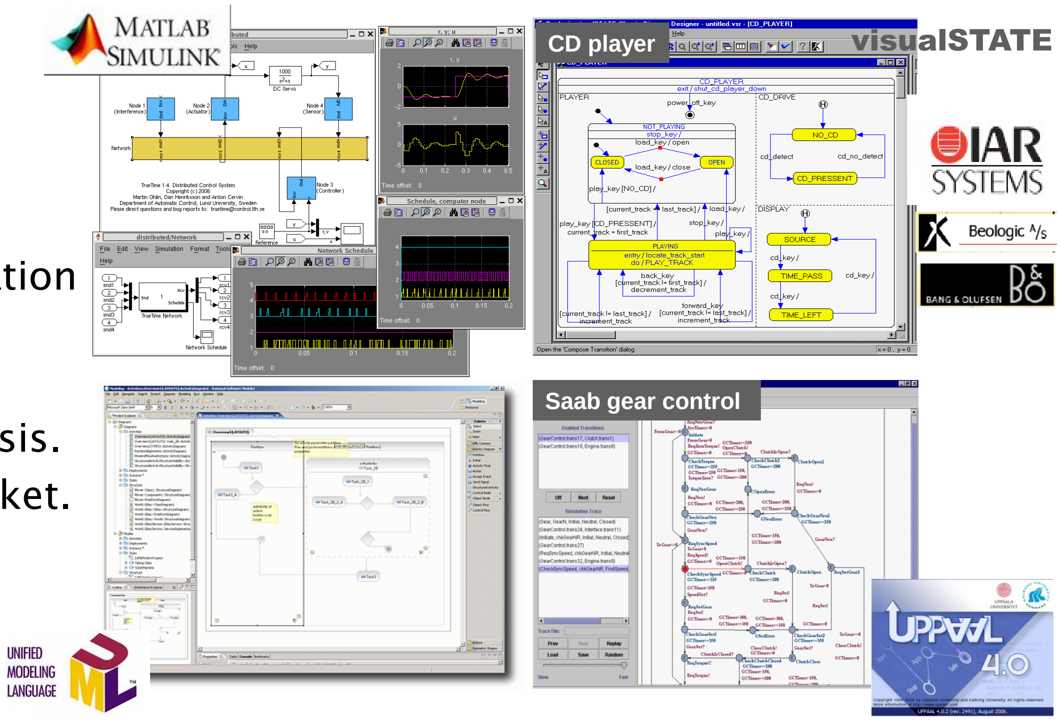
erc

VILLUM FONDEN

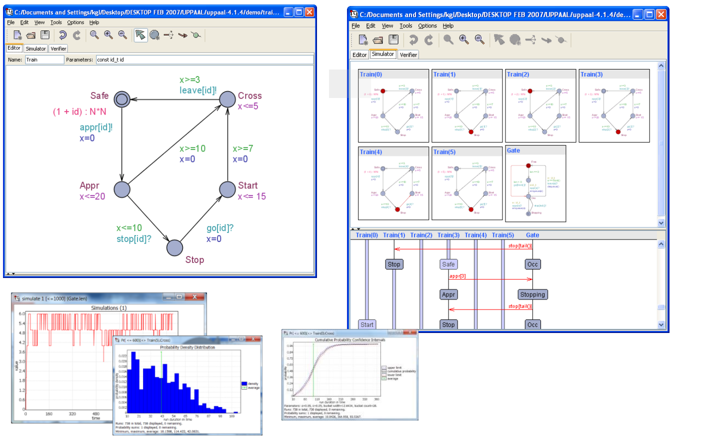
UPPAAL 4.0

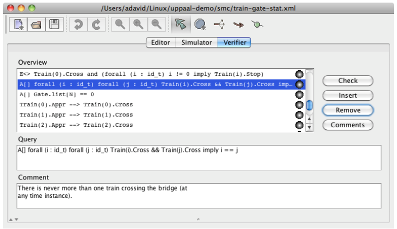
Model Driven Development

- High-level designs
- Early design-space exploration
- Early error-detection
- Efficient code generation
- Automatization of testing.
- Verification & synthesis.
- Reduced time-to-market.
- Outsourcing
- Reuse and reconfiguration



UPPAAL Tool Suite





Overview

```
E<> Train(0).Cross and (forall (i : id_t) i != 0 imply Train(i).Stop)
A[] forall (i : id_t) forall (j : id_t) Train(i).Cross && Train(j).Cross imp…
A[] Gate.list[N] == 0
Train(0).Appr --> Train(0).Cross
Train(1).Appr --> Train(1).Cross
Train(2).Appr --> Train(2).Cross
```

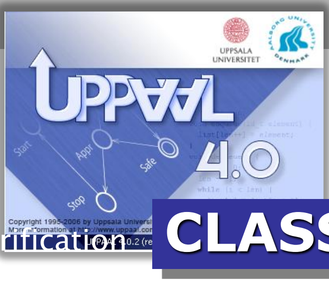
Query

A[] forall (i : id_t) forall (j : id_t) Train(i).Cross && Train(j).Cross imply i == j

Comment

There is never more than one train crossing the bridge (at any time instance).

CAV AWARD 2013



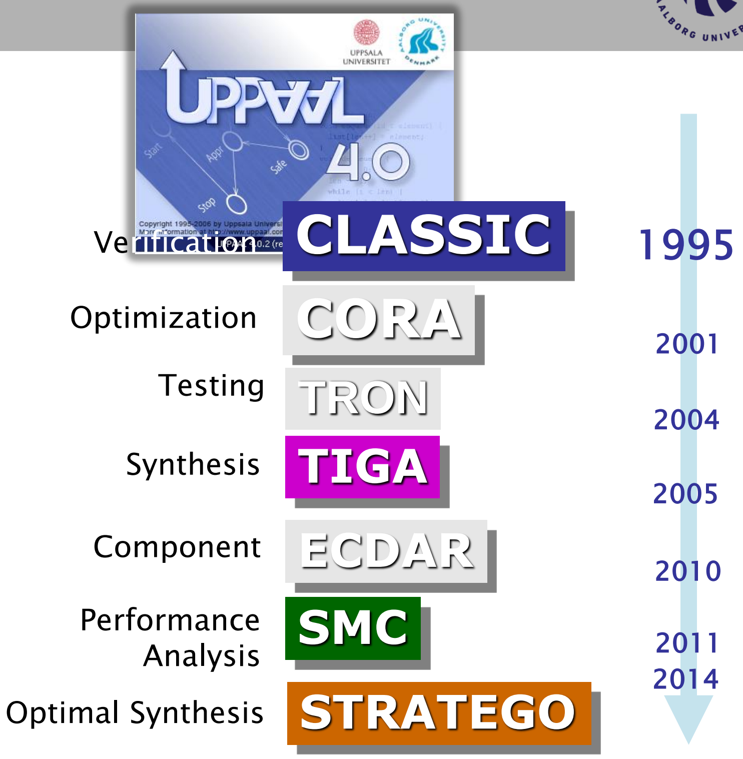
Verification	CLASSIC	1995
Optimization	CORA	2001
Testing	TRON	2004
Synthesis	TIGA	2005
Component	ECDAR	2010
Performance Analysis	SMC	2011
Optimal Synthesis	STRATEGO	2014

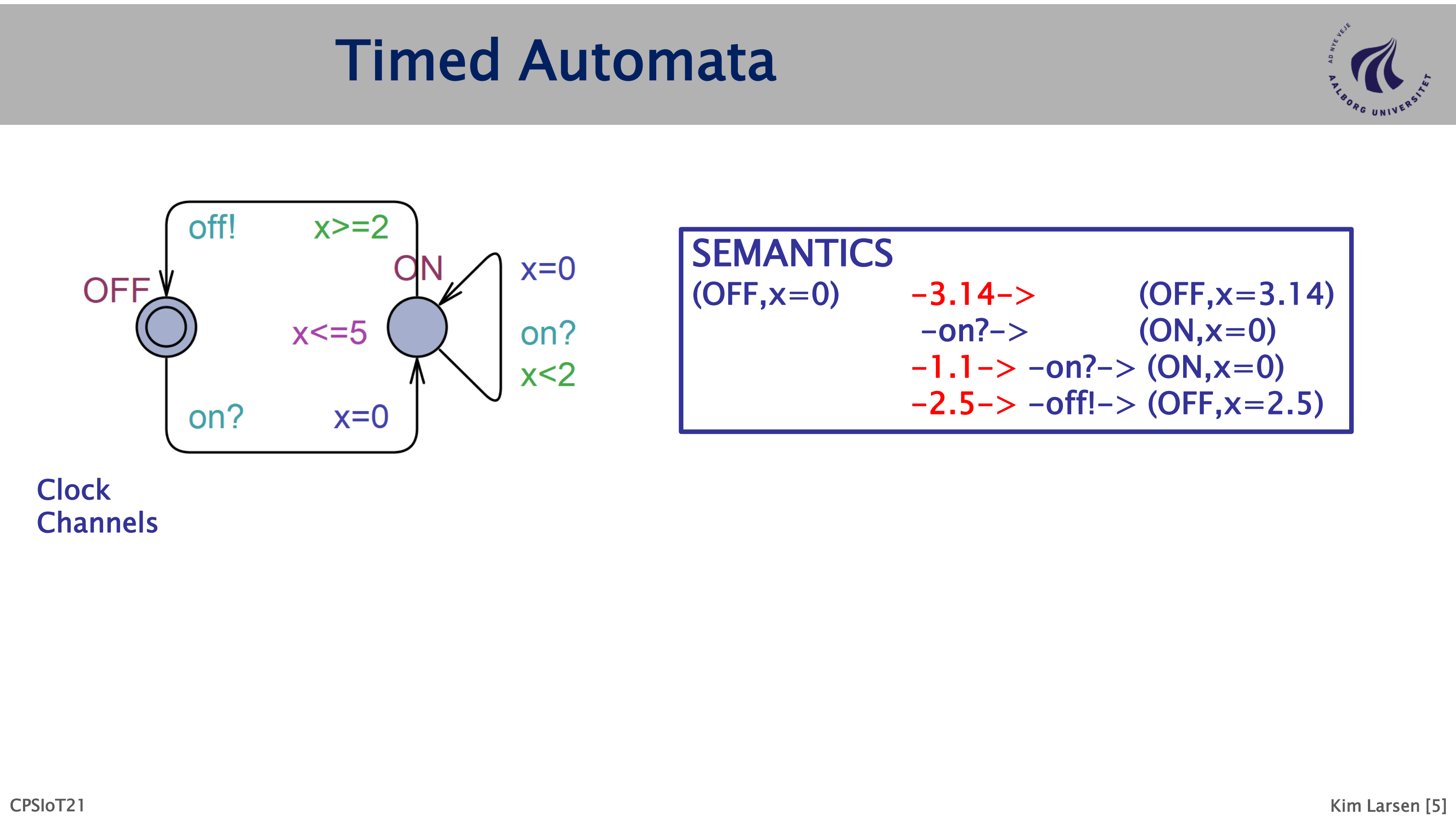
CPSIoT21

Kim Larsen [3]

Overview

- UPPAAL Formalism
- Verification
  - Automatic Gear Control
  - Protocols
- Performance Analysis
  - Schedulability & Mixed-Criticality Systems
  - Energy-Aware Sensor Networks
- Learning & Optimization
  - Traffic Control
  - Autonomous Farming
- References





Timed Automata

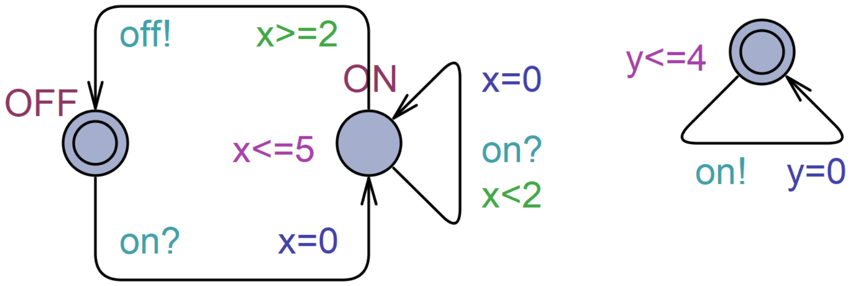
SEMANTICS
(OFF,x=0) -3.14-> (OFF,x=3.14)
-on?-> (ON,x=0)
-1.1-> -on?-> (ON,x=0)
-2.5-> -off!-> (OFF,x=2.5)

Clock
Channels

CPSIoT21

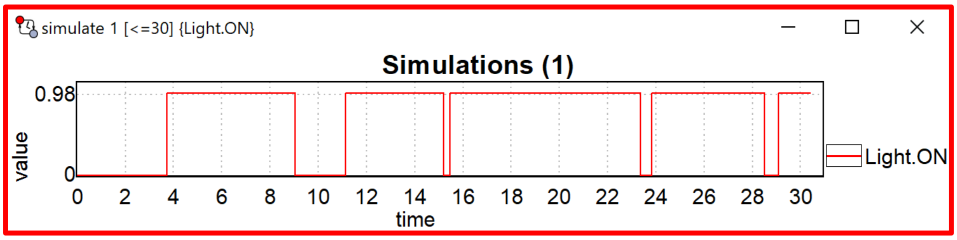
Kim Larsen [5]

Timed Automata



```
broadcast chan on, off;
clock x, y;
```

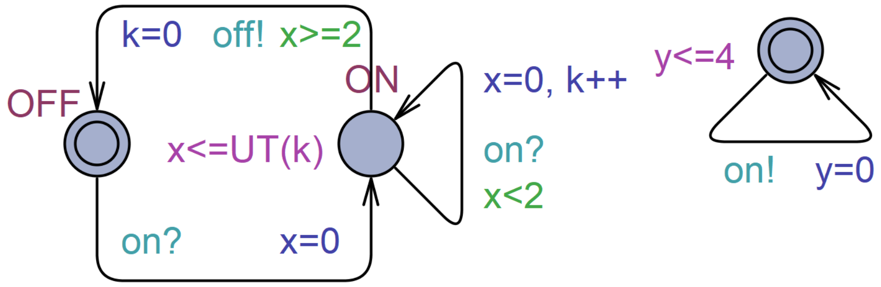
Clock
Channels
Networks


simulate 1 [<=30] {Light.ON}

CPSIoT21

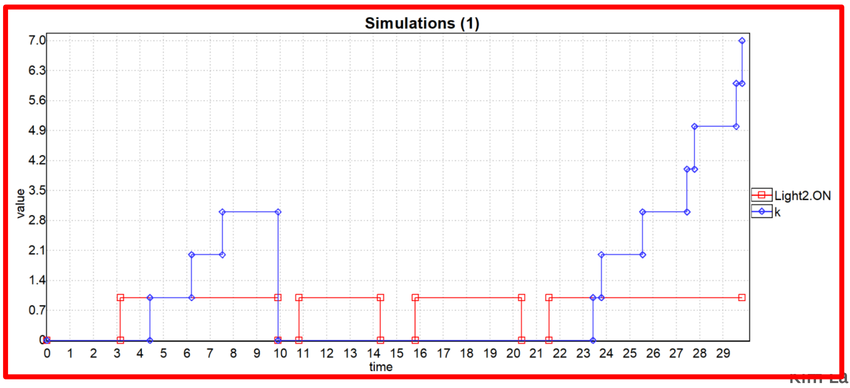
Kim Larsen [6]

Extended Timed Automata



```
broadcast chan on, off;
clock x, y;

int k;
int UT (int X)
{
     return X+5;
}
```

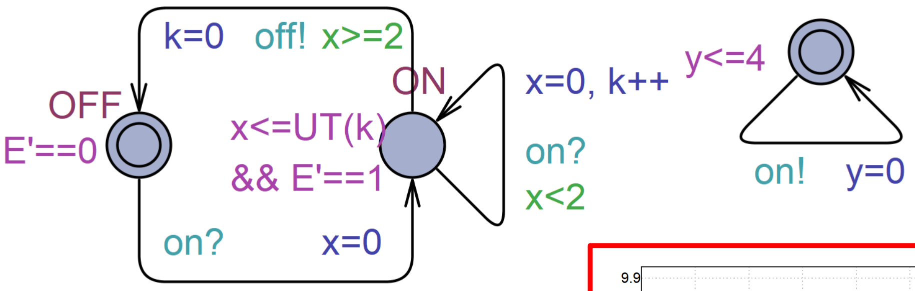
Clock
Channels
Networks
Integer variables
Structured variables, clocks, channels
User defined types, functions



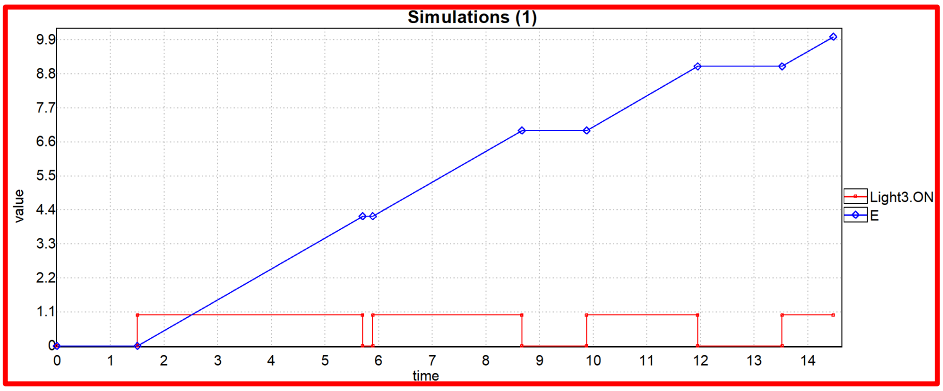
CPSIoT21

Kim Larsen [7]

Priced Timed Automata

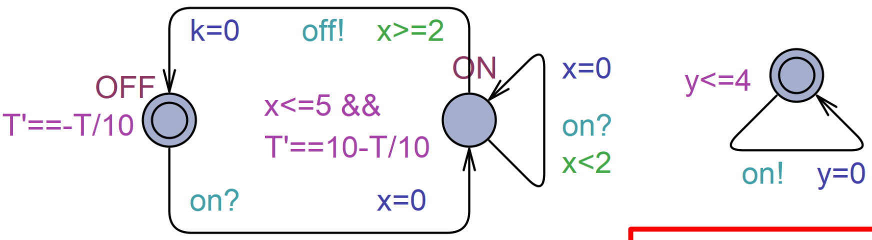


```
broadcast chan on, off;
clock x, y;
hybrid clock E;
```

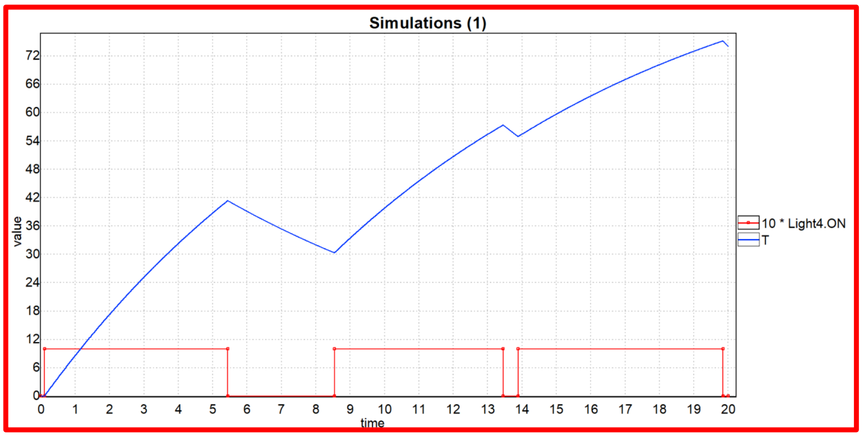


Clock
Channels
Networks
Integer variables
Structured variables, clocks, channels
User defined types, functions
Linear Rate Price Functions

Hybrid Automata

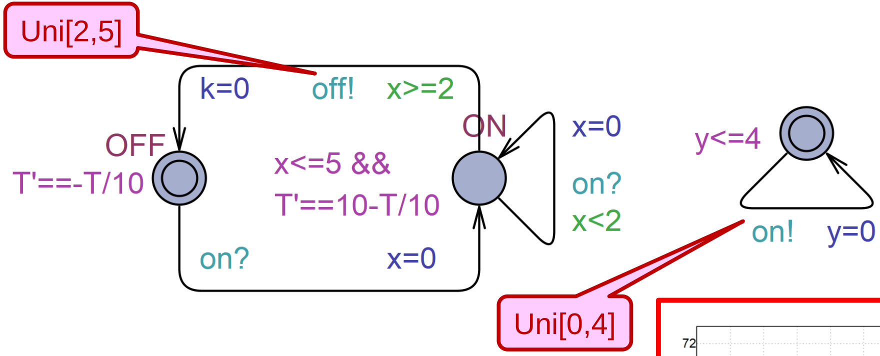


```
broadcast chan on, off;
clock x, y;
hybrid clock T;
```

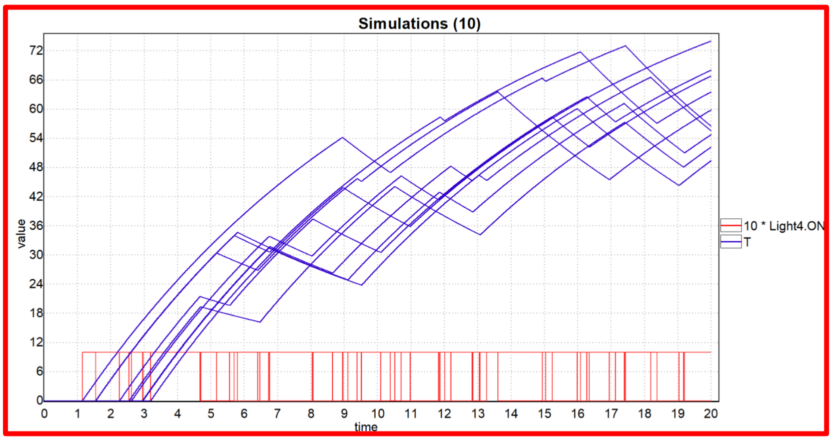


Clock
Channels
Networks
Integer variables
Structured variables, clocks, channels
User defined types, functions
Linear Rate Price Functions
Continuous Variables

Stochastic Hybrid Automata

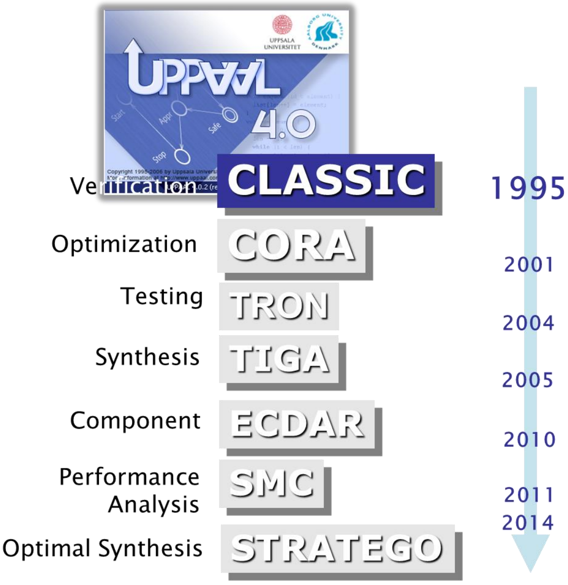


```
broadcast chan on, off;
clock x, y;
hybrid clock T;
```



Clock
Channels
Networks
Integer variables
Structured variables, clocks, channels
User defined types, functions
Linear Rate Price Functions
Continuous Variables
Delay Distributions, Discrete Probabilities

Verification



Verification CLASSIC 1995

Optimization CORA 2001

Testing TRON 2004

Synthesis TIGA 2005

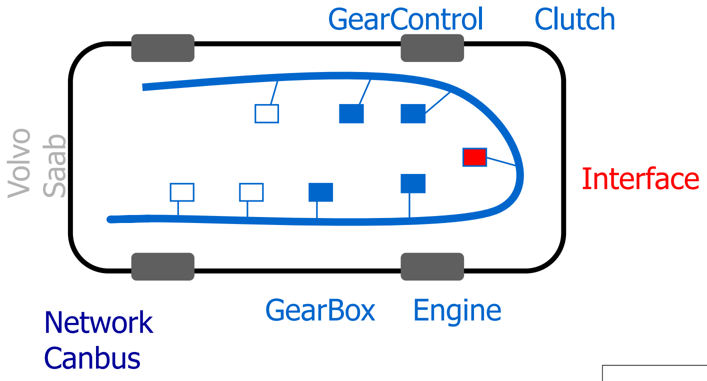
Component ECDAR 2010

Performance Analysis SMC 2011

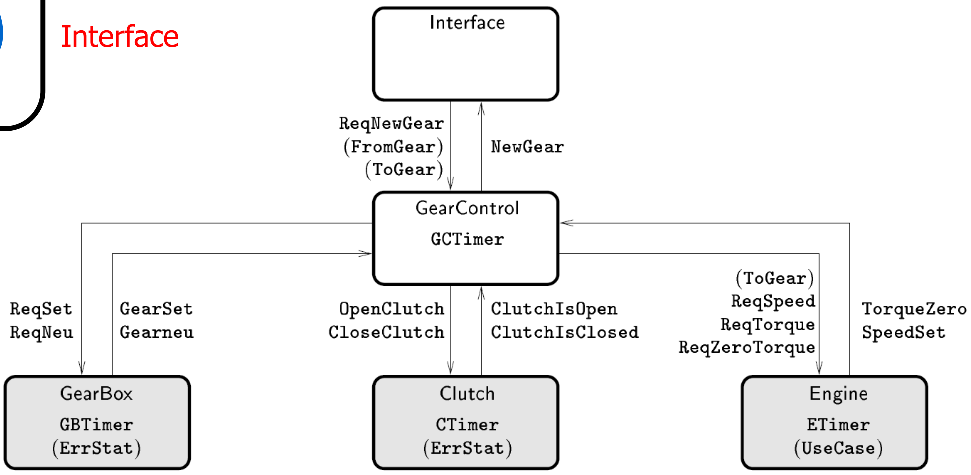
Optimal Synthesis STRATEGO 2014

Gear Controller

with MECEL AB



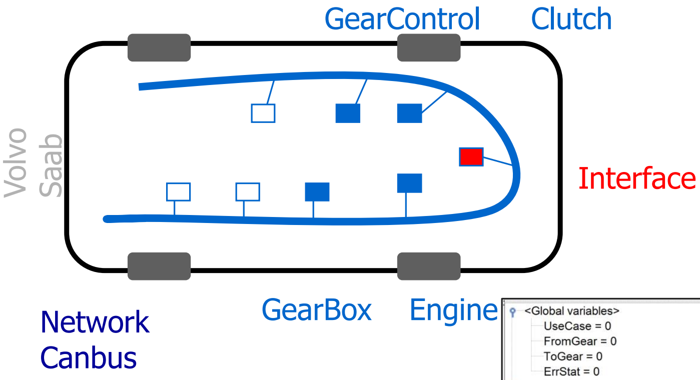
Flowgraph

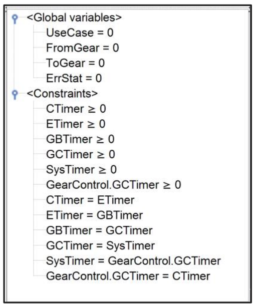


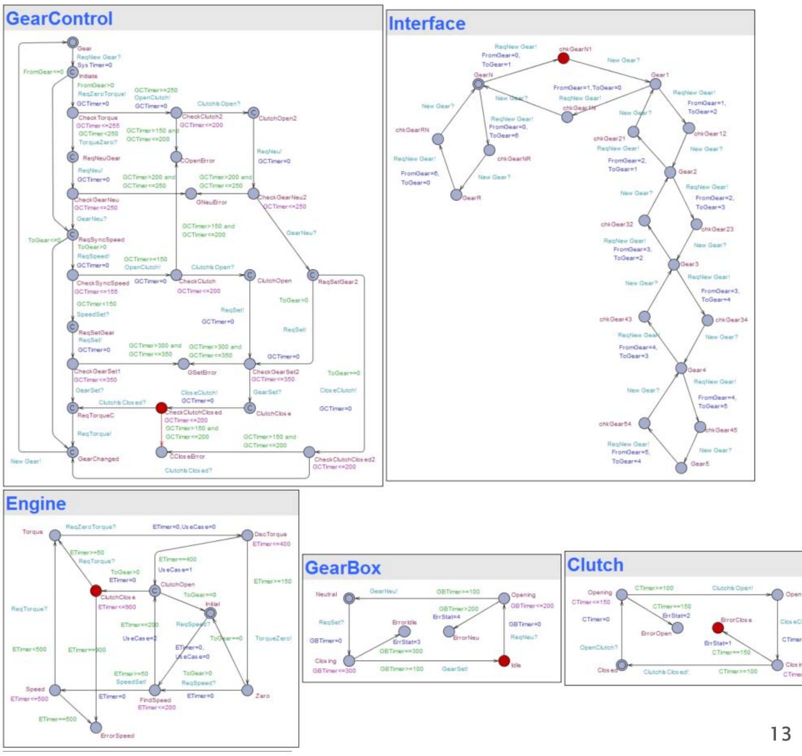
Magnus Lindahl
Paul Pettersson
Wang Yi
1998

Gear Controller

with MECEL AB




<Global variables>
UseCase = 0
FromGear = 0
ToGear = 0
ErrStat = 0
<Constraints>
CTimer ≥ 0
ETimer ≥ 0
GBTimer ≥ 0
GCTimer ≥ 0
SysTimer ≥ 0
GearControl.GCTimer ≥ 0
CTimer = ETimer
ETimer = GBTimer
GBTimer = GCTimer
GCTimer = SysTimer
SysTimer = GearControl.GCTimer
GearControl.GCTimer = CTimer

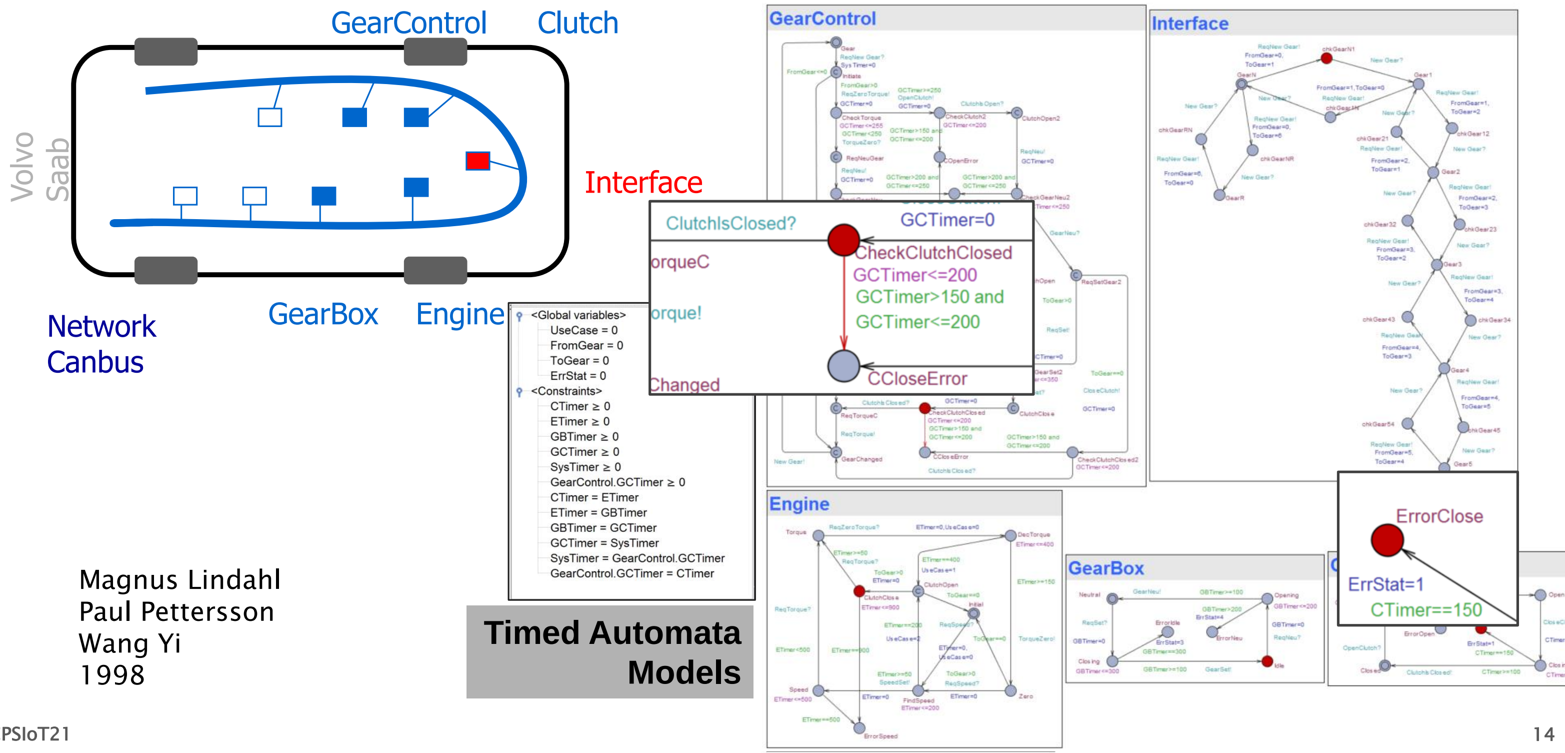


Magnus Lindahl
Paul Pettersson
Wang Yi
1998

Timed Automata Models

Gear Controller

with MECEL AB



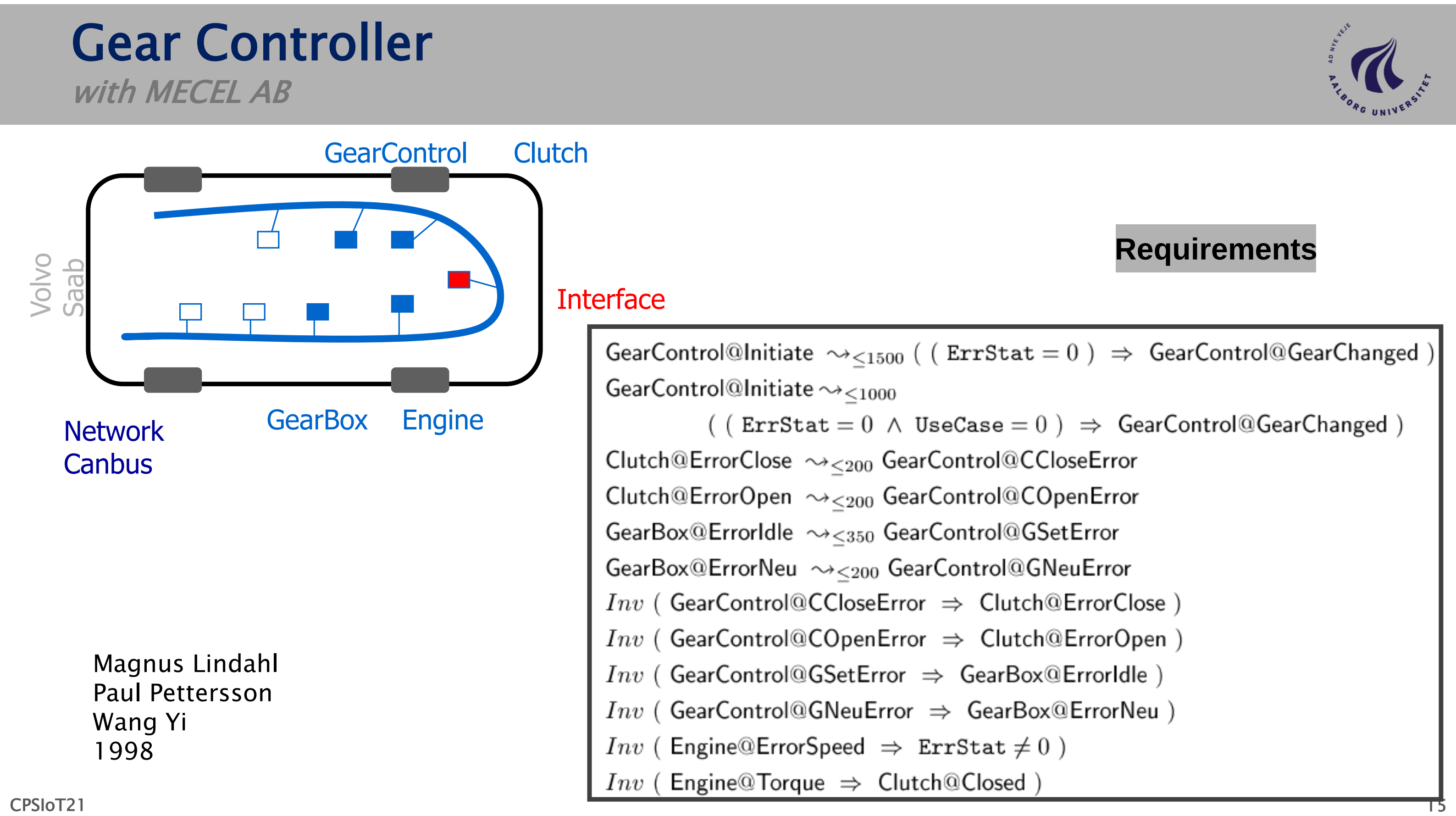
```
<Global variables>
    UseCase = 0
    FromGear = 0
    ToGear = 0
    ErrStat = 0
<Constraints>
    CTimer ≥ 0
    ETimer ≥ 0
    GBTimer ≥ 0
    GCTimer ≥ 0
    SysTimer ≥ 0
    GearControl.GCTimer ≥ 0
    CTimer = ETimer
    ETimer = GBTimer
    GBTimer = GCTimer
    GCTimer = SysTimer
    SysTimer = GearControl.GCTimer
    GearControl.GCTimer = CTimer
```

Magnus Lindahl
Paul Pettersson
Wang Yi
1998

Timed Automata Models

CPSIoT21

14



Gear Controller

with MECEL AB

Requirements

GearControl@Initiate $\leadsto_{\leq 1500}$ (($\mathtt{ErrStat} = 0$) $\Rightarrow$ GearControl@GearChanged)

GearControl@Initiate $\leadsto_{\leq 1000}$

(($\mathtt{ErrStat} = 0 \wedge \mathtt{UseCase} = 0$) $\Rightarrow$ GearControl@GearChanged)

Clutch@ErrorClose $\leadsto_{\leq 200}$ GearControl@CCloseError

Clutch@ErrorOpen $\leadsto_{\leq 200}$ GearControl@COpenError

GearBox@ErrorIdle $\leadsto_{\leq 350}$ GearControl@GSetError

GearBox@ErrorNeu $\leadsto_{\leq 200}$ GearControl@GNeuError

Inv (GearControl@CCloseError $\Rightarrow$ Clutch@ErrorClose)

Inv (GearControl@COpenError $\Rightarrow$ Clutch@ErrorOpen)

Inv (GearControl@GSetError $\Rightarrow$ GearBox@ErrorIdle)

Inv (GearControl@GNeuError $\Rightarrow$ GearBox@ErrorNeu)

Inv (Engine@ErrorSpeed $\Rightarrow$ $\mathtt{ErrStat} \neq 0$)

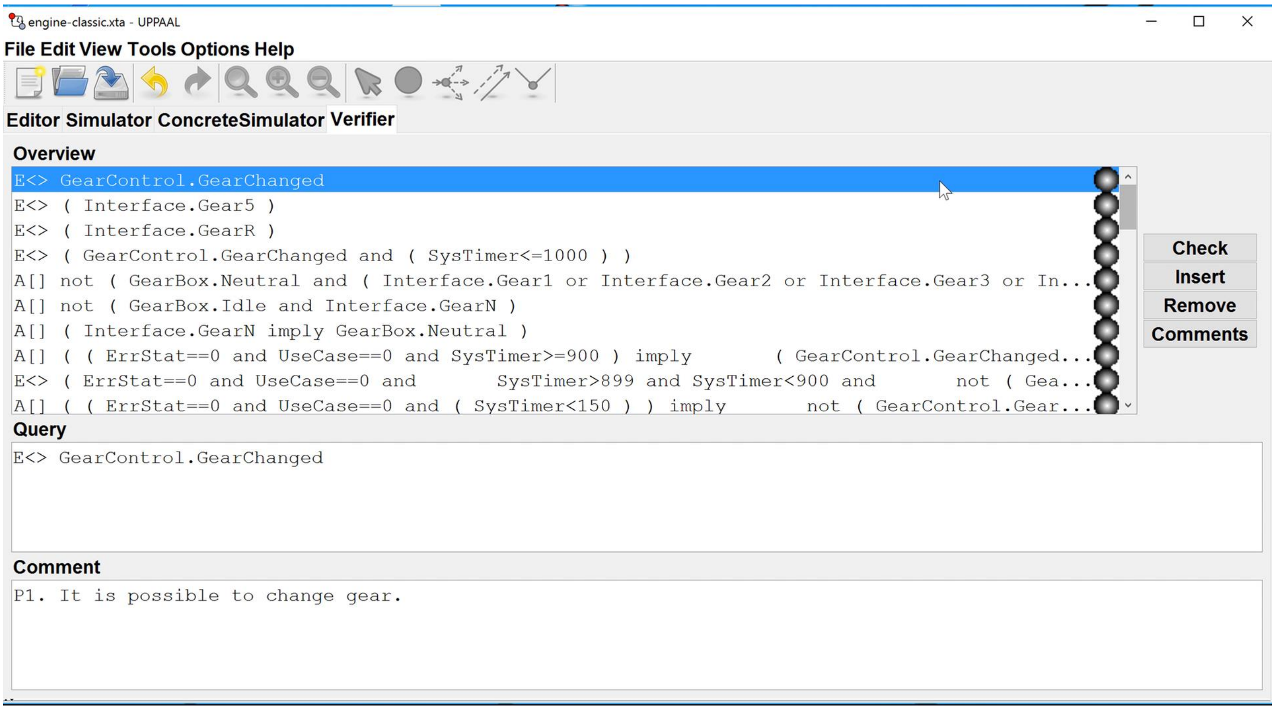
Inv (Engine@Torque $\Rightarrow$ Clutch@Closed)

Magnus Lindahl
Paul Pettersson
Wang Yi
1998

CPSIoT21

15

UPPAAL Model Checking – Demo

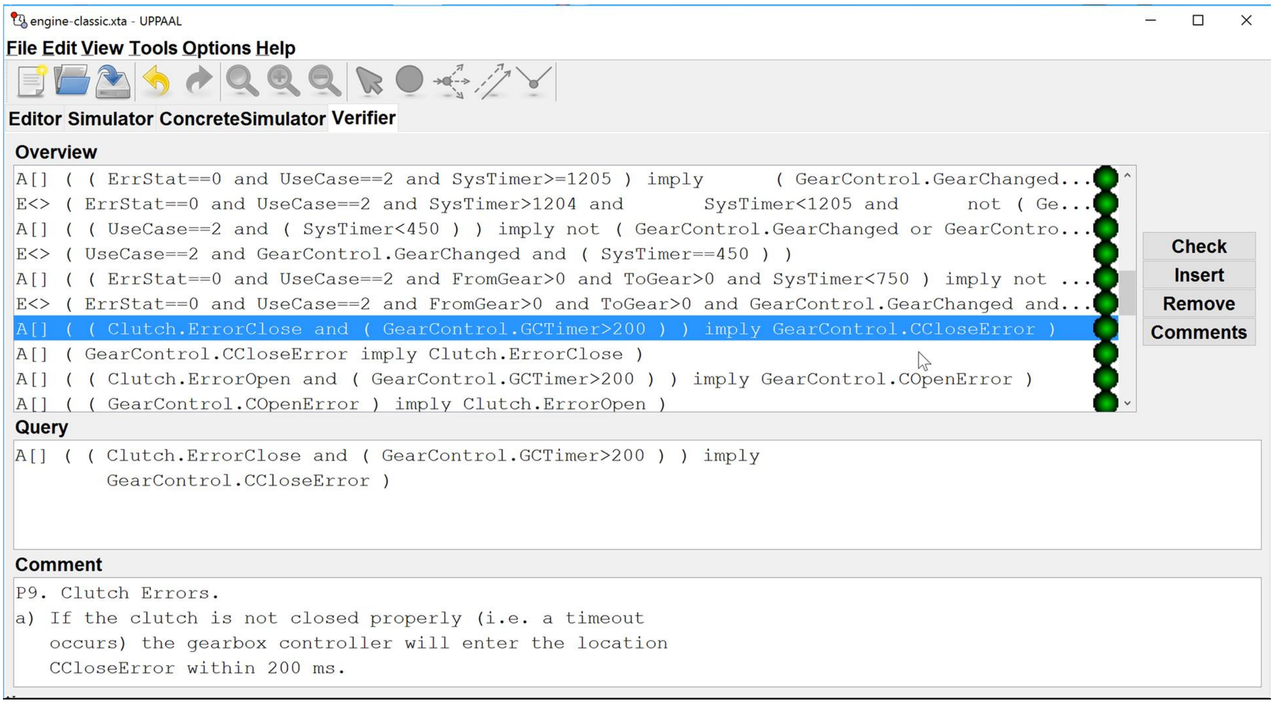

engine-classic.xta - UPPAAL
File Edit View Tools Options Help
Editor Simulator ConcreteSimulator Verifier
Overview
Check
Insert
Remove
Comments
Query
Comment

```
E<> GearControl.GearChanged
E<> ( Interface.Gear5 )
E<> ( Interface.GearR )
E<> ( GearControl.GearChanged and ( SysTimer<=1000 ) )
A[] not ( GearBox.Neutral and ( Interface.Gear1 or Interface.Gear2 or Interface.Gear3 or In...
A[] not ( GearBox.Idle and Interface.GearN )
A[] ( Interface.GearN imply GearBox.Neutral )
A[] ( ( ErrStat==0 and UseCase==0 and SysTimer>=900 ) imply       ( GearControl.GearChanged...
E<> ( ErrStat==0 and UseCase==0 and       SysTimer>899 and SysTimer<900 and       not ( Gea...
A[] ( ( ErrStat==0 and UseCase==0 and ( SysTimer<150 ) ) imply       not ( GearControl.Gear...
```

```
E<> GearControl.GearChanged
```

```
P1. It is possible to change gear.
```

UPPAAL Model Checking – Demo


engine-classic.xta - UPPAAL
File Edit View Tools Options Help
Editor Simulator ConcreteSimulator Verifier
Check
Insert
Remove
Comments

Overview

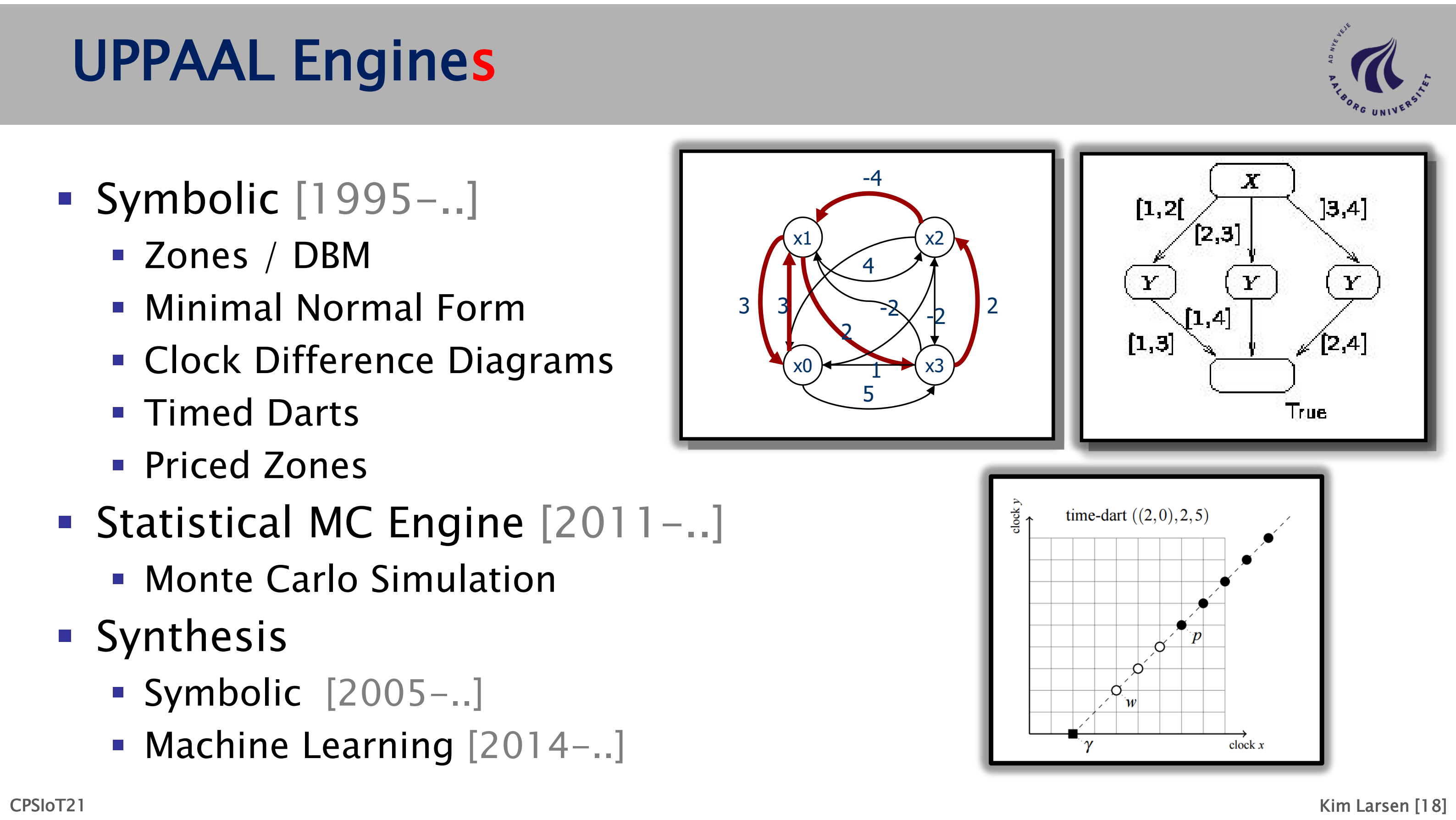
```
A[] ( ( ErrStat==0 and UseCase==2 and SysTimer>=1205 ) imply      ( GearControl.GearChanged...
E<> ( ErrStat==0 and UseCase==2 and SysTimer>1204 and       SysTimer<1205 and      not ( Ge...
A[] ( ( UseCase==2 and ( SysTimer<450 ) ) imply not ( GearControl.GearChanged or GearContro...
E<> ( UseCase==2 and GearControl.GearChanged and ( SysTimer==450 ) )
A[] ( ( ErrStat==0 and UseCase==2 and FromGear>0 and ToGear>0 and SysTimer<750 ) imply not ...
E<> ( ErrStat==0 and UseCase==2 and FromGear>0 and ToGear>0 and GearControl.GearChanged and...
A[] ( ( Clutch.ErrorClose and ( GearControl.GCTimer>200 ) ) imply GearControl.CCloseError )
A[] ( GearControl.CCloseError imply Clutch.ErrorClose )
A[] ( ( Clutch.ErrorOpen and ( GearControl.GCTimer>200 ) ) imply GearControl.COpenError )
A[] ( ( GearControl.COpenError ) imply Clutch.ErrorOpen )
```

Query

```
A[] ( ( Clutch.ErrorClose and ( GearControl.GCTimer>200 ) ) imply
        GearControl.CCloseError )
```

Comment

```
P9. Clutch Errors.
a) If the clutch is not closed properly (i.e. a timeout
   occurs) the gearbox controller will enter the location
   CCloseError within 200 ms.
```



UPPAAL Engines

- Symbolic [1995-..]
  - Zones / DBM
  - Minimal Normal Form
  - Clock Difference Diagrams
  - Timed Darts
  - Priced Zones
- Statistical MC Engine [2011-..]
  - Monte Carlo Simulation
- Synthesis
  - Symbolic [2005-..]
  - Machine Learning [2014-..]

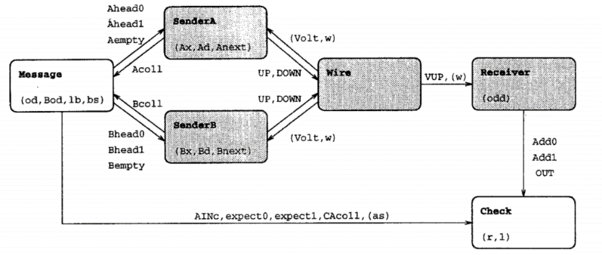
-4
x1
x2
4
3
3
-2
-2
2
2
x0
x3
1
5
X
[1,2[
[2,3]
]3,4]
Y
Y
Y
[1,4]
[1,3]
[2,4]
True
time-dart ((2,0),2,5)
clock y
clock x
p
w
γ

CPSIoT21

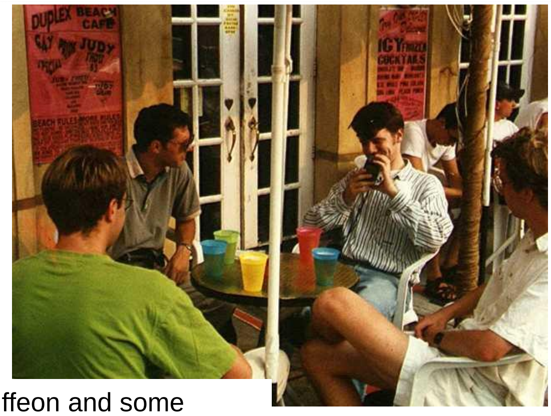
Kim Larsen [18]

Philips Audio Protocol [1996]
with collision

- **Bosscher, Polak, Vaandrager**
- Physical layer of interface bus (tuner, CD player,..)
- Manuel, HyTech, UPPAAL/Kronos verification
- Challenge:
  Several senders & collision
- Committed Locations
  Now POR for TA (CAV18)
- 8.82 hrs /527.4MB on SGI ONYX
  Now 0.5 sec /2.5MB
- Biggest verified timed model at the time
  (1000 x larger discrete state-space)



Frits Vaandrager



David Griffeon and some Scandinavian friends at CAV96

CPSIoT21

Kim Larsen [19]

Bang & Olufsen [1997]
IR-Link

- Bug known to exist for 10 years
- Ill-described:
  2.800 loc +
  3 flowchart +
  1 B&O eng.
- 3 months for modeling.
- UPPAAL detects error with 1.998 transition steps (shortest)
- Error trace was confirmed in B&O laboratory.
- Error corrected and verified in UPPAAL.
- Follow-up project.

Arne Skou, Klaus Havelund

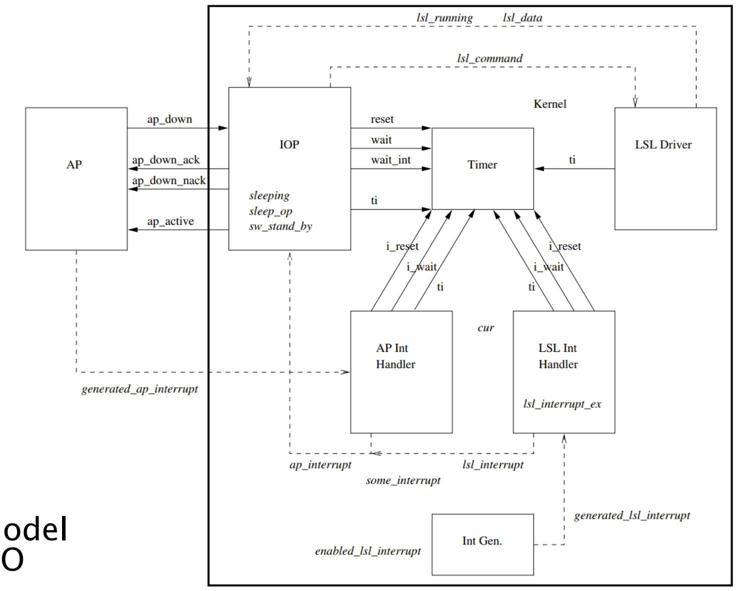
CPSIoT21

Kim Larsen [20]

Bang & Olufsen [1999]

Power-Down Control

- **Power down/up without loosing data**
- Week 1
  - Intense collaboration on a sketch of a model
- Week 2 & 3
  - Model Completion
  - Property Formulation
  - Model Checking
- Week 4
  - Report writing
- Findings
  - 3 bugs where found during development and simulation
  - A timing error was found during model checking resulting in change of B&O design

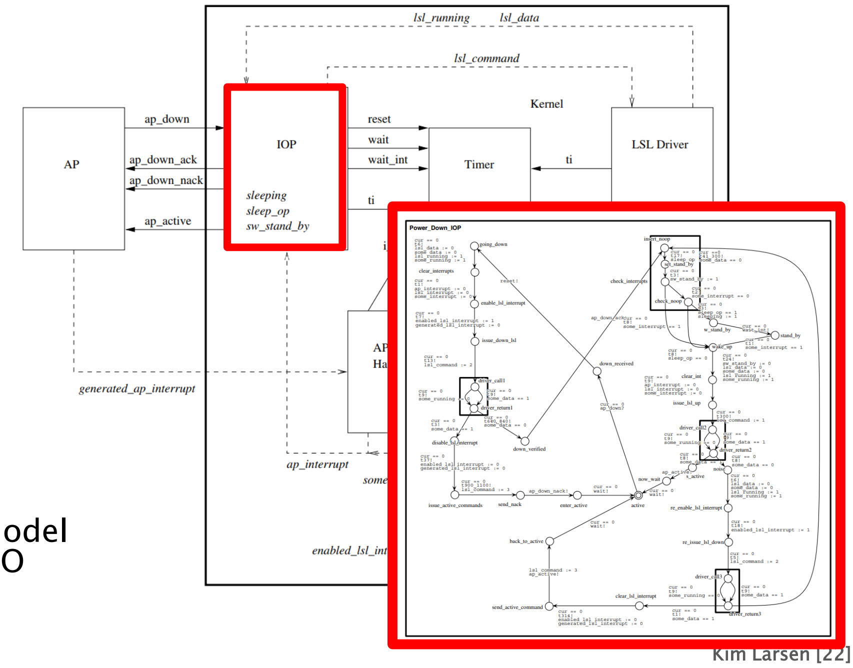


Bang & Olufsen [1999]
Power–Down Control

- **Power down/up without loosing data**

- Week 1
  - Intense collaboration on a sketch of a model
- Week 2 & 3
  - Model Completion
  - Property Formulation
  - Model Checking
- Week 4
  - Report writing

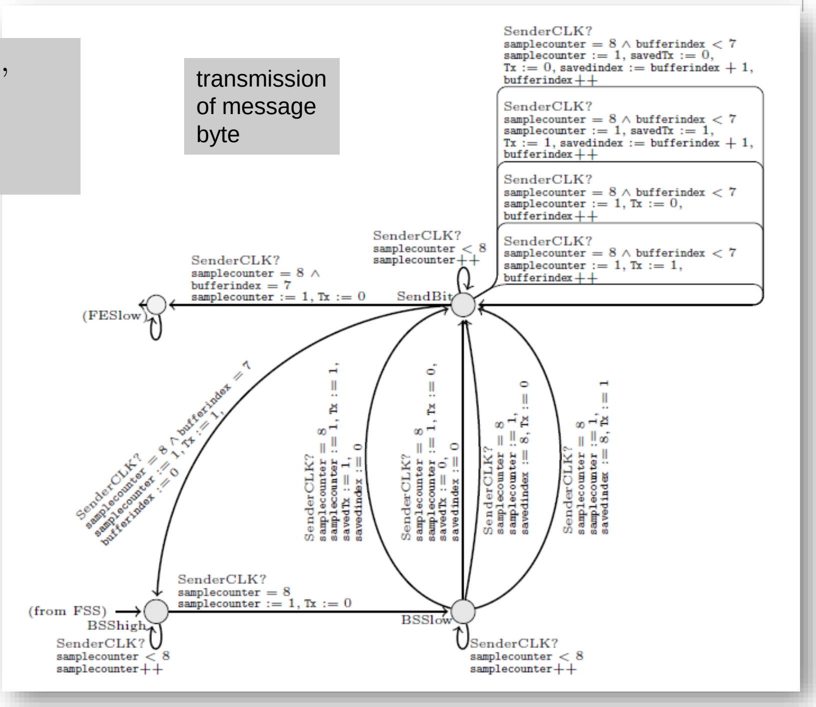
- Findings
  - 3 bugs where found during development and simulation
  - A timing error was found during model checking resulting in change of B&O design



FlexRay

BMW, Bosch, Daimler, Freescale, General Motors, NXP Semiconductors, and Volkswagen

Fault-tolerance
Timed hardware model
Parameterized error models
(glitches, jitter)
Voting & bit-clock alignment


transmission of message byte

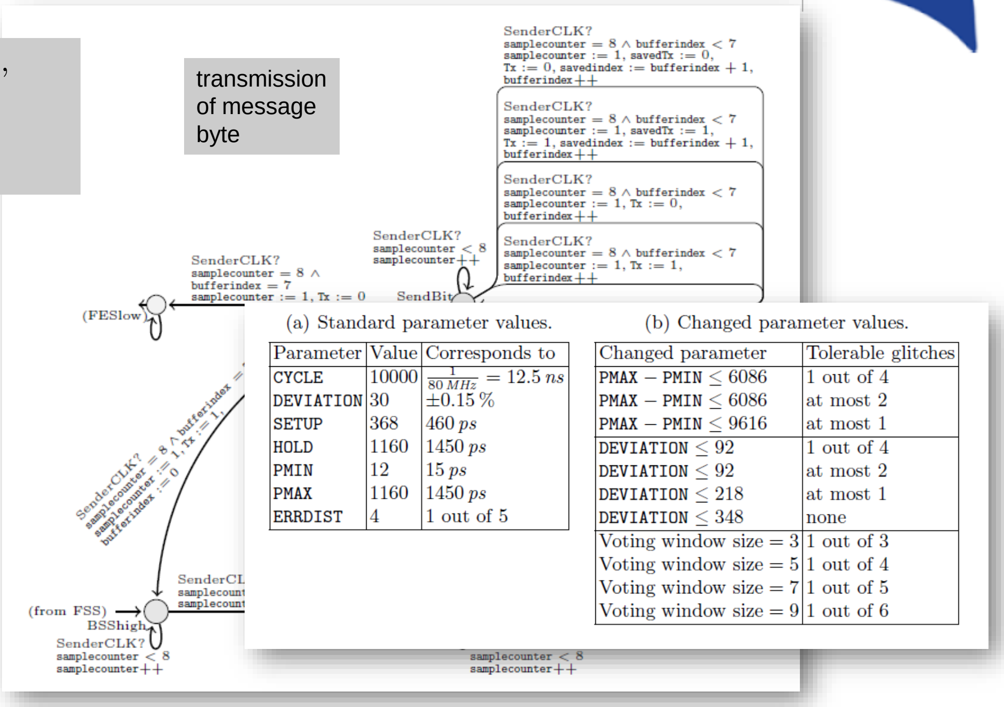
CPSIoT21

Kim Larsen [23]

FlexRay

BMW, Bosch, Daimler, Freescale, General Motors, NXP Semiconductors, and Volkswagen

Fault-tolerance
Timed hardware model
Parameterized error models
(glitches, jitter)
Voting & bit-clock alignment


SenderCLK?
samplecounter = 8 ∧ bufferindex < 7
samplecounter := 1, savedTx := 0,
Tx := 0, savedindex := bufferindex + 1,
bufferindex++
SenderCLK?
samplecounter = 8 ∧ bufferindex < 7
samplecounter := 1, savedTx := 1,
Tx := 1, savedindex := bufferindex + 1,
bufferindex++
SenderCLK?
samplecounter = 8 ∧ bufferindex < 7
samplecounter := 1, Tx := 0,
bufferindex++
SenderCLK?
samplecounter = 8 ∧ bufferindex < 7
samplecounter := 1, Tx := 1,
bufferindex++
SenderCLK?
samplecounter < 8
samplecounter++
SendBit
SenderCLK?
samplecounter = 8 ∧
bufferindex = 7
samplecounter := 1, Tx := 0
(FESlow)
SenderCLK?
samplecounter = 8 ∧ bufferindex =
samplecounter := 1, Tx := 1,
bufferindex := 0
SenderCL
samplecount
samplecount
(from FSS)
BSShigh
SenderCLK?
samplecounter < 8
samplecounter++
samplecounter < 8
samplecounter++

transmission of message byte

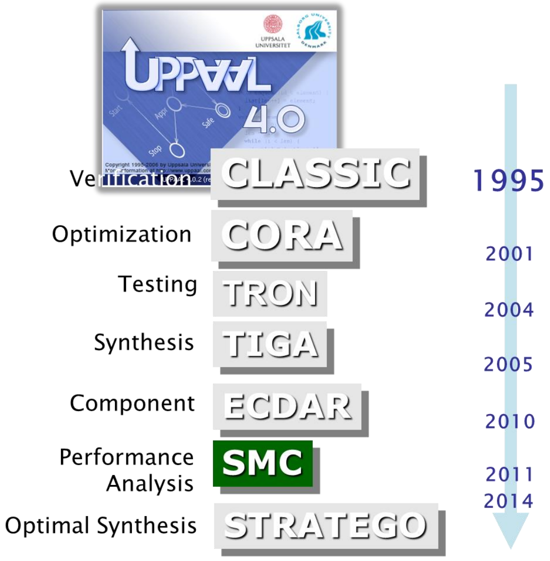
(a) Standard parameter values.

Parameter	Value	Corresponds to
CYCLE	10000	$\frac{1}{80\,MHz} = 12.5\,ns$
DEVIATION	30	$\pm 0.15\,\%$
SETUP	368	460 ps
HOLD	1160	1450 ps
PMIN	12	15 ps
PMAX	1160	1450 ps
ERRDIST	4	1 out of 5

(b) Changed parameter values.

Changed parameter	Tolerable glitches
PMAX − PMIN $\leq$ 6086	1 out of 4
PMAX − PMIN $\leq$ 6086	at most 2
PMAX − PMIN $\leq$ 9616	at most 1
DEVIATION $\leq$ 92	1 out of 4
DEVIATION $\leq$ 92	at most 2
DEVIATION $\leq$ 218	at most 1
DEVIATION $\leq$ 348	none
Voting window size = 3	1 out of 3
Voting window size = 5	1 out of 4
Voting window size = 7	1 out of 5
Voting window size = 9	1 out of 6

Performance Evaluation



UPPAAL 4.0

Verification CLASSIC

Optimization CORA

Testing TRON

Synthesis TIGA

Component ECDAR

Performance Analysis SMC

Optimal Synthesis STRATEGO

1995

2001

2004

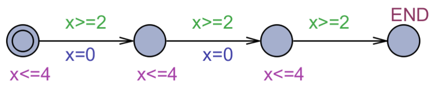
2005

2010

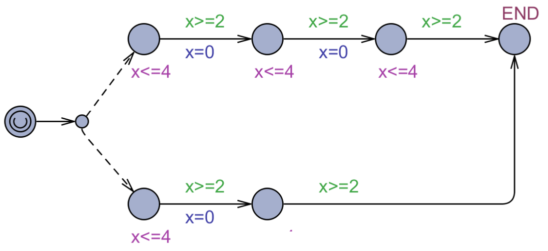
2011

2014

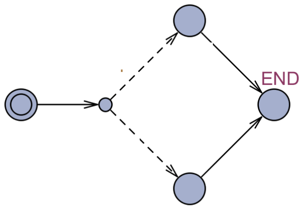
Stochastic Timed Automata



[6,12]

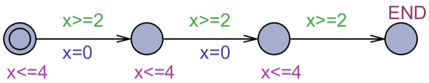


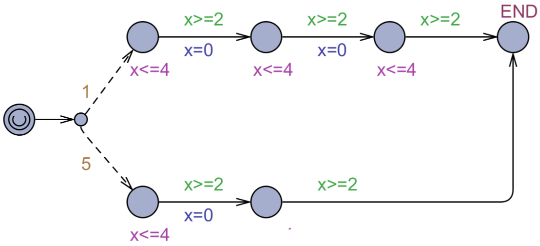
[4,12]

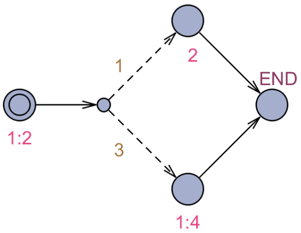


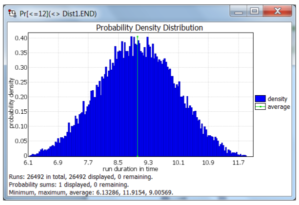
[0,∞[

Stochastic Timed Automata







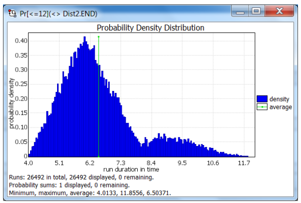


Pr[<=12](<> Dist1.END)

Probability Density Distribution

Runs: 26492 in total, 26492 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 6.13286, 11.9154, 9.00569.

$\Pr(\langle\rangle_{\leq 9}\ \mathrm{END}) = \tfrac{1}{2}$

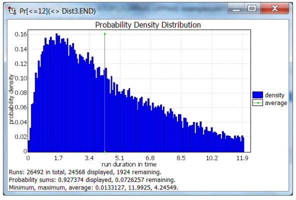


Pr[<=12](<> Dist2.END)

Probability Density Distribution

Runs: 26492 in total, 26492 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 4.0133, 11.8556, 6.50371.

$\Pr(\langle\rangle_{\leq 7}\ \mathrm{END}) \geq \tfrac{1}{2}$



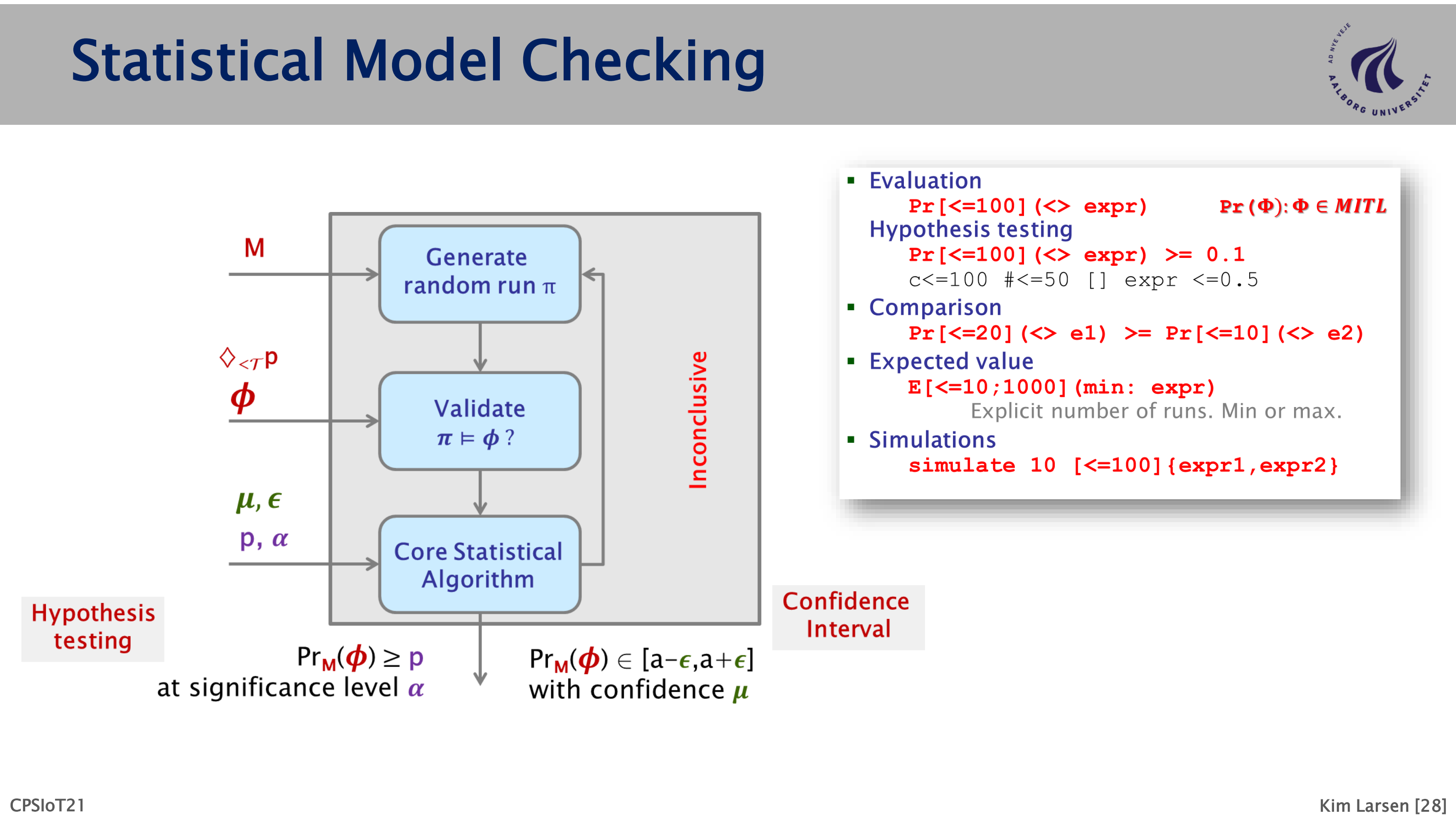
Pr[<=12](<> Dist3.END)

Probability Density Distribution

Runs: 26492 in total, 24568 displayed, 1924 remaining.
Probability sums: 0.927374 displayed, 0.0726257 remaining.
Minimum, maximum, average: 0.0133127, 11.9925, 4.24549.

Includes all Phase-Type Distributions.

Can encode any distribution with arbitrary precision.



Statistical Model Checking

M

$\Diamond_{<T}$p

ϕ

μ, ϵ

p, α

Generate random run π

Validate $\pi \vDash \phi$?

Core Statistical Algorithm

Inconclusive

Hypothesis testing

Pr$_M$(ϕ) ≥ p at significance level α

Pr$_M$(ϕ) ∈ [a−ϵ,a+ϵ] with confidence μ

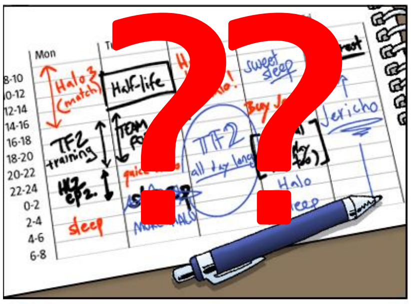
Confidence Interval

- Evaluation
  ```
  Pr[<=100](<> expr)        Pr(Φ): Φ ∈ MITL
  ```
  Hypothesis testing
  ```
  Pr[<=100](<> expr) >= 0.1
  c<=100 #<=50 [] expr <=0.5
  ```
- Comparison
  ```
  Pr[<=20](<> e1) >= Pr[<=10](<> e2)
  ```
- Expected value
  ```
  E[<=10;1000](min: expr)
  ```
  Explicit number of runs. Min or max.
- Simulations
  ```
  simulate 10 [<=100]{expr1,expr2}
  ```

CPSIoT21

Kim Larsen [28]

Schedulability & Performance Analysis



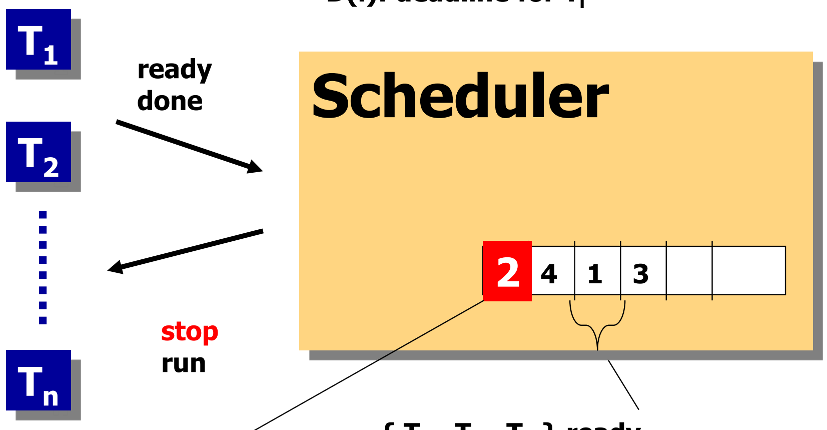
Task Scheduling

utilization of CPU

P(i), UNI[E(i), L(i)], .. : period or earliest/latest arrival or .. for T_i

C(i), UNI[BC(i),WC(i)] : execution time for T_i

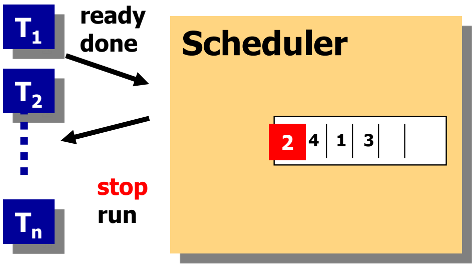
D(i): deadline for T_i

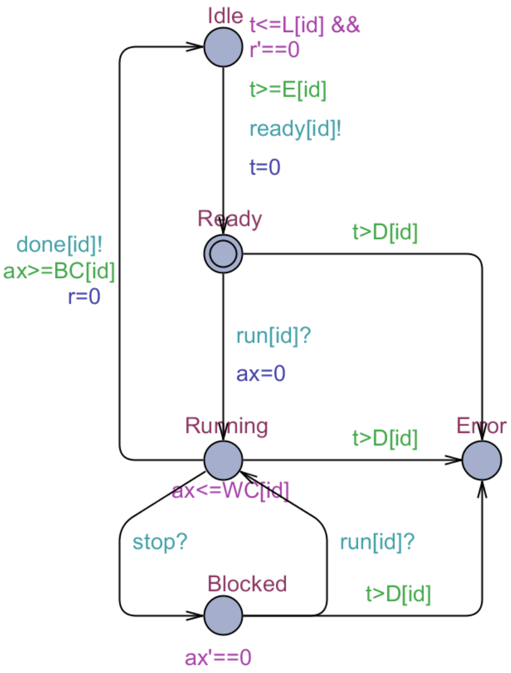


T_2 is running

{ T_4 , T_1 , T_3 } ready ordered according to some given priority: (e.g. Fixed Priority, Earliest Deadline,..)

Modeling Task

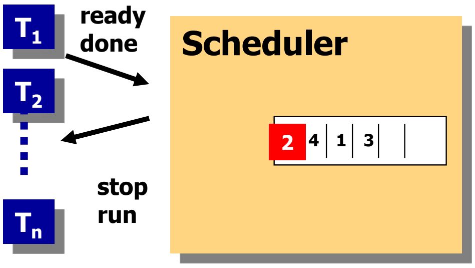


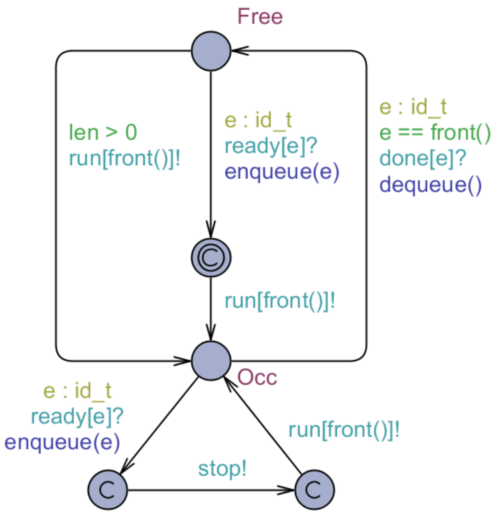


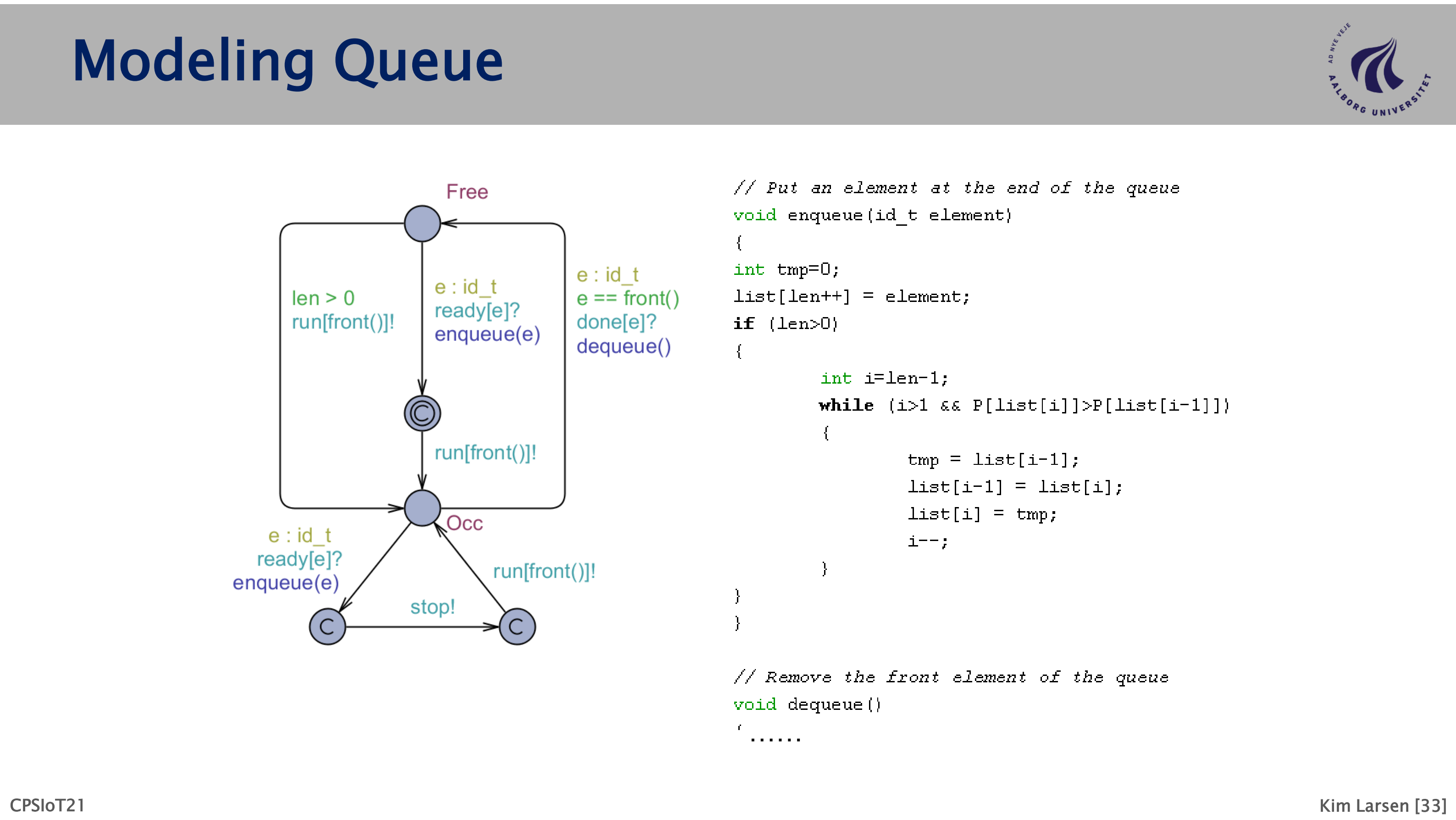
CPSIoT21

Kim Larsen [31]

Modeling Scheduler







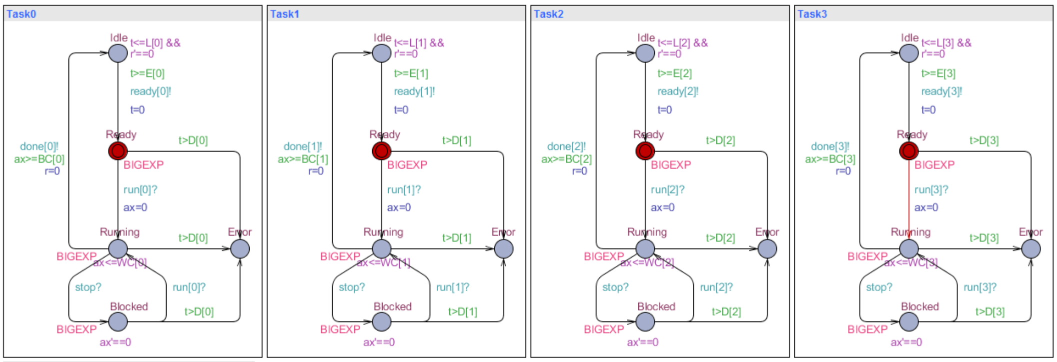
Modeling Queue

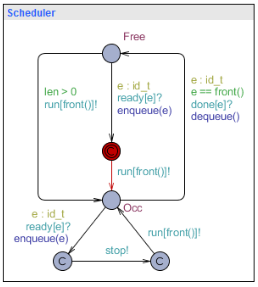
```
// Put an element at the end of the queue
void enqueue(id_t element)
{
int tmp=0;
list[len++] = element;
if (len>0)
{
        int i=len-1;
        while (i>1 && P[list[i]]>P[list[i-1]])
        {
                tmp = list[i-1];
                list[i-1] = list[i];
                list[i] = tmp;
                i--;
        }
}
}

// Remove the front element of the queue
void dequeue()
{ ......
```

CPSIoT21

Kim Larsen [33]

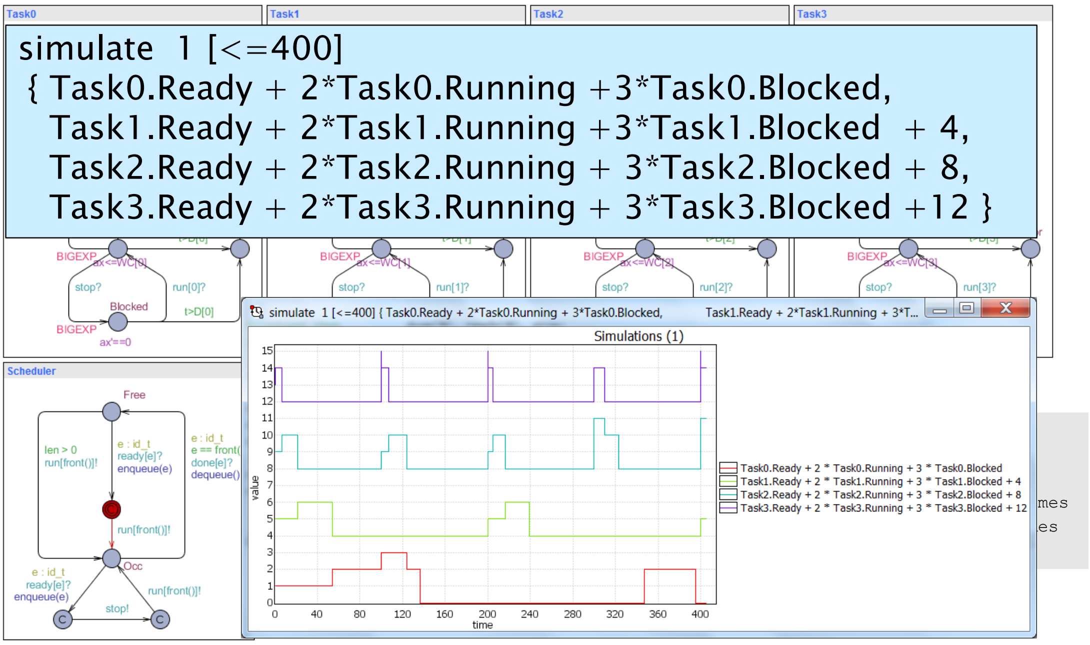
Schedulability Analysis





```
const int E[N]  = { 200, 200, 100, 100 };
const int L[N]  = { 400, 200, 100, 100 };  // Ready interval
const int D[N]  = { 400, 200, 100, 100 };  // Deadlines
const int WC[N] = {  60,  40,  20,  10 };  // Worst Computation Times
const int BC[N] = {  20,  20,  10,   5 };  // Best Computation Times
const int P[N]  = {   1,   2,   3,   4 };  // Priorities
```

Schedulability Analysis



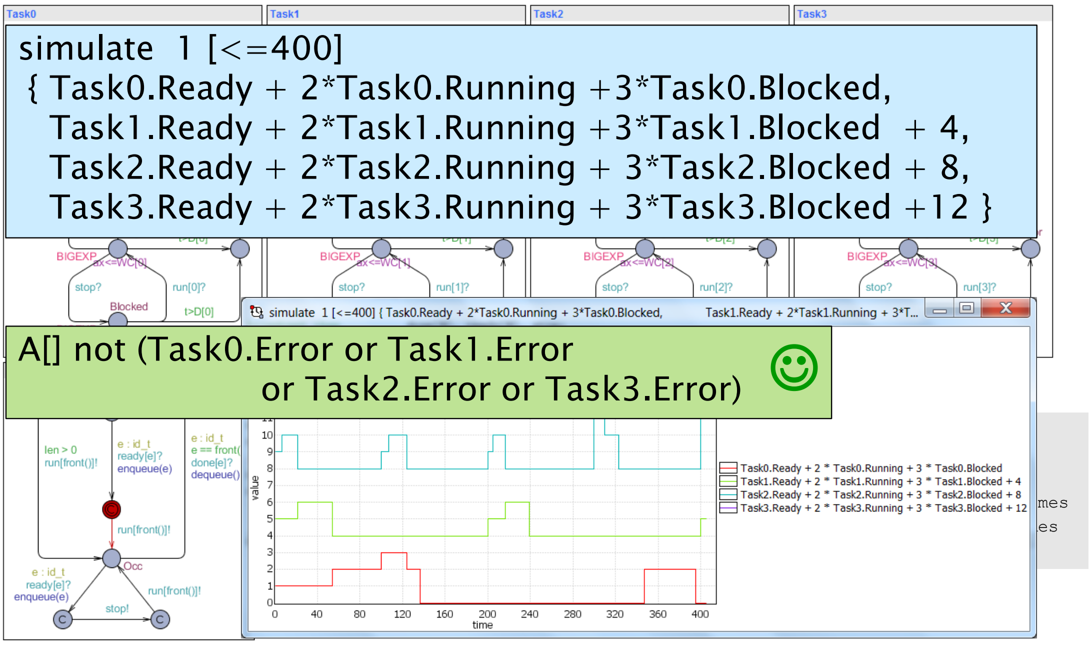
```
simulate 1 [<=400]
{ Task0.Ready + 2*Task0.Running +3*Task0.Blocked,
  Task1.Ready + 2*Task1.Running +3*Task1.Blocked  + 4,
  Task2.Ready + 2*Task2.Running + 3*Task2.Blocked + 8,
  Task3.Ready + 2*Task3.Running + 3*Task3.Blocked +12 }
```

Task0
Task1
Task2
Task3
BIGEXP
x<=WC[0]
stop?
run[0]?
Blocked
t>D[0]
x'==0
Scheduler
Free
len > 0
run[front()]!
e : id_t
ready[e]?
enqueue(e)
e == front()
done[e]?
dequeue()
Occ
stop!
simulate 1 [<=400] { Task0.Ready + 2*Task0.Running + 3*Task0.Blocked, Task1.Ready + 2*Task1.Running + 3*T...
Simulations (1)
value
time
0
40
80
120
160
200
240
280
320
360
400
Task0.Ready + 2 * Task0.Running + 3 * Task0.Blocked
Task1.Ready + 2 * Task1.Running + 3 * Task1.Blocked + 4
Task2.Ready + 2 * Task2.Running + 3 * Task2.Blocked + 8
Task3.Ready + 2 * Task3.Running + 3 * Task3.Blocked + 12

CPSIoT21

Kim Larsen [35]

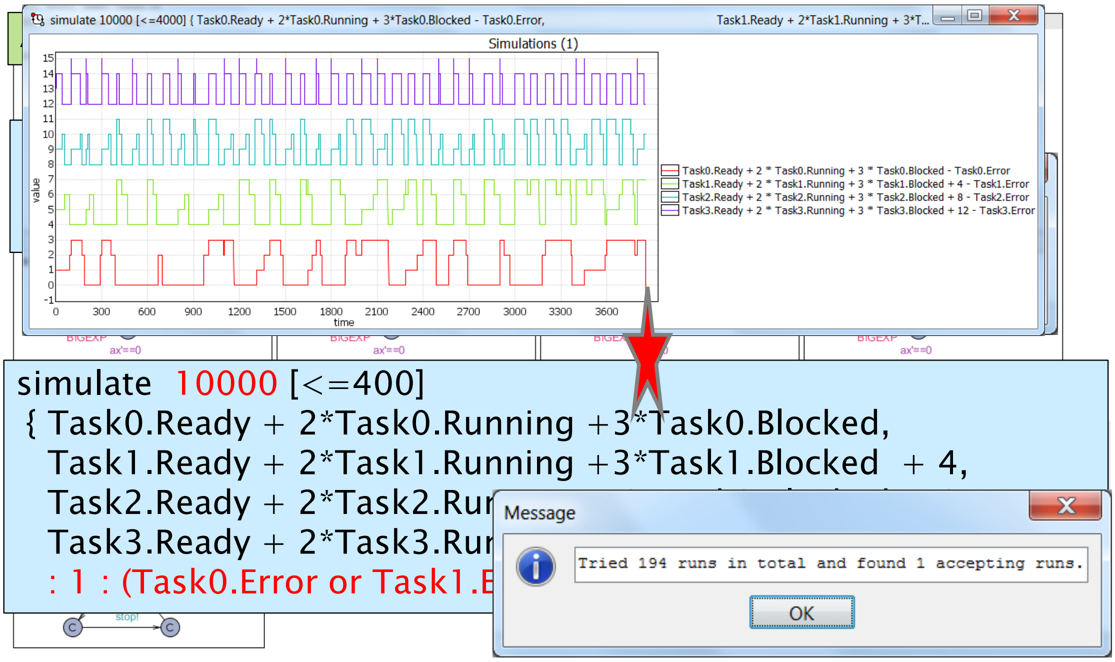
Schedulability Analysis


Task0
Task1
Task2
Task3
BIGEXP
stop?
run[0]?
run[1]?
run[2]?
run[3]?
Blocked
t>D[0]
len > 0
run[front()]!
e : id_t
ready[e]?
enqueue(e)
e == front()
done[e]?
dequeue()
Occ
stop!
C
simulate 1 [<=400] { Task0.Ready + 2*Task0.Running + 3*Task0.Blocked, Task1.Ready + 2*Task1.Running + 3*T...
value
time
0
40
80
120
160
200
240
280
320
360
400
1
2
3
4
5
6
7
8
9
10
11
Task0.Ready + 2 * Task0.Running + 3 * Task0.Blocked
Task1.Ready + 2 * Task1.Running + 3 * Task1.Blocked + 4
Task2.Ready + 2 * Task2.Running + 3 * Task2.Blocked + 8
Task3.Ready + 2 * Task3.Running + 3 * Task3.Blocked + 12
mes
es

```
simulate  1 [<=400]
 { Task0.Ready + 2*Task0.Running +3*Task0.Blocked,
   Task1.Ready + 2*Task1.Running +3*Task1.Blocked  + 4,
   Task2.Ready + 2*Task2.Running + 3*Task2.Blocked + 8,
   Task3.Ready + 2*Task3.Running + 3*Task3.Blocked +12 }
```

```
A[] not (Task0.Error or Task1.Error
                  or Task2.Error or Task3.Error)
```
☺

Schedulability Analysis


simulate 10000 [<=4000] { Task0.Ready + 2*Task0.Running + 3*Task0.Blocked - Task0.Error,
Task1.Ready + 2*Task1.Running + 3*T...
Simulations (1)
value
time
0
300
600
900
1200
1500
1800
2100
2400
2700
3000
3300
3600
-1
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
🟥 Task0.Ready + 2 * Task0.Running + 3 * Task0.Blocked - Task0.Error
🟩 Task1.Ready + 2 * Task1.Running + 3 * Task1.Blocked + 4 - Task1.Error
🟦 Task2.Ready + 2 * Task2.Running + 3 * Task2.Blocked + 8 - Task2.Error
🟪 Task3.Ready + 2 * Task3.Running + 3 * Task3.Blocked + 12 - Task3.Error
BIGEXP
ax'==0
stop!
C
OK

```
simulate  10000 [<=400]
 { Task0.Ready + 2*Task0.Running +3*Task0.Blocked,
   Task1.Ready + 2*Task1.Running +3*Task1.Blocked  + 4,
   Task2.Ready + 2*Task2.Rur
   Task3.Ready + 2*Task3.Rur
   : 1 : (Task0.Error or Task1.E
```

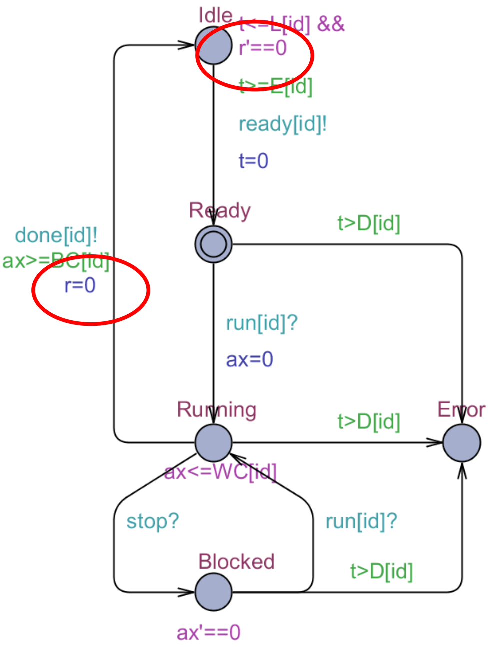
Message

Tried 194 runs in total and found 1 accepting runs.

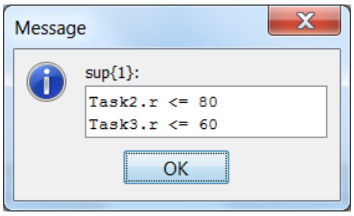
CPSIoT21

Kim Larsen [37]

Performance Analysis



sup : Task2.r, Task3.r



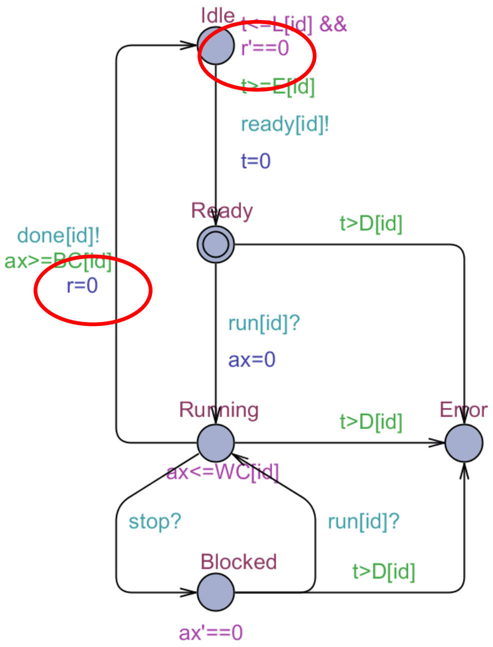
sup{1}:

```
Task2.r <= 80
Task3.r <= 60
```

CPSIoT21

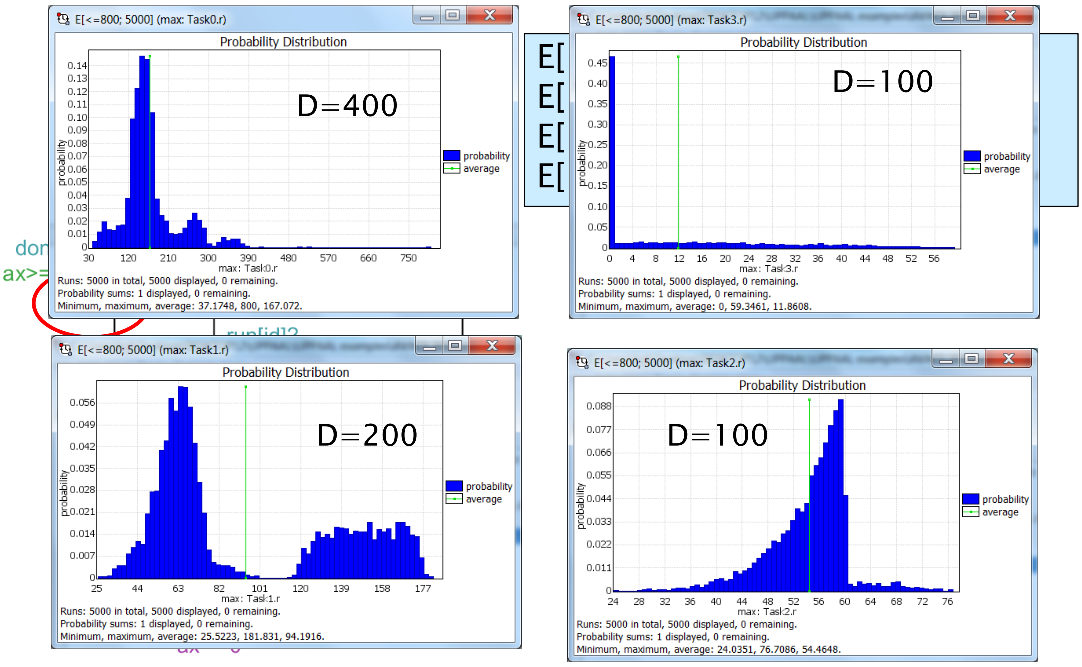
Kim Larsen [38]

Performance Analysis



E[<=800; 5000] (max: Task0.r)
E[<=800; 5000] (max: Task0.r)
E[<=800; 5000] (max: Task0.r)
E[<=800; 5000] (max: Task0.r)

Performance Analysis



E[<=800; 5000] (max: Task0.r)

Runs: 5000 in total, 5000 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 37.1748, 800, 167.072.

E[<=800; 5000] (max: Task3.r)

Runs: 5000 in total, 5000 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 0, 59.3461, 11.8608.

E[<=800; 5000] (max: Task1.r)

Runs: 5000 in total, 5000 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 25.5223, 181.831, 94.1916.

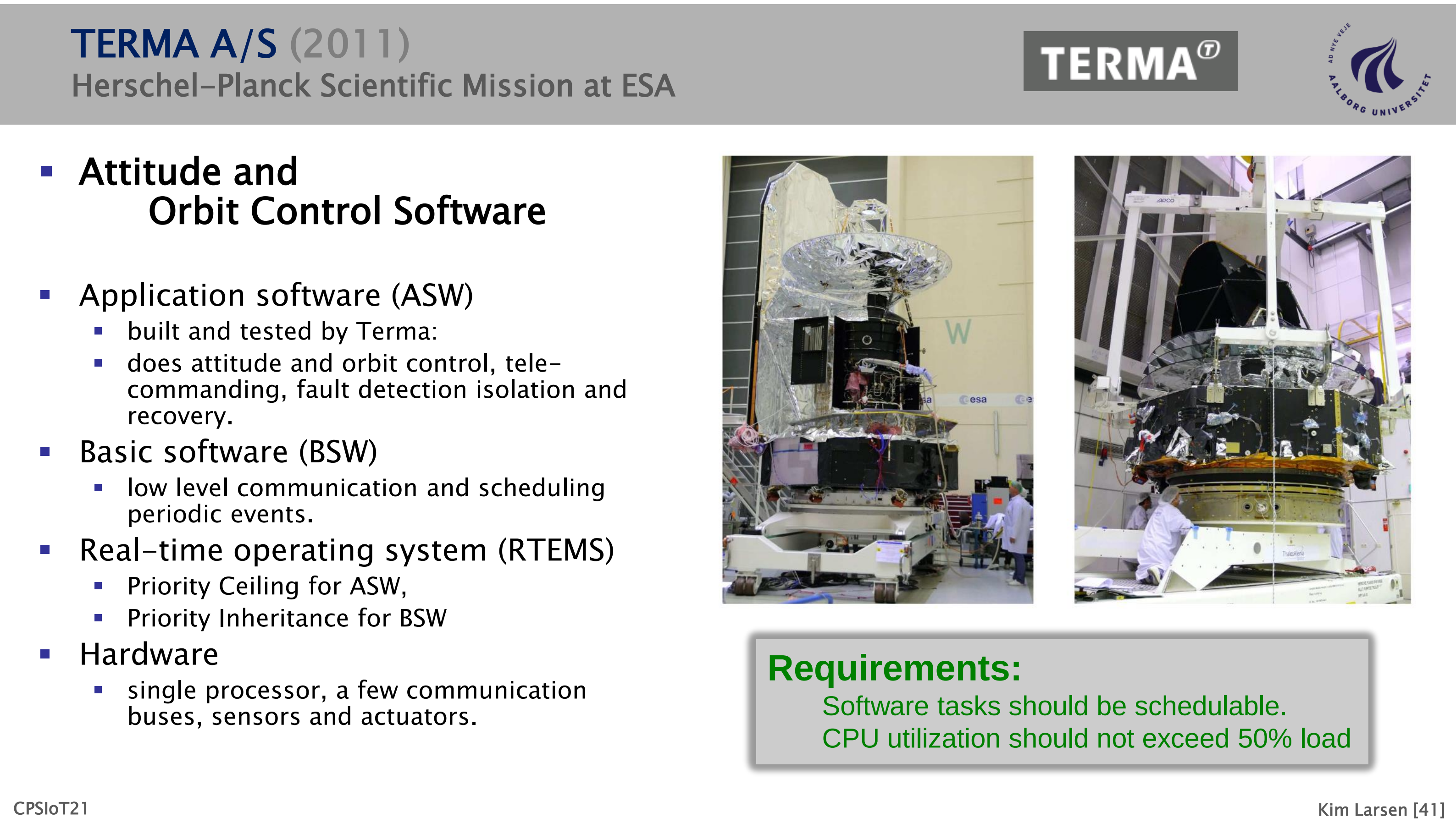
E[<=800; 5000] (max: Task2.r)

Runs: 5000 in total, 5000 displayed, 0 remaining.
Probability sums: 1 displayed, 0 remaining.
Minimum, maximum, average: 24.0351, 76.7086, 54.4648.

CPSIoT21

Kim Larsen [40]

©MECO.net



TERMA A/S (2011)
Herschel-Planck Scientific Mission at ESA

- Attitude and Orbit Control Software
- Application software (ASW)
  - built and tested by Terma:
  - does attitude and orbit control, tele-commanding, fault detection isolation and recovery.
- Basic software (BSW)
  - low level communication and scheduling periodic events.
- Real-time operating system (RTEMS)
  - Priority Ceiling for ASW,
  - Priority Inheritance for BSW
- Hardware
  - single processor, a few communication buses, sensors and actuators.

Requirements:
Software tasks should be schedulable.
CPU utilization should not exceed 50% load

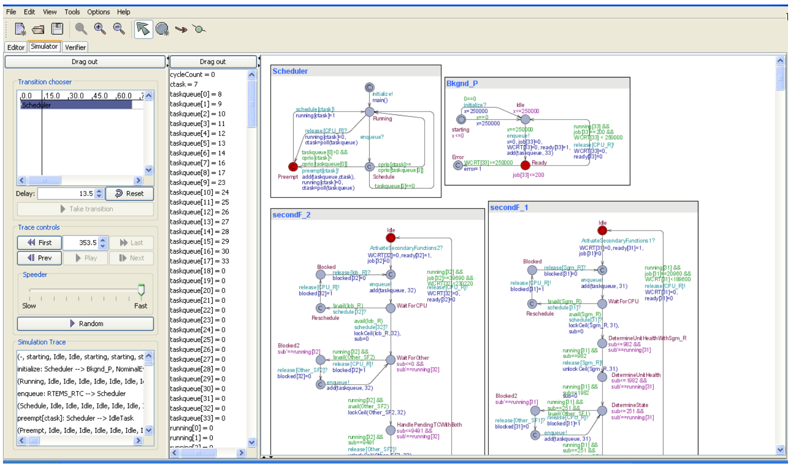
CPSIoT21

Kim Larsen [41]

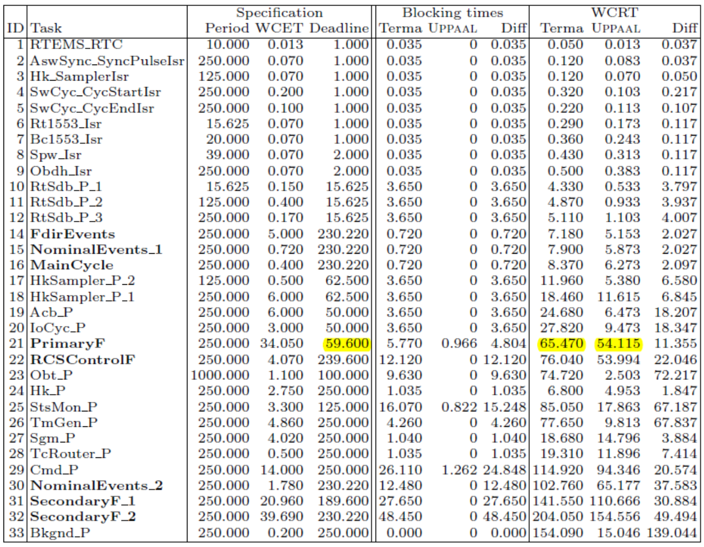
TERMA A/S (2011)

Herschel-Planck Scientific Mission at ESA

TERMA



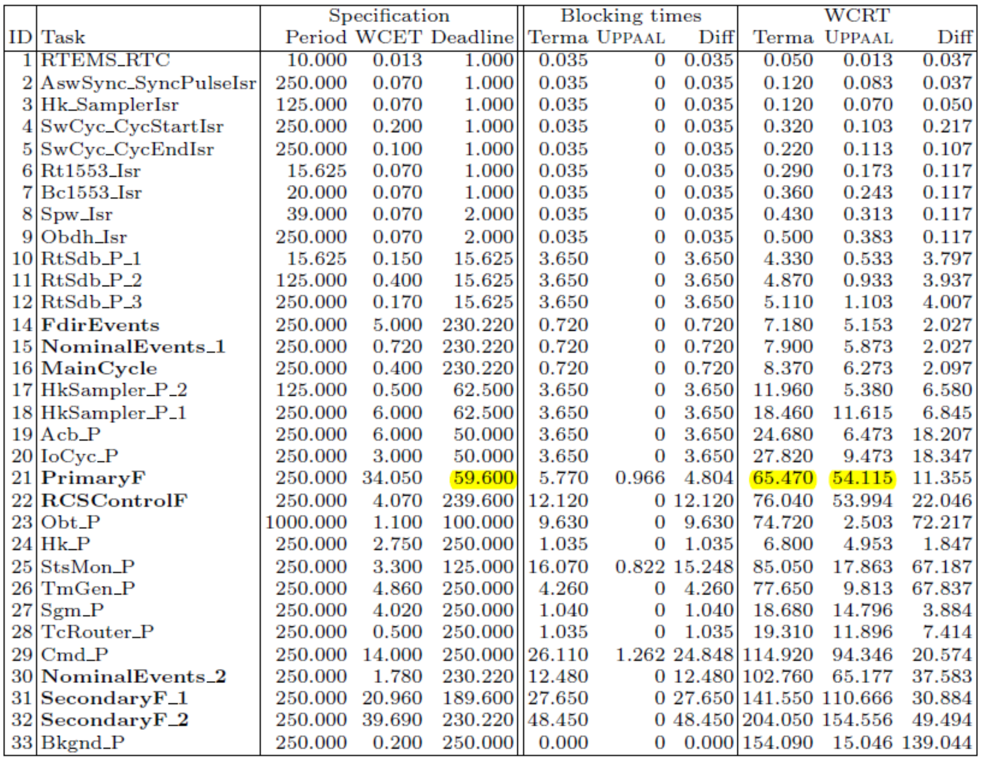
UPPAAL 4.1 Framework for Schedulability



ID	Task	Specification			Blocking times			WCRT		
		Period	WCET	Deadline	Terma	UPPAAL	Diff	Terma	UPPAAL	Diff
1	RTEMS_RTC	10.000	0.013	1.000	0.035	0	0.035	0.050	0.013	0.037
2	AswSync_SyncPulseIsr	250.000	0.070	1.000	0.035	0	0.035	0.120	0.083	0.037
3	Hk_SamplerIsr	125.000	0.070	1.000	0.035	0	0.035	0.120	0.070	0.050
4	SwCyc_CycStartIsr	250.000	0.200	1.000	0.035	0	0.035	0.320	0.103	0.217
5	SwCyc_CycEndIsr	250.000	0.100	1.000	0.035	0	0.035	0.220	0.113	0.107
6	Rt1553_Isr	15.625	0.070	1.000	0.035	0	0.035	0.290	0.173	0.117
7	Bc1553_Isr	20.000	0.070	1.000	0.035	0	0.035	0.360	0.243	0.117
8	Spw_Isr	39.000	0.070	2.000	0.035	0	0.035	0.430	0.313	0.117
9	Obdh_Isr	250.000	0.070	2.000	0.035	0	0.035	0.500	0.383	0.117
10	RtSdb_P_1	15.625	0.150	15.625	3.650	0	3.650	4.330	0.533	3.797
11	RtSdb_P_2	125.000	0.400	15.625	3.650	0	3.650	4.870	0.933	3.937
12	RtSdb_P_3	250.000	0.170	15.625	3.650	0	3.650	5.110	1.103	4.007
14	**FdirEvents**	250.000	5.000	230.220	0.720	0	0.720	7.180	5.153	2.027
15	**NominalEvents_1**	250.000	0.720	230.220	0.720	0	0.720	7.900	5.873	2.027
16	**MainCycle**	250.000	0.400	230.220	0.720	0	0.720	8.370	6.273	2.097
17	HkSampler_P_2	125.000	0.500	62.500	3.650	0	3.650	11.960	5.380	6.580
18	HkSampler_P_1	250.000	6.000	62.500	3.650	0	3.650	18.460	11.615	6.845
19	Acb_P	250.000	6.000	50.000	3.650	0	3.650	24.680	6.473	18.207
20	IoCyc_P	250.000	3.000	50.000	3.650	0	3.650	27.820	9.473	18.347
21	**PrimaryF**	250.000	34.050	59.600	5.770	0.966	4.804	65.470	54.115	11.355
22	**RCSControlF**	250.000	4.070	239.600	12.120	0	12.120	76.040	53.994	22.046
23	Obt_P	1000.000	1.100	100.000	9.630	0	9.630	74.720	2.503	72.217
24	Hk_P	250.000	2.750	250.000	1.035	0	1.035	6.800	4.953	1.847
25	StsMon_P	250.000	3.300	125.000	16.070	0.822	15.248	85.050	17.863	67.187
26	TmGen_P	250.000	4.860	250.000	4.260	0	4.260	77.650	9.813	67.837
27	Sgm_P	250.000	4.020	250.000	1.040	0	1.040	18.680	14.796	3.884
28	TcRouter_P	250.000	0.500	250.000	1.035	0	1.035	19.310	11.896	7.414
29	Cmd_P	250.000	14.000	250.000	26.110	1.262	24.848	114.920	94.346	20.574
30	**NominalEvents_2**	250.000	1.780	230.220	12.480	0	12.480	102.760	65.177	37.583
31	**SecondaryF_1**	250.000	20.960	189.600	27.650	0	27.650	141.550	110.666	30.884
32	**SecondaryF_2**	250.000	39.690	230.220	48.450	0	48.450	204.050	154.556	49.494
33	Bkgnd_P	250.000	0.200	250.000	0.000	0	0.000	154.090	15.046	139.044

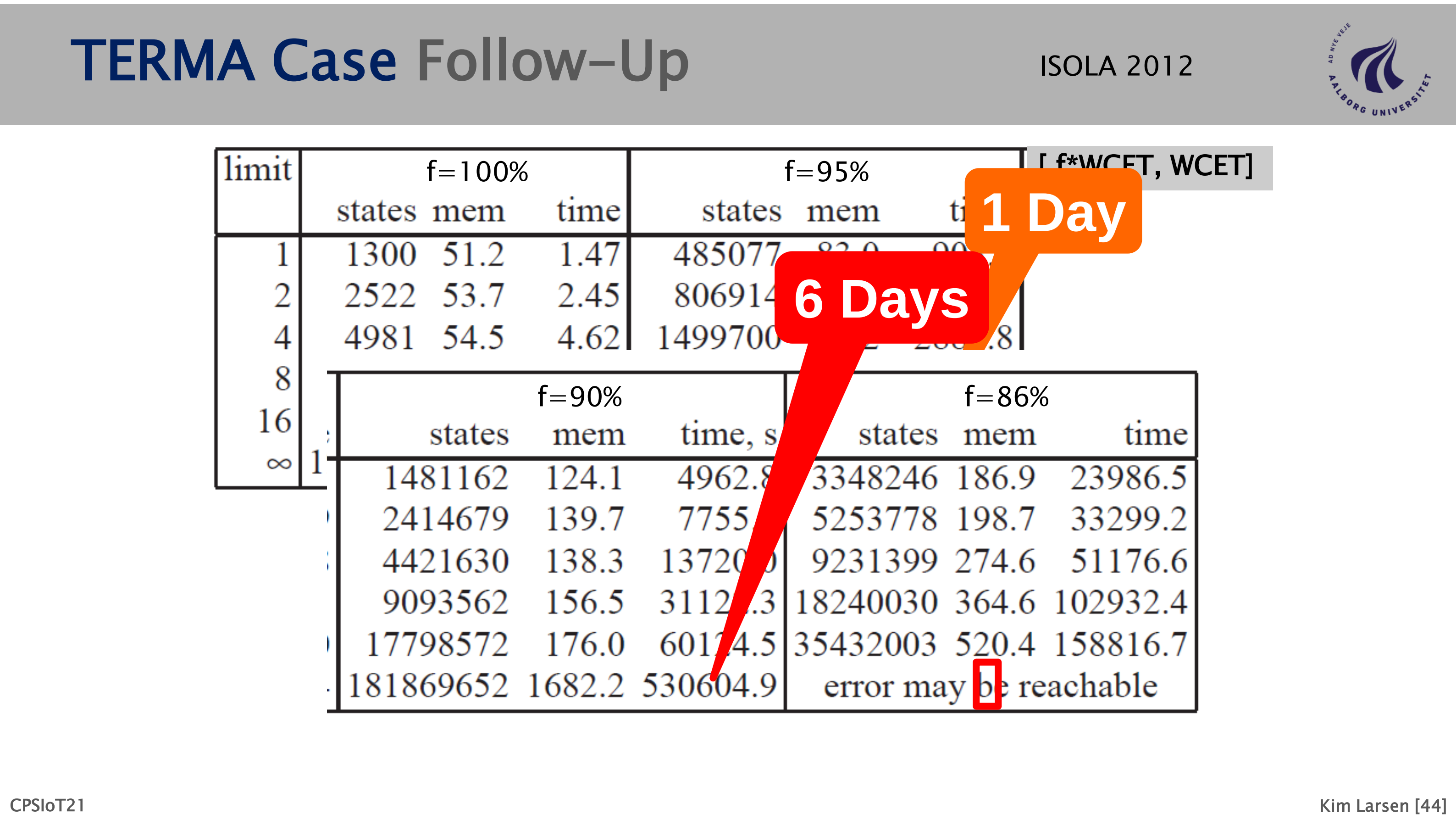
Depending on WCET the task set is schedulable or not

Blocking & WCRT



		Specification			Blocking times			WCRT		
ID	Task	Period	WCET	Deadline	Terma	UPPAAL	Diff	Terma	UPPAAL	Diff
1	RTEMS_RTC	10.000	0.013	1.000	0.035	0	0.035	0.050	0.013	0.037
2	AswSync_SyncPulseIsr	250.000	0.070	1.000	0.035	0	0.035	0.120	0.083	0.037
3	Hk_SamplerIsr	125.000	0.070	1.000	0.035	0	0.035	0.120	0.070	0.050
4	SwCyc_CycStartIsr	250.000	0.200	1.000	0.035	0	0.035	0.320	0.103	0.217
5	SwCyc_CycEndIsr	250.000	0.100	1.000	0.035	0	0.035	0.220	0.113	0.107
6	Rt1553_Isr	15.625	0.070	1.000	0.035	0	0.035	0.290	0.173	0.117
7	Bc1553_Isr	20.000	0.070	1.000	0.035	0	0.035	0.360	0.243	0.117
8	Spw_Isr	39.000	0.070	2.000	0.035	0	0.035	0.430	0.313	0.117
9	Obdh_Isr	250.000	0.070	2.000	0.035	0	0.035	0.500	0.383	0.117
10	RtSdb_P_1	15.625	0.150	15.625	3.650	0	3.650	4.330	0.533	3.797
11	RtSdb_P_2	125.000	0.400	15.625	3.650	0	3.650	4.870	0.933	3.937
12	RtSdb_P_3	250.000	0.170	15.625	3.650	0	3.650	5.110	1.103	4.007
14	**FdirEvents**	250.000	5.000	230.220	0.720	0	0.720	7.180	5.153	2.027
15	**NominalEvents_1**	250.000	0.720	230.220	0.720	0	0.720	7.900	5.873	2.027
16	**MainCycle**	250.000	0.400	230.220	0.720	0	0.720	8.370	6.273	2.097
17	HkSampler_P_2	125.000	0.500	62.500	3.650	0	3.650	11.960	5.380	6.580
18	HkSampler_P_1	250.000	6.000	62.500	3.650	0	3.650	18.460	11.615	6.845
19	Acb_P	250.000	6.000	50.000	3.650	0	3.650	24.680	6.473	18.207
20	IoCyc_P	250.000	3.000	50.000	3.650	0	3.650	27.820	9.473	18.347
21	**PrimaryF**	250.000	34.050	59.600	5.770	0.966	4.804	65.470	54.115	11.355
22	**RCSControlF**	250.000	4.070	239.600	12.120	0	12.120	76.040	53.994	22.046
23	Obt_P	1000.000	1.100	100.000	9.630	0	9.630	74.720	2.503	72.217
24	Hk_P	250.000	2.750	250.000	1.035	0	1.035	6.800	4.953	1.847
25	StsMon_P	250.000	3.300	125.000	16.070	0.822	15.248	85.050	17.863	67.187
26	TmGen_P	250.000	4.860	250.000	4.260	0	4.260	77.650	9.813	67.837
27	Sgm_P	250.000	4.020	250.000	1.040	0	1.040	18.680	14.796	3.884
28	TcRouter_P	250.000	0.500	250.000	1.035	0	1.035	19.310	11.896	7.414
29	Cmd_P	250.000	14.000	250.000	26.110	1.262	24.848	114.920	94.346	20.574
30	**NominalEvents_2**	250.000	1.780	230.220	12.480	0	12.480	102.760	65.177	37.583
31	**SecondaryF_1**	250.000	20.960	189.600	27.650	0	27.650	141.550	110.666	30.884
32	**SecondaryF_2**	250.000	39.690	230.220	48.450	0	48.450	204.050	154.556	49.494
33	Bkgnd_P	250.000	0.200	250.000	0.000	0	0.000	154.090	15.046	139.044

Marius Mikučionis



TERMA Case Follow-Up

ISOLA 2012

[f*WCET, WCET]

limit	f=100%			f=95%		
	states	mem	time	states	mem	ti
1	1300	51.2	1.47	485077	[illegible]	[illegible]
2	2522	53.7	2.45	806914	[illegible]	[illegible]
4	4981	54.5	4.62	1499700	[illegible]	[illegible].8
8						
16						
∞	1					

f=90%			f=86%		
states	mem	time, s	states	mem	time
1481162	124.1	4962.8	3348246	186.9	23986.5
2414679	139.7	7755.[illegible]	5253778	198.7	33299.2
4421630	138.3	1372[illegible]0	9231399	274.6	51176.6
9093562	156.5	3112[illegible].3	18240030	364.6	102932.4
17798572	176.0	601[illegible]4.5	35432003	520.4	158816.7
181869652	1682.2	530604.9	error may be reachable		

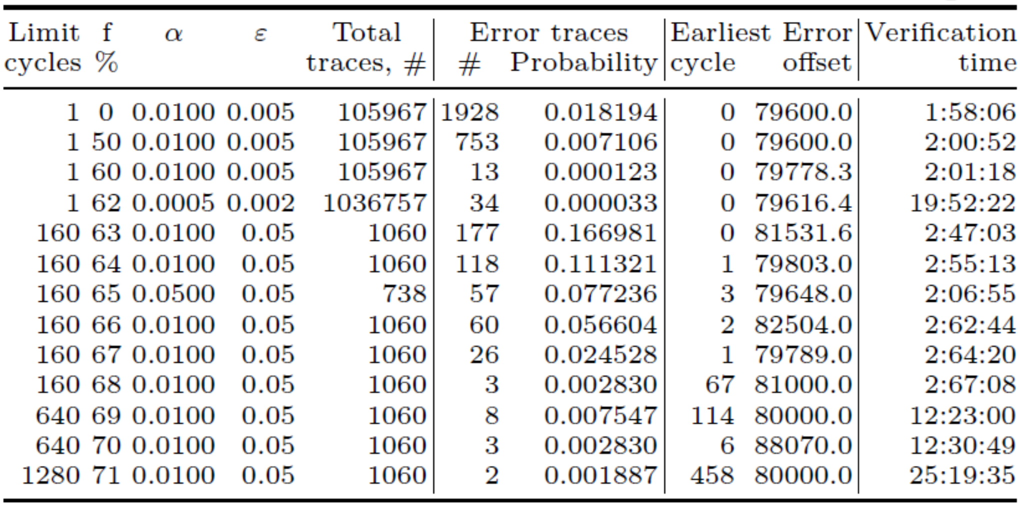
1 Day

6 Days

CPSIoT21

Kim Larsen [44]

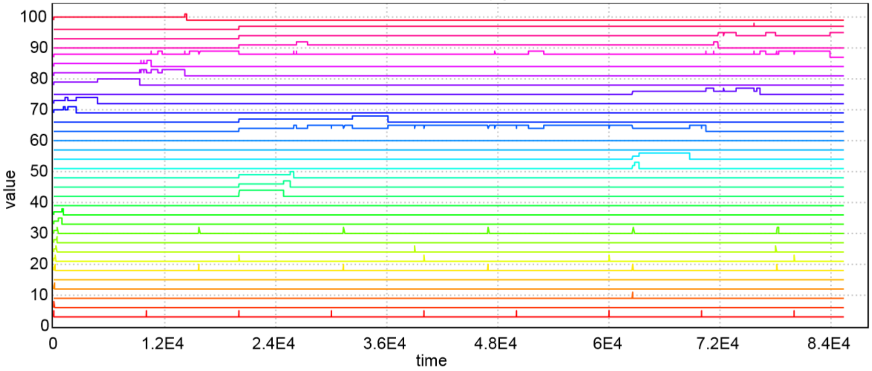
TERMA Case – Statistical MC



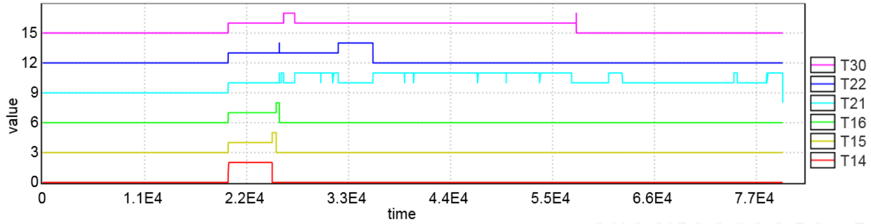
Limit cycles	f %	α	ε	Total traces, #	Error traces #	Probability	Earliest Error cycle	offset	Verification time
1	0	0.0100	0.005	105967	1928	0.018194	0	79600.0	1:58:06
1	50	0.0100	0.005	105967	753	0.007106	0	79600.0	2:00:52
1	60	0.0100	0.005	105967	13	0.000123	0	79778.3	2:01:18
1	62	0.0005	0.002	1036757	34	0.000033	0	79616.4	19:52:22
160	63	0.0100	0.05	1060	177	0.166981	0	81531.6	2:47:03
160	64	0.0100	0.05	1060	118	0.111321	1	79803.0	2:55:13
160	65	0.0500	0.05	738	57	0.077236	3	79648.0	2:06:55
160	66	0.0100	0.05	1060	60	0.056604	2	82504.0	2:62:44
160	67	0.0100	0.05	1060	26	0.024528	1	79789.0	2:64:20
160	68	0.0100	0.05	1060	3	0.002830	67	81000.0	2:67:08
640	69	0.0100	0.05	1060	8	0.007547	114	80000.0	12:23:00
640	70	0.0100	0.05	1060	3	0.002830	6	88070.0	12:30:49
1280	71	0.0100	0.05	1060	2	0.001887	458	80000.0	25:19:35

TERMA Case – Conclusion

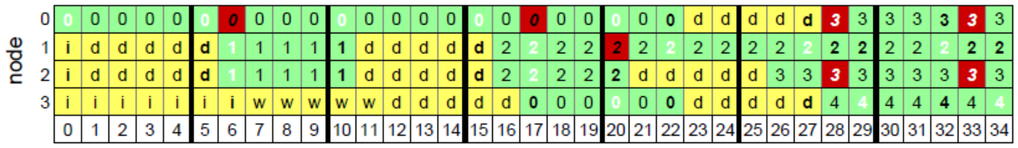
Herschel simulation run with $f = 90\%$:



Herschel deadline violation with $f = 50\%$:



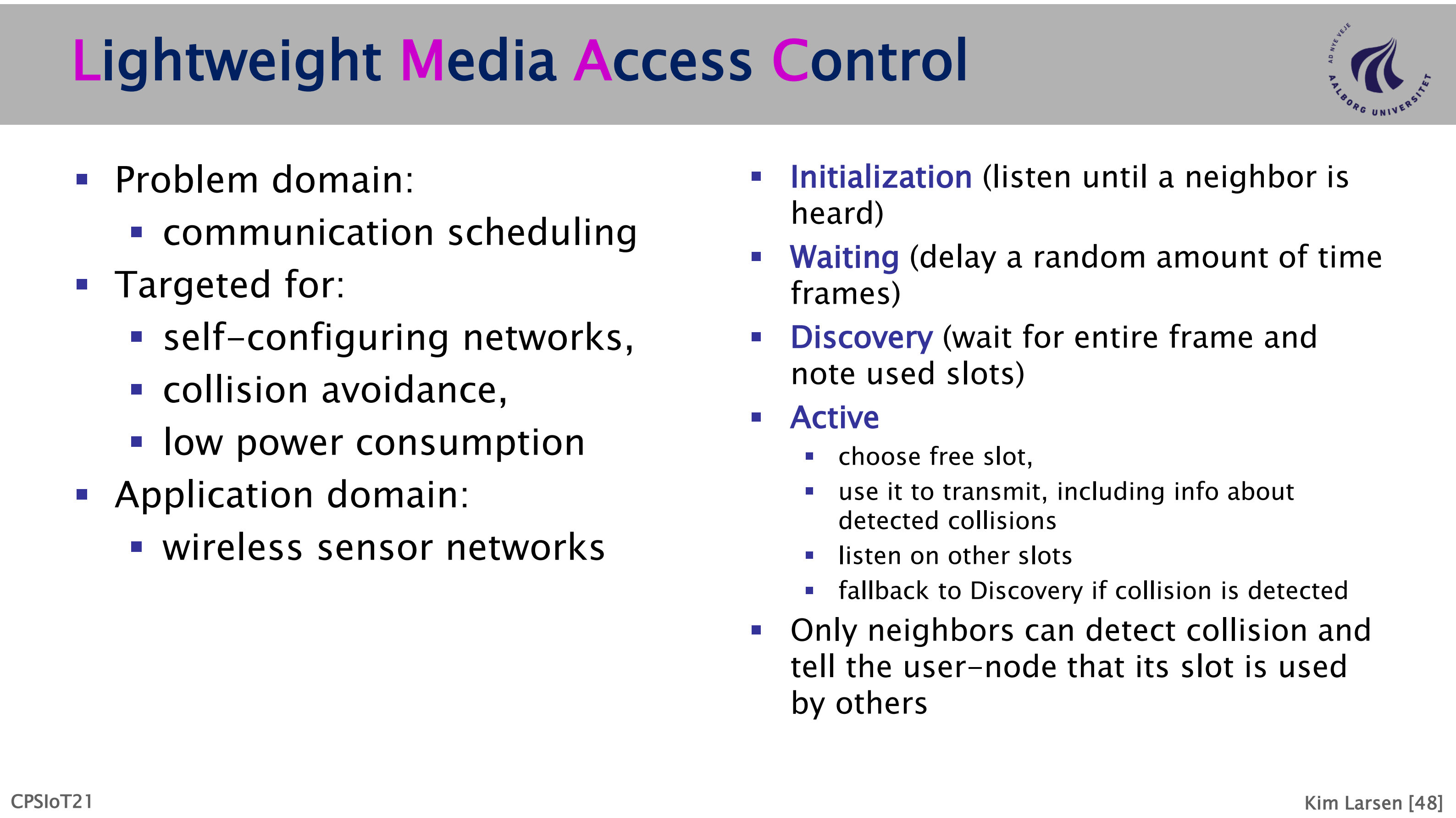
LMAC
Energy Aware Sensor Networks



node

0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	d	d	d	d	d	3	3	3	3	3	3	3
1	i	d	d	d	d	d	1	1	1	1	1	d	d	d	d	d	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
2	i	d	d	d	d	d	1	1	1	1	1	d	d	d	d	d	2	2	2	2	2	d	d	d	d	d	3	3	3	3	3	3	3	3	3
3	i	i	i	i	i	i	i	w	w	w	w	w	d	d	d	d	d	0	0	0	0	0	0	d	d	d	d	d	4	4	4	4	4	4	4
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34

A



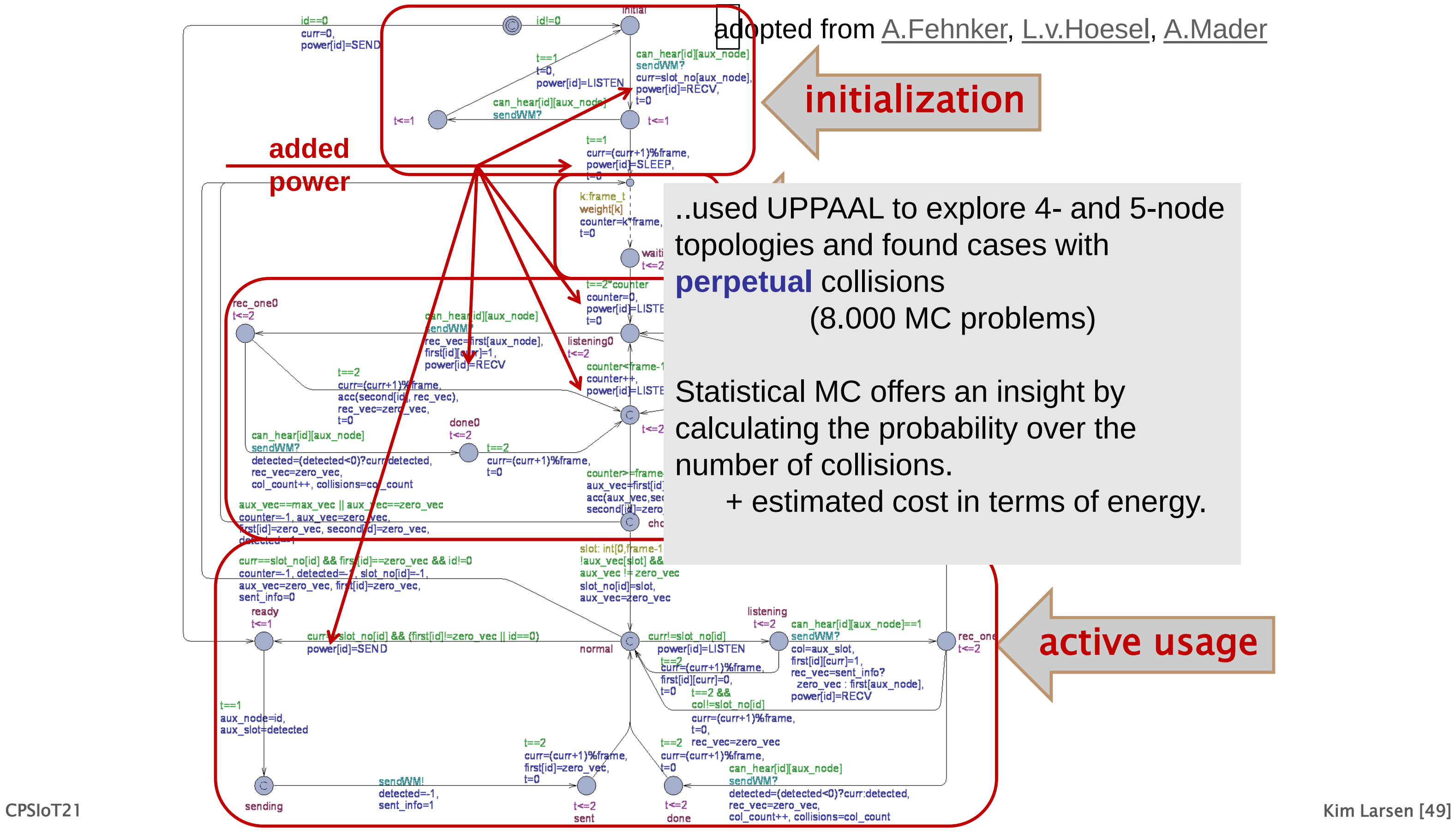
Lightweight Media Access Control

- Problem domain:
  - communication scheduling
- Targeted for:
  - self-configuring networks,
  - collision avoidance,
  - low power consumption
- Application domain:
  - wireless sensor networks

- **Initialization** (listen until a neighbor is heard)
- **Waiting** (delay a random amount of time frames)
- **Discovery** (wait for entire frame and note used slots)
- **Active**
  - choose free slot,
  - use it to transmit, including info about detected collisions
  - listen on other slots
  - fallback to Discovery if collision is detected
- Only neighbors can detect collision and tell the user-node that its slot is used by others

CPSIoT21

Kim Larsen [48]



adopted from A.Fehnker, L.v.Hoesel, A.Mader

initialization

added power

..used UPPAAL to explore 4- and 5-node topologies and found cases with **perpetual** collisions (8.000 MC problems)

Statistical MC offers an insight by calculating the probability over the number of collisions.
+ estimated cost in terms of energy.

active usage

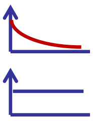
CPSIoT21

Kim Larsen [49]

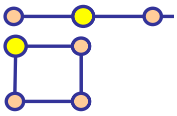
©MECO.net

SMC of LMAC with 4 Nodes

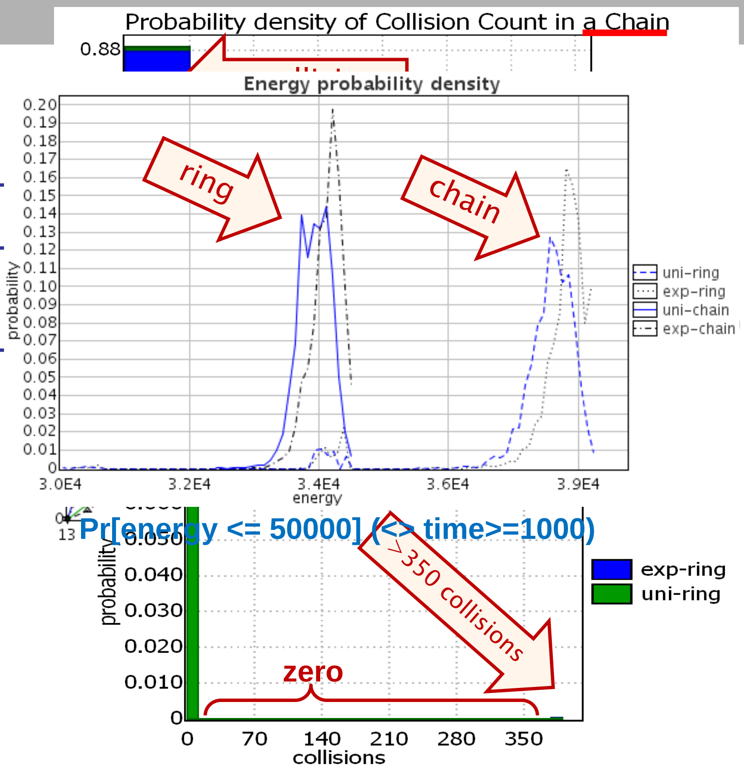
- Wait distribution:
  - geometric
  - uniform



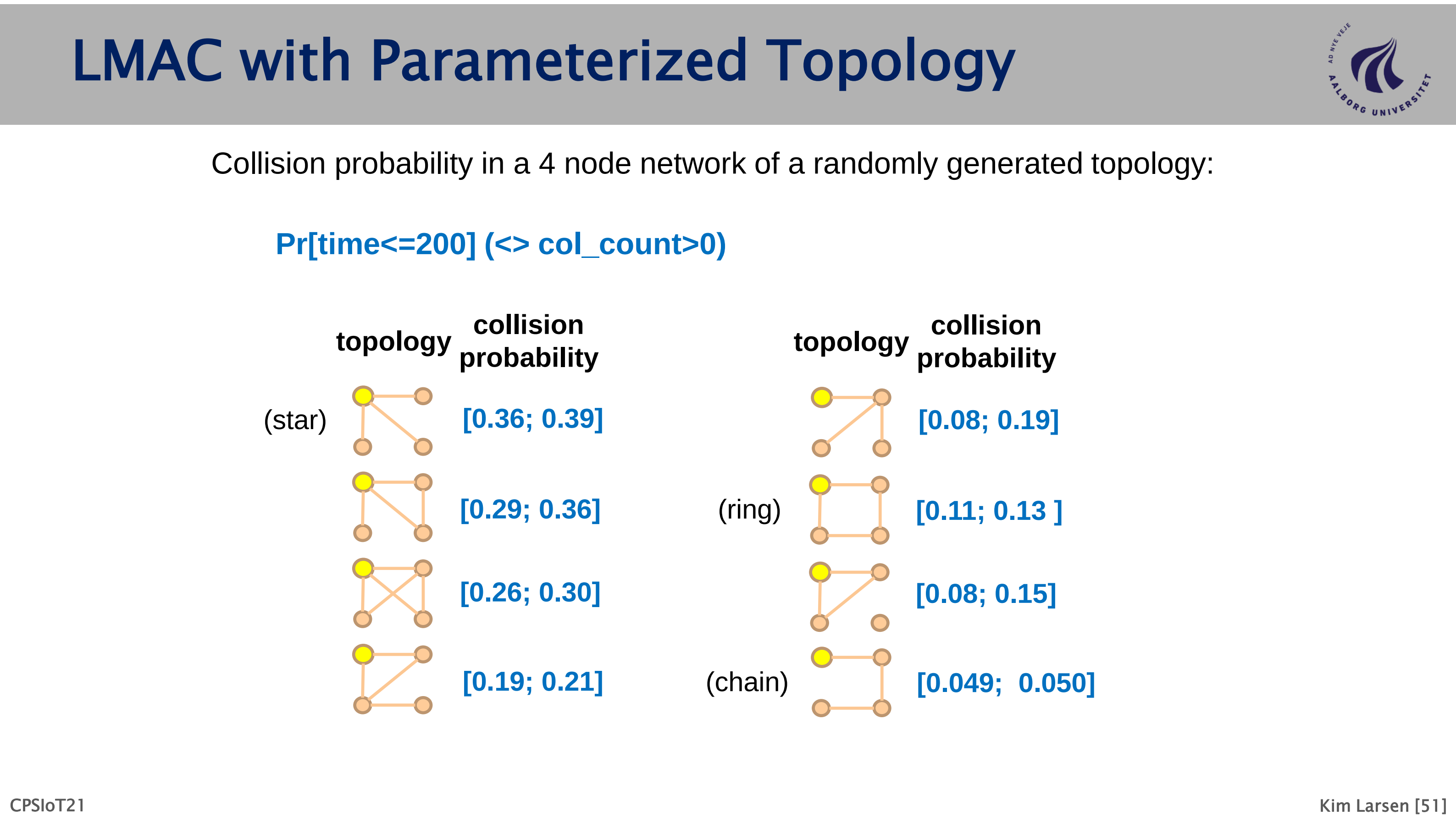
- Network topology:
  - chain
  - ring



- Collision probability
- Collision count
- Power consumption



Pr[collisions<=50000] (<> time>=1000)



LMAC with Parameterized Topology

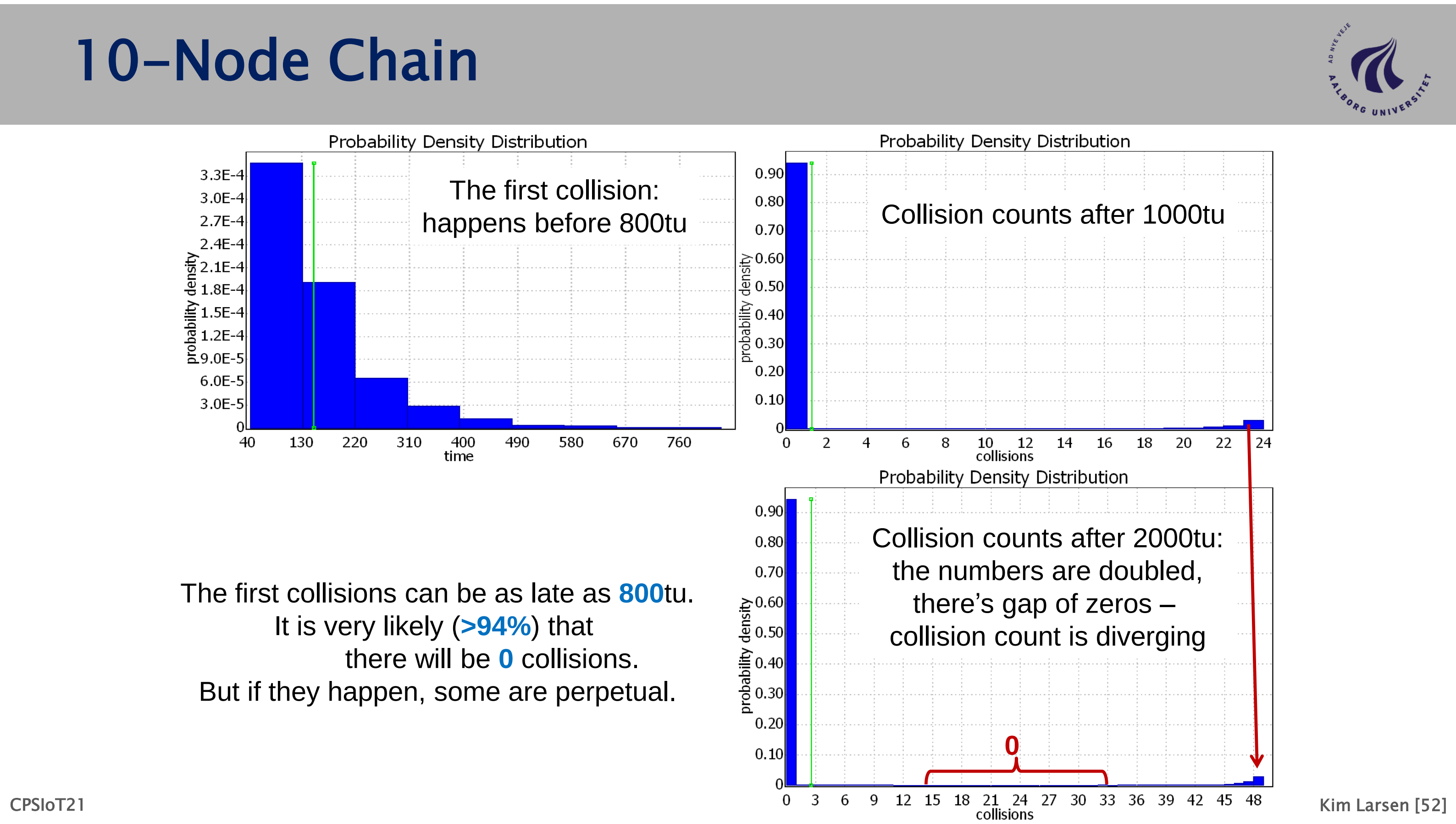
Collision probability in a 4 node network of a randomly generated topology:

Pr[time<=200] (<> col_count>0)

	topology	collision probability		topology	collision probability
(star)		[0.36; 0.39]			[0.08; 0.19]
		[0.29; 0.36]	(ring)		[0.11; 0.13]
		[0.26; 0.30]			[0.08; 0.15]
		[0.19; 0.21]	(chain)		[0.049; 0.050]

CPSIoT21

Kim Larsen [51]



10–Node Chain

The first collision: happens before 800tu

Collision counts after 1000tu

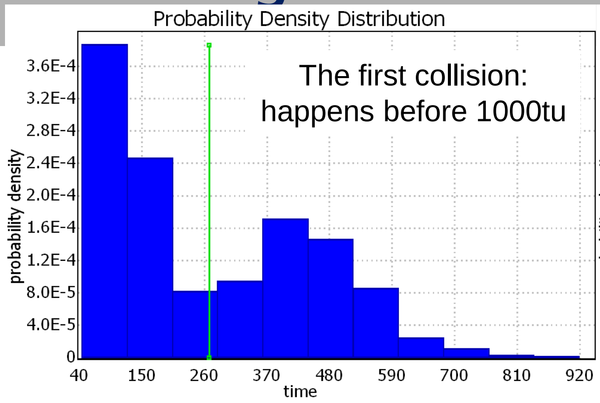
Collision counts after 2000tu: the numbers are doubled, there's gap of zeros – collision count is diverging

The first collisions can be as late as 800tu. It is very likely (>94%) that there will be 0 collisions. But if they happen, some are perpetual.

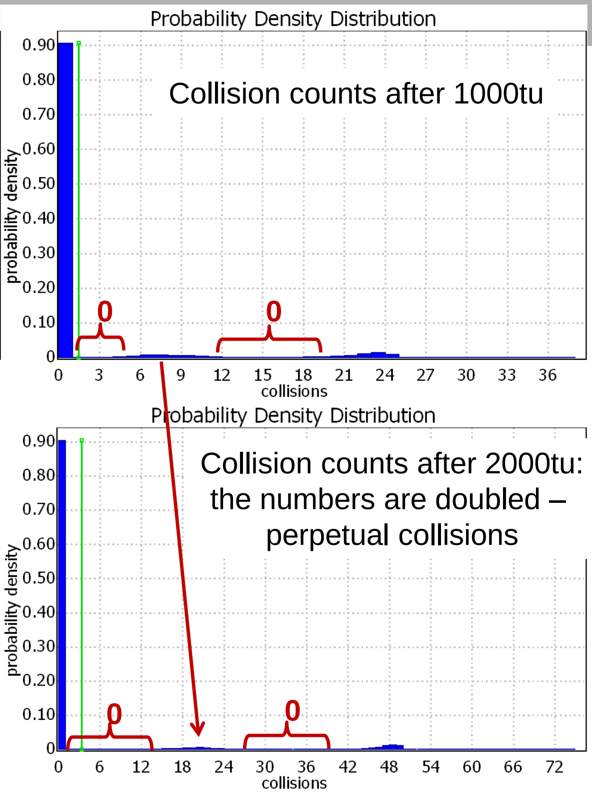
CPSIoT21

Kim Larsen [52]

10-Node Ring



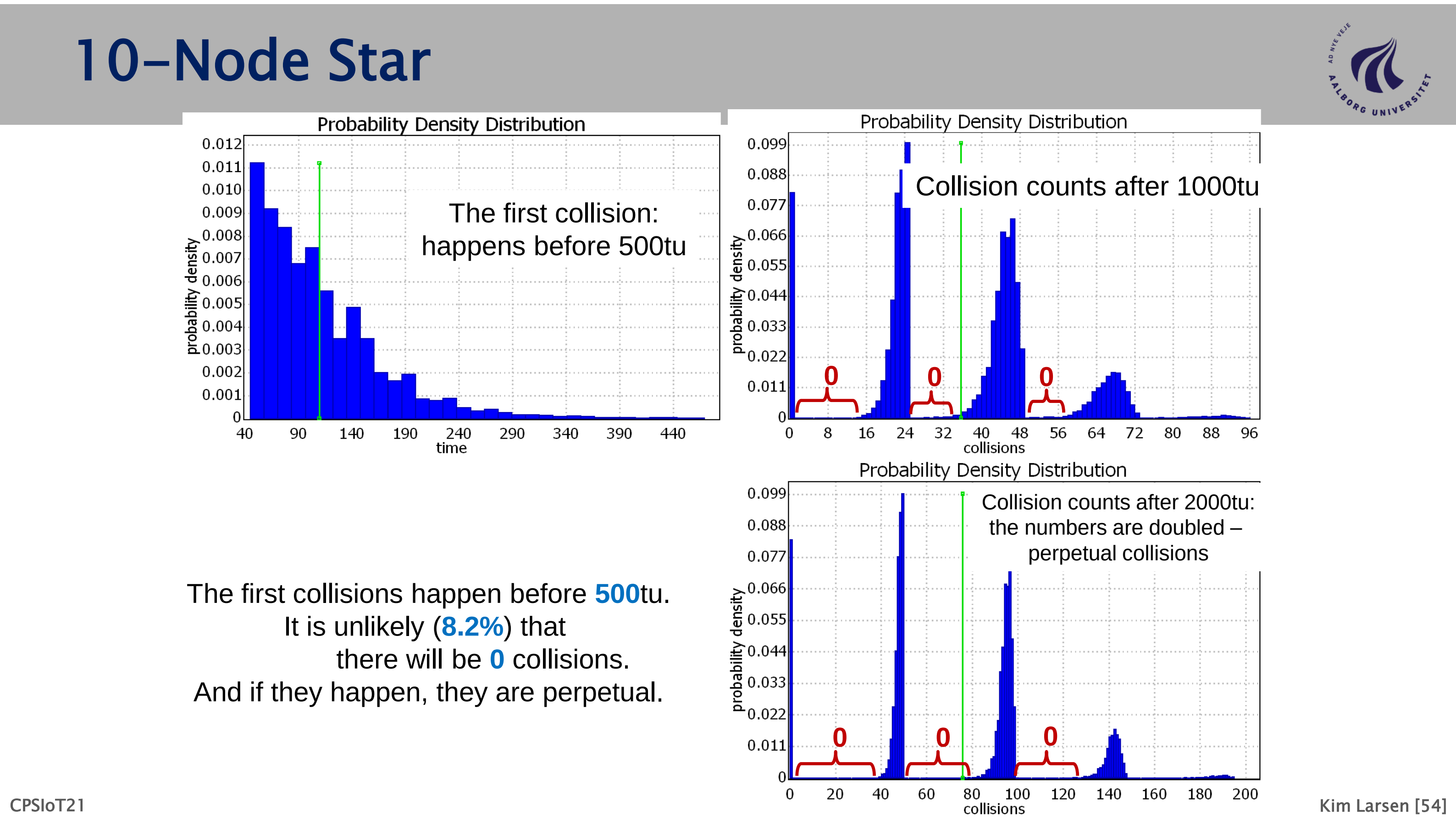
The first collision: happens before 1000tu



Collision counts after 1000tu

Collision counts after 2000tu: the numbers are doubled – perpetual collisions

The first collisions can be as late as **920**tu.
It is very likely (**>90%**) that
there will be **0** collisions.
But if they happen, they are perpetual.



10–Node Star

The first collision: happens before 500tu

Collision counts after 1000tu

Collision counts after 2000tu: the numbers are doubled – perpetual collisions

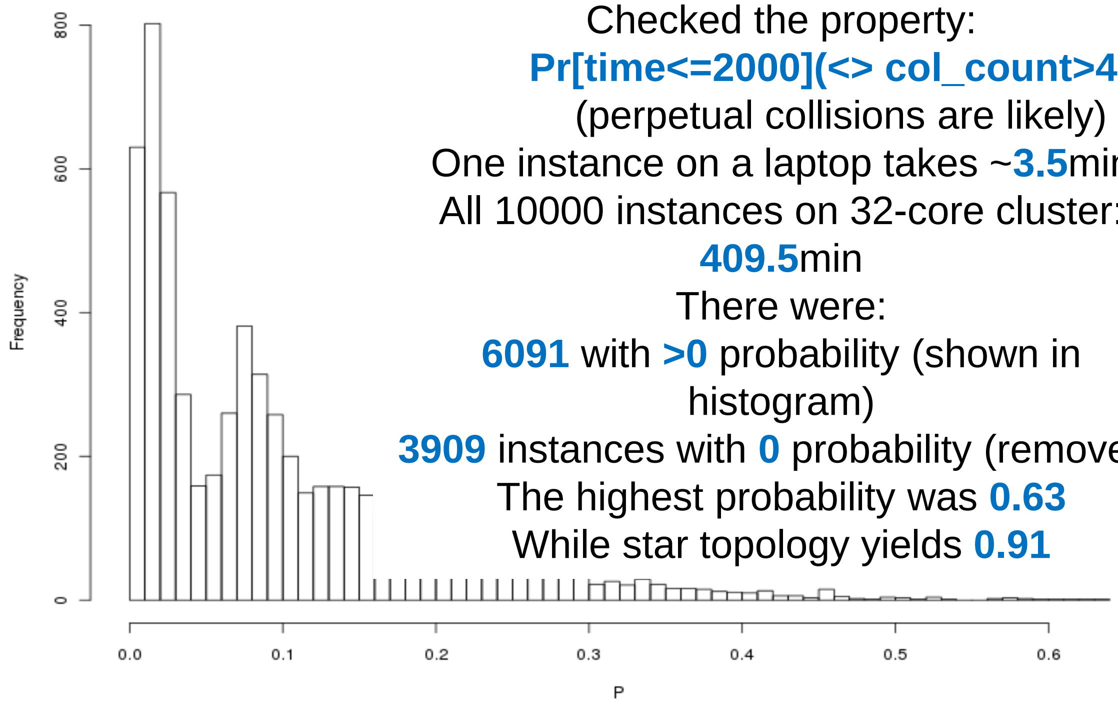
The first collisions happen before 500tu. It is unlikely (8.2%) that there will be 0 collisions. And if they happen, they are perpetual.

CPSIoT21

Kim Larsen [54]

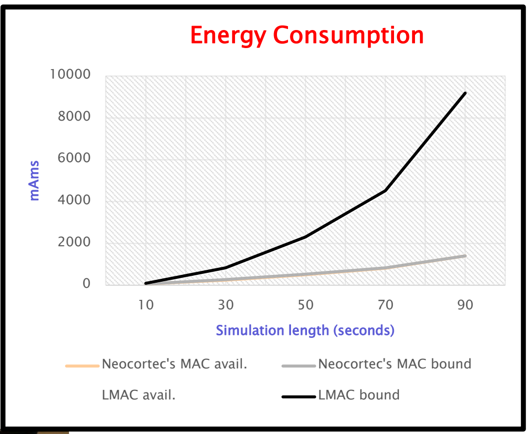
10–Node Random Topologies

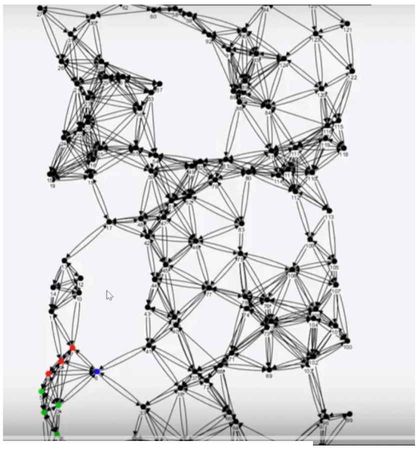
Generated **10000** random topologies
Checked the property:
Pr[time<=2000](<> col_count>42)
(perpetual collisions are likely)
One instance on a laptop takes ~**3.5**min
All 10000 instances on 32-core cluster:
409.5min
There were:
6091 with **>0** probability (shown in histogram)
3909 instances with **0** probability (removed)
The highest probability was **0.63**
While star topology yields **0.91**

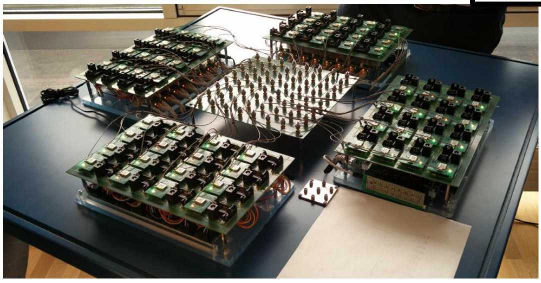


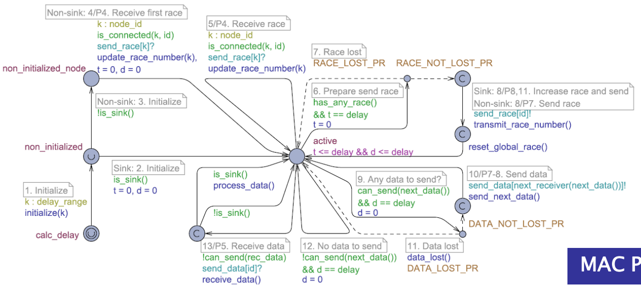
REACHI Eurostars [2018,2021]

- Energy Aware WSN
- Disaster Areaa (Red Cross)
- Modelled and analyzed using UPPAAL SMC
- NEOCORTEC
- Honeywell







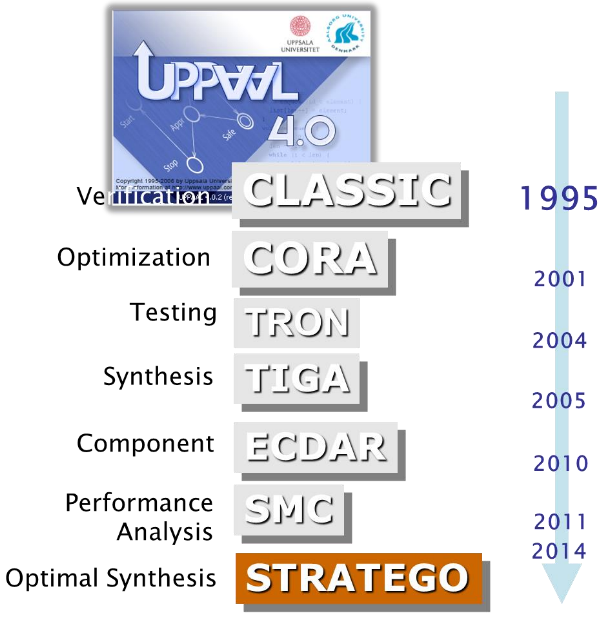


MAC Protocol

CPSIoT21 56

©MECO.net

Learning & Optimization



Verification CLASSIC 1995

Optimization CORA 2001

Testing TRON 2004

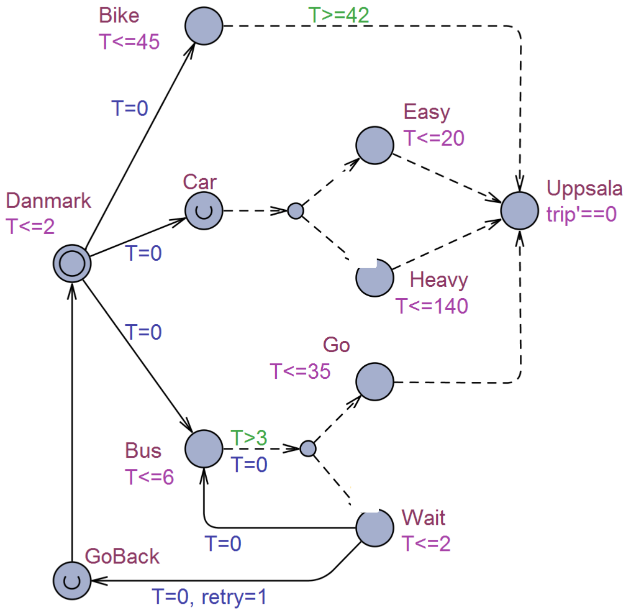
Synthesis TIGA 2005

Component ECDAR 2010

Performance Analysis SMC 2011

Optimal Synthesis STRATEGO 2014

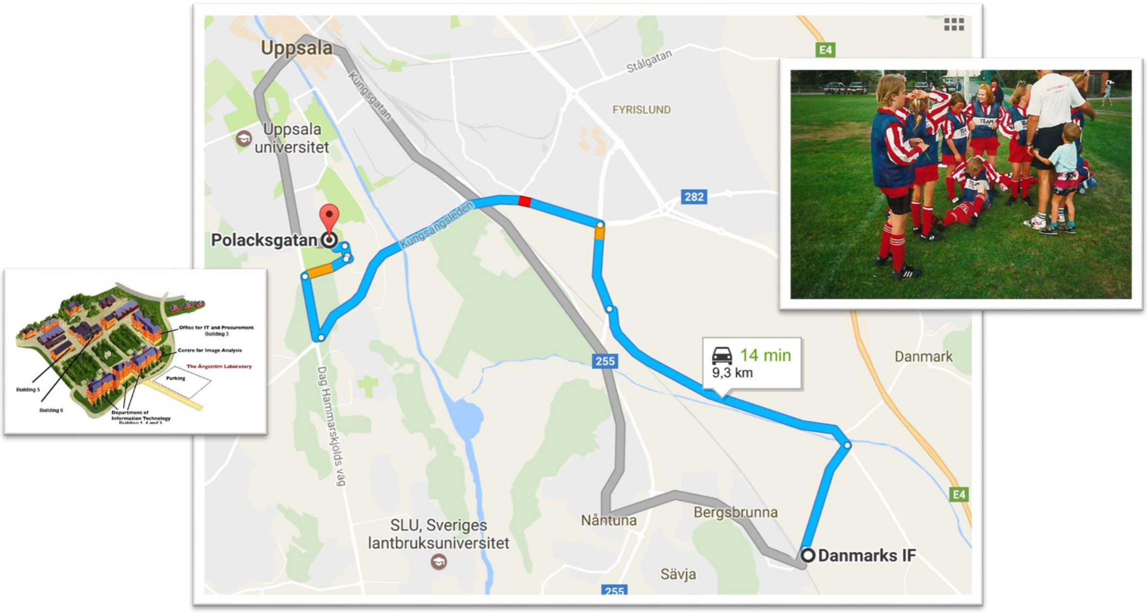
Going to Uppsala – in 1 hour



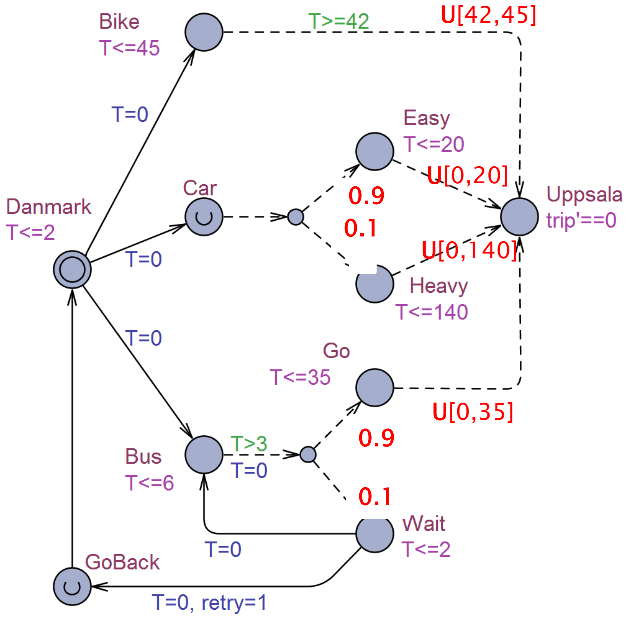
CPSIoT21

Kim Larsen [58]

Going to Uppsala – in 1 hour



Going to Uppsala – in 1 hour



Optimal WC Strategy
(2-player)
Take bike
WC=45

Optimal Expected Strategy
(1½ player)
Take car
E = 16
WC = 140

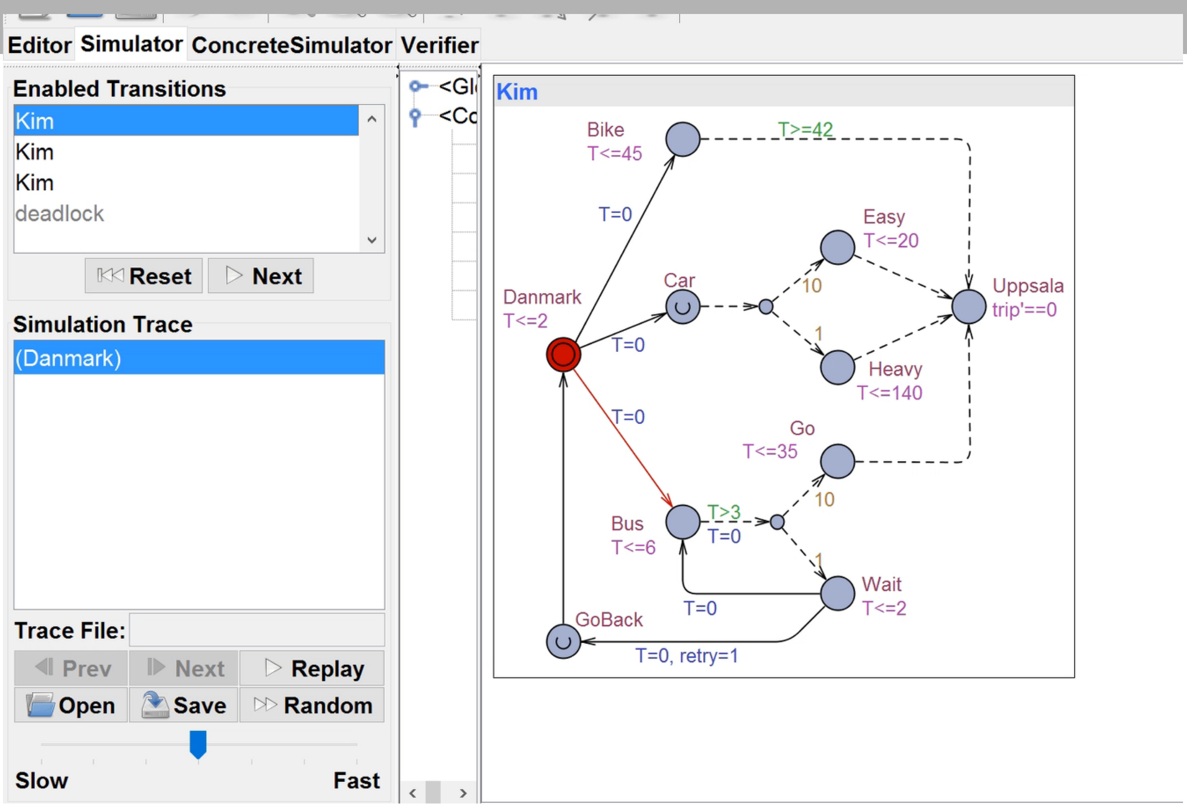
Optimal Expected Strategy
guaranteeing WC<=60
?????

CPSIoT21

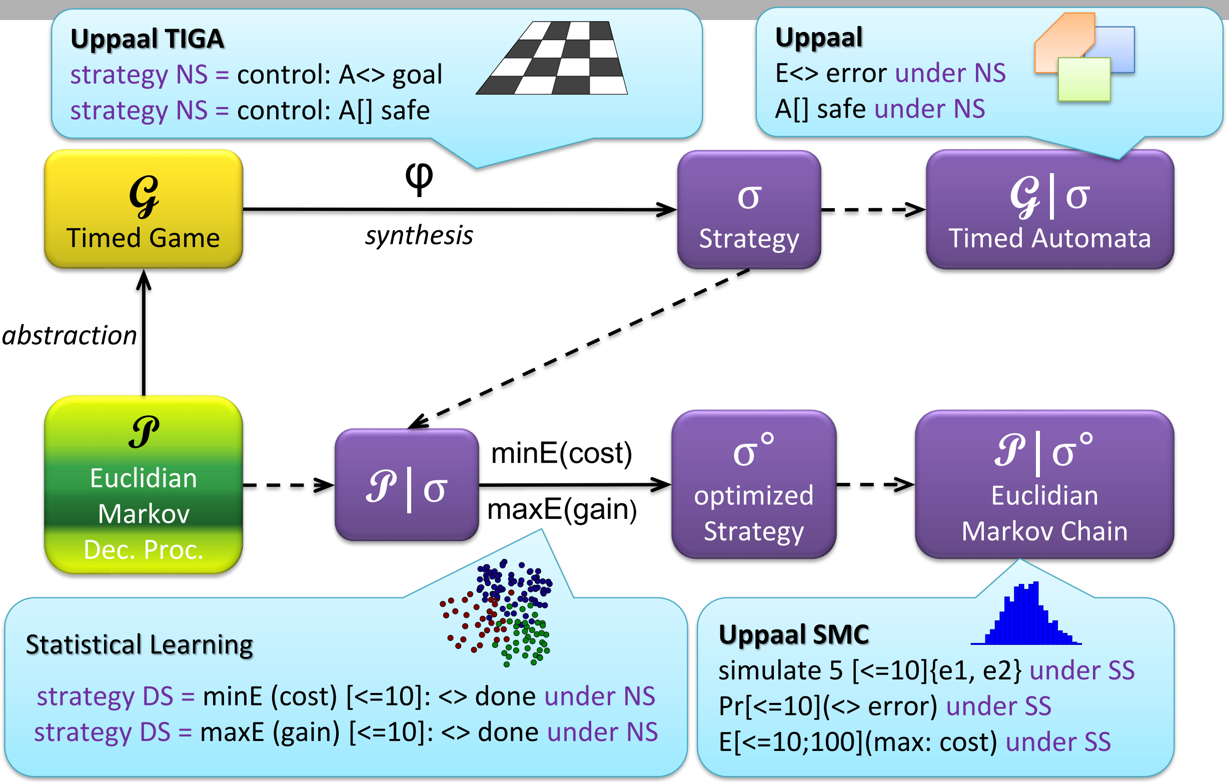
Kim Larsen [60]

©MECO.net

UPPAAL STRATEGO



Workflow under UPPAAL Stratego



Uppaal TIGA
strategy NS = control: A<> goal
strategy NS = control: A[] safe

Uppaal
E<> error under NS
A[] safe under NS

𝒢
Timed Game

φ
synthesis

σ
Strategy

𝒢|σ
Timed Automata

abstraction

𝒫
Euclidian
Markov
Dec. Proc.

𝒫|σ

minE(cost)
maxE(gain)

σ°
optimized
Strategy

𝒫|σ°
Euclidian
Markov Chain

Statistical Learning

strategy DS = minE (cost) [<=10]: <> done under NS
strategy DS = maxE (gain) [<=10]: <> done under NS

Uppaal SMC
simulate 5 [<=10]{e1, e2} under SS
Pr[<=10](<> error) under SS
E[<=10;100](max: cost) under SS

CPSIoT21

Kim Larsen [62]

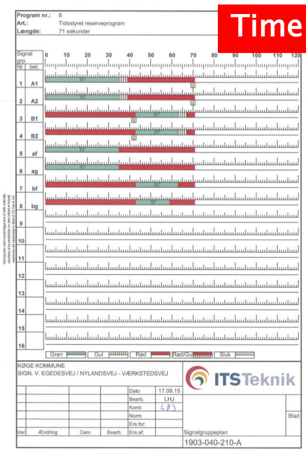
Traffic Control

On-Line Optimal Control Synthesis

Traffic Lights

- Observation: Unnecessary waiting time
- Currently:
  - Time triggered
  - Induction loops
- Exploit new information from radars

Time Triggered



Program nr.: 8
Art.: Tidsstyret reserveprogram
Længde: 71 sekunder

Signal grp. Nr.	bet.
1	A1
2	A2
3	B1
4	B2
5	af
6	ag
7	bf
8	bg
9	
10	
11	
12	
13	
14	
15	
16	

KØGE KOMMUNE
SIGN. V. EGEDESVEJ / NYLANDSVEJ - VÆRKSTEDSVEJ

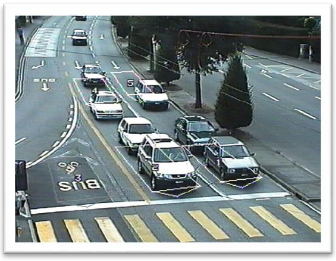
ITSTeknik

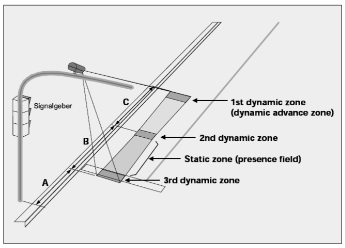
				Dato	17.09.15
				Bearb.	LHJ
				Kontr.	LHJ
				Norm	
				Ers.for:	
Ver	Ændring	Dato	Bearb.	Ers.af:	

Signalgruppeplan
Blad
1903-040-210-A

Loop Induction

Radar





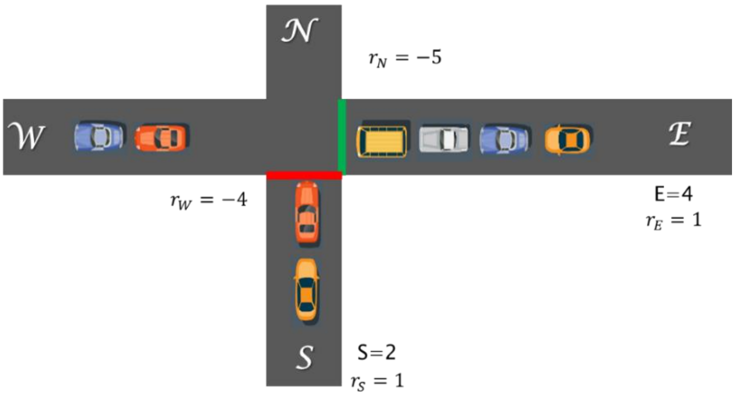
Signalgeber
A
B
C
1st dynamic zone (dynamic advance zone)
2nd dynamic zone
Static zone (presence field)
3rd dynamic zone

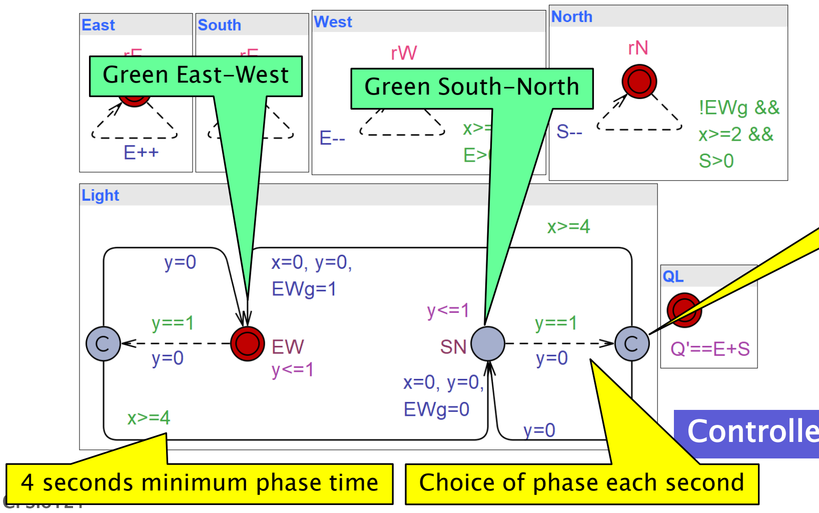
Detection fields

Kim Larsen [64]

Playing Games with Traffic Lights

```
int E, S;
clock x, t;
const int rE=1, rS=6, rW=5, rN=4;
bool EWg=1;
hybrid clock Q;
```





Green East-West

Green South-North

4 seconds minimum phase time

Choice of phase each second

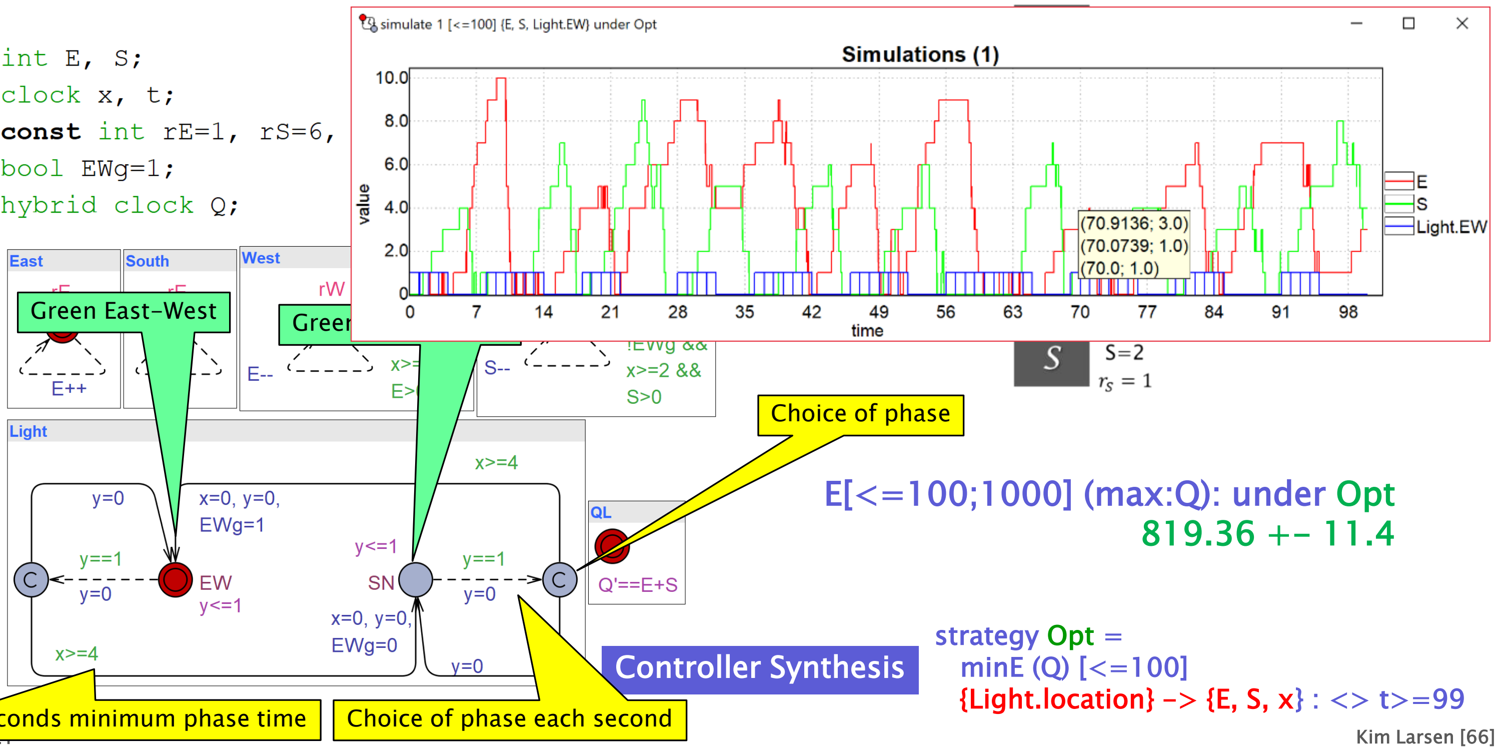
Choice of phase

Controller Synthesis

Kim Larsen [65]

Playing Games with Traffic Lights

```
int E, S;
clock x, t;
const int rE=1, rS=6,
bool EWg=1;
hybrid clock Q;
```



Green East-West

Green

Choice of phase

4 seconds minimum phase time

Choice of phase each second

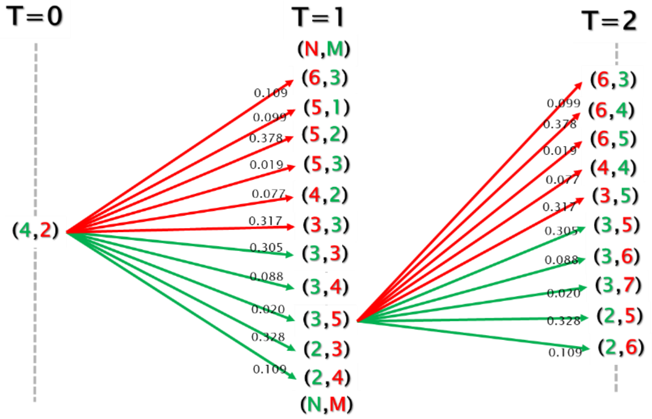
Controller Synthesis

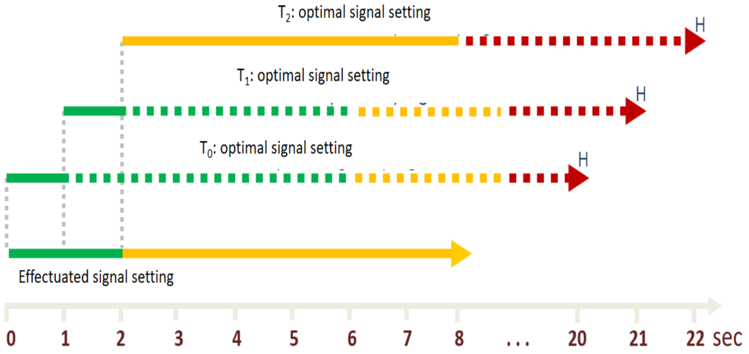
E[<=100;1000] (max:Q): under Opt
819.36 +- 11.4

strategy Opt =
minE (Q) [<=100]
{Light.location} -> {E, S, x} : <> t>=99

Kim Larsen [66]

On-line Learning

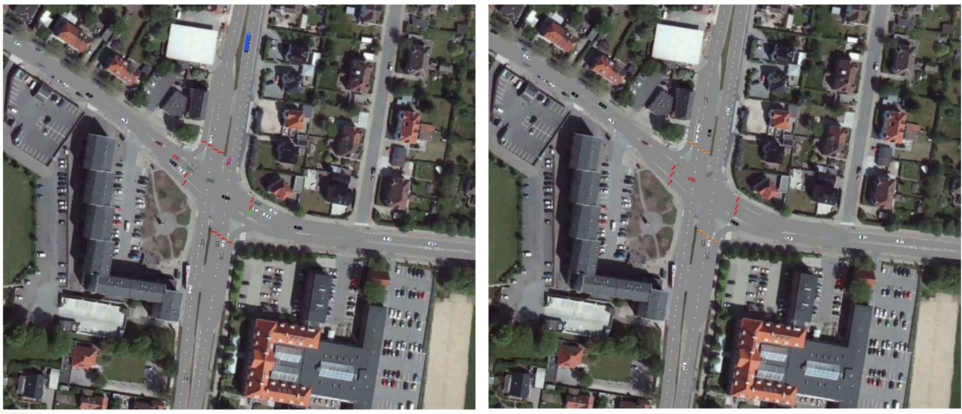


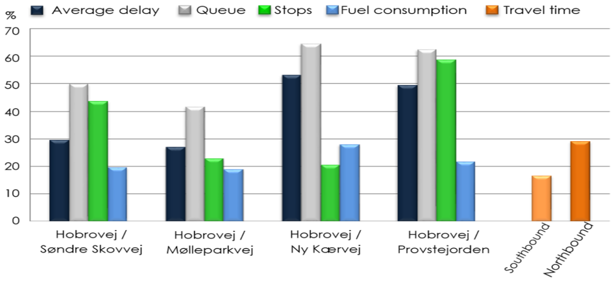

T2: optimal signal setting
H
T1: optimal signal setting
H
T0: optimal signal setting
H
Effectuated signal setting
0
1
2
3
4
5
6
7
8
...
20
21
22 sec

We learn a strategy up to a horizon, we then after a second learn a new strategy using the updated information from the radar.

Playing On-Line Games with Simulated Traffic

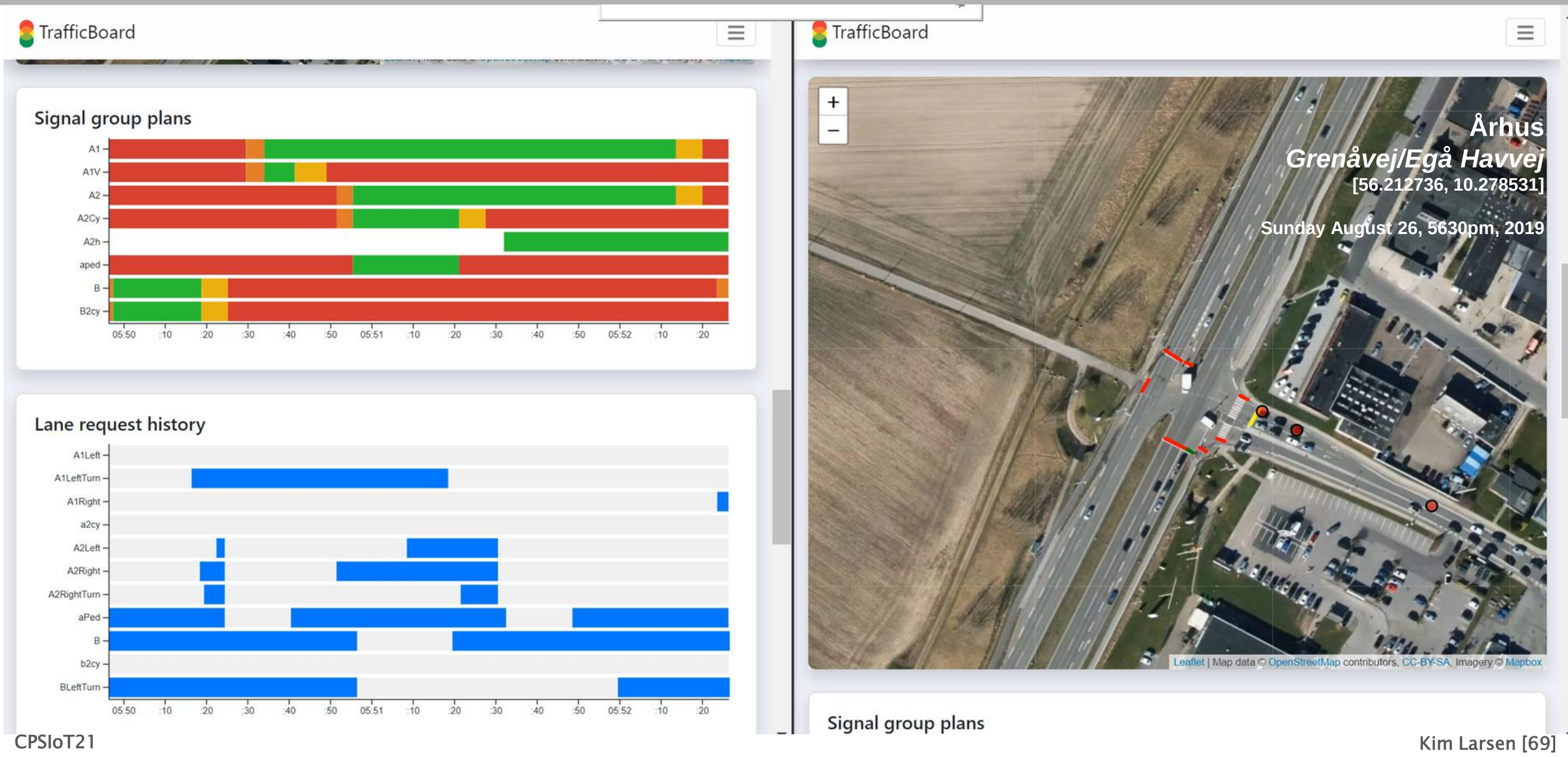
- Hobrovej
  - 2 km stretch
  - 6 signalized intersections
  - 20.000-30.000 vh/day
  - VISSEM (7.00-9.00)





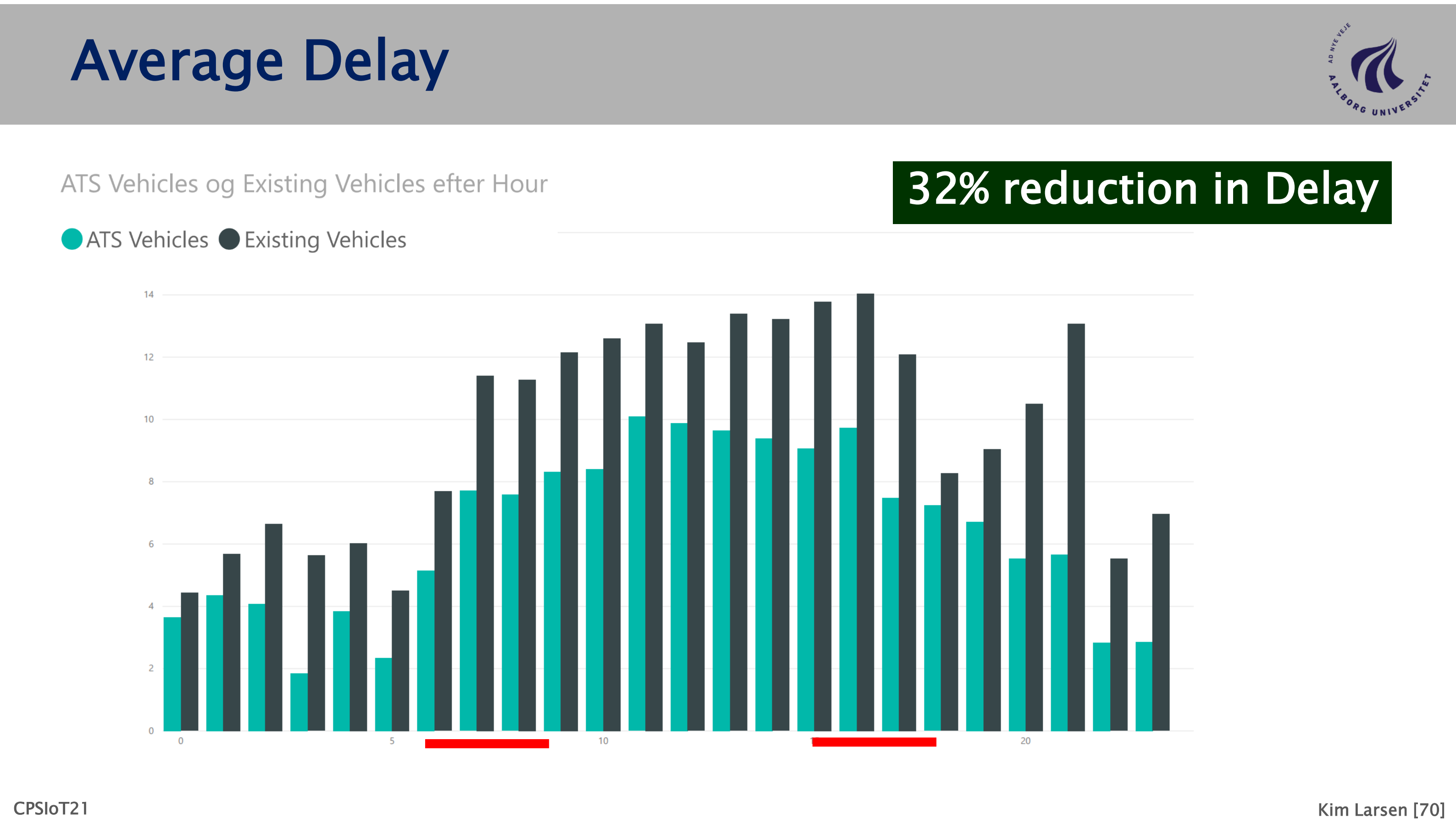
...n Larsen [68]

Playing On-Line Games with Real Traffic



Århus
Grenåvej/Egå Havvej
[56.212736, 10.278531]

Sunday August 26, 5630pm, 2019



Average Delay

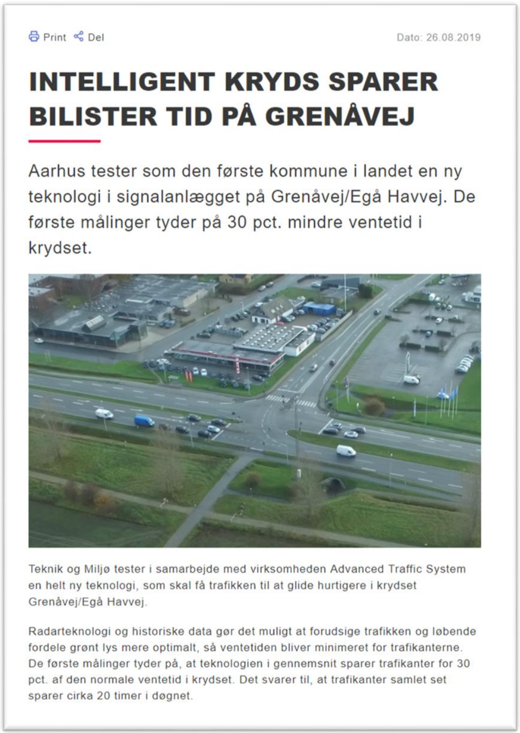
ATS Vehicles og Existing Vehicles efter Hour

32% reduction in Delay

CPSIoT21

Kim Larsen [70]

Advanced Traffic Systems



Print Del Dato: 26.08.2019

INTELLIGENT KRYDS SPARER BILISTER TID PÅ GRENÅVEJ

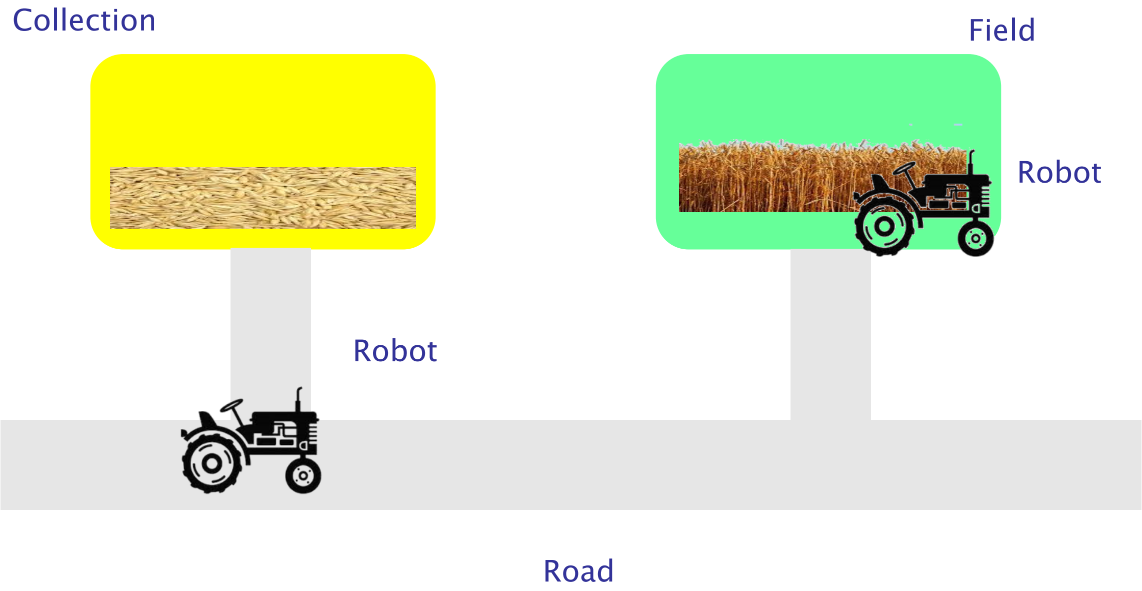
Aarhus tester som den første kommune i landet en ny teknologi i signalanlægget på Grenåvej/Egå Havvej. De første målinger tyder på 30 pct. mindre ventetid i krydset.

Teknik og Miljø tester i samarbejde med virksomheden Advanced Traffic System en helt ny teknologi, som skal få trafikken til at glide hurtigere i krydset Grenåvej/Egå Havvej.

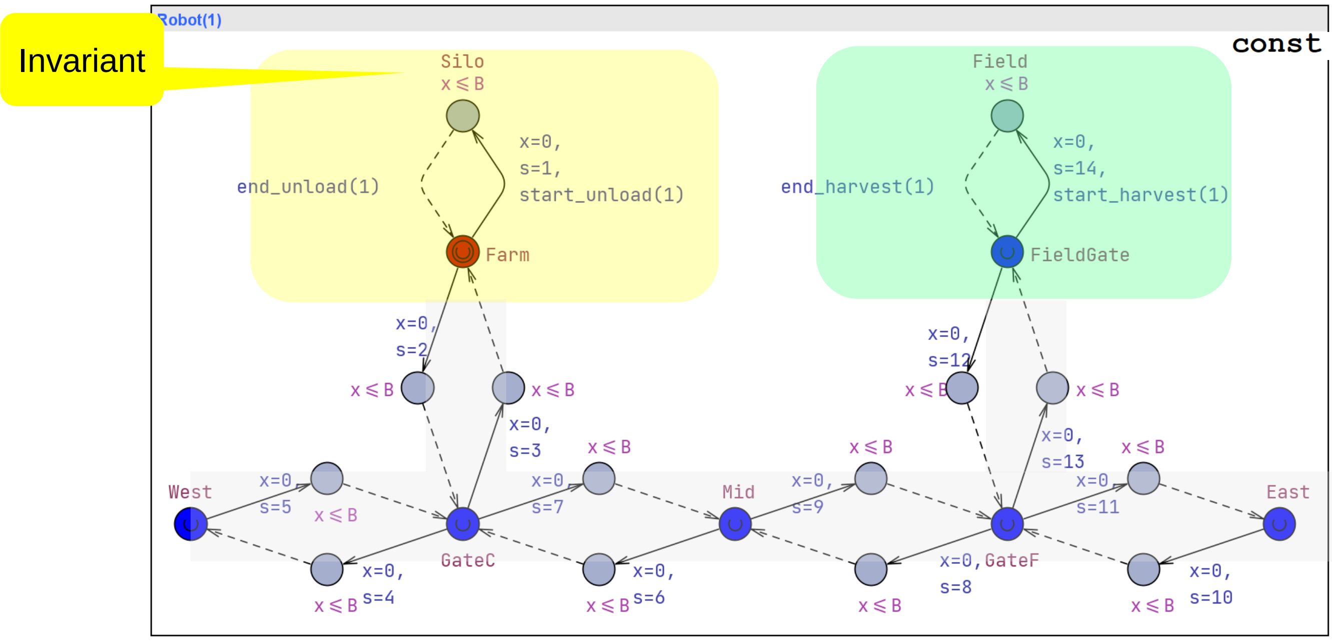
Radarteknologi og historiske data gør det muligt at forudsige trafikken og løbende fordele grønt lys mere optimalt, så ventetiden bliver minimeret for trafikanterne. De første målinger tyder på, at teknologien i gennemsnit sparer trafikanter for 30 pct. af den normale ventetid i krydset. Det svarer til, at trafikanter samlet set sparer cirka 20 timer i døgnet.

Smart Farming

Smart Farming / Dagstuhl 19432 Oct19



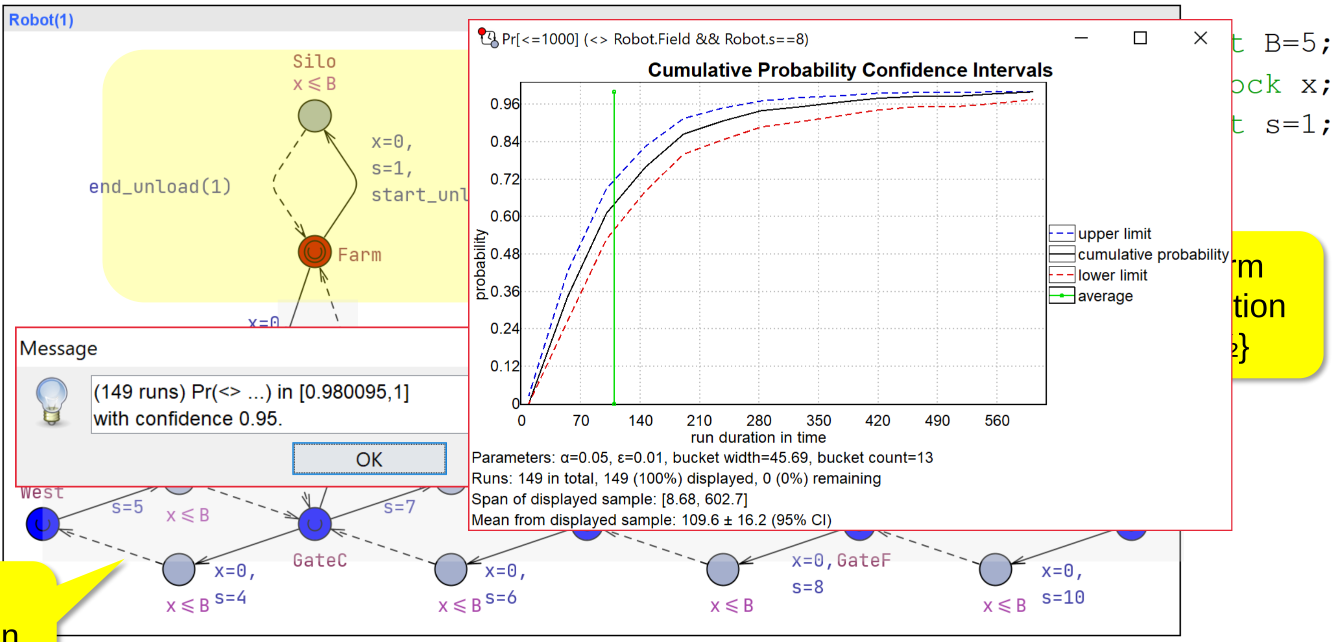
Smart Farming – Timed Automata



```
const int B=5;
clock x;
int s=1;
```

E<> Robot(1).Field && Robot(1).s==14

Smart Farming – Stochastic Timed Automata



Message

(149 runs) Pr(<> ...) in [0.980095,1]
with confidence 0.95.

OK

Parameters: α=0.05, ε=0.01, bucket width=45.69, bucket count=13
Runs: 149 in total, 149 (100%) displayed, 0 (0%) remaining
Span of displayed sample: [8.68, 602.7]
Mean from displayed sample: 109.6 ± 16.2 (95% CI)

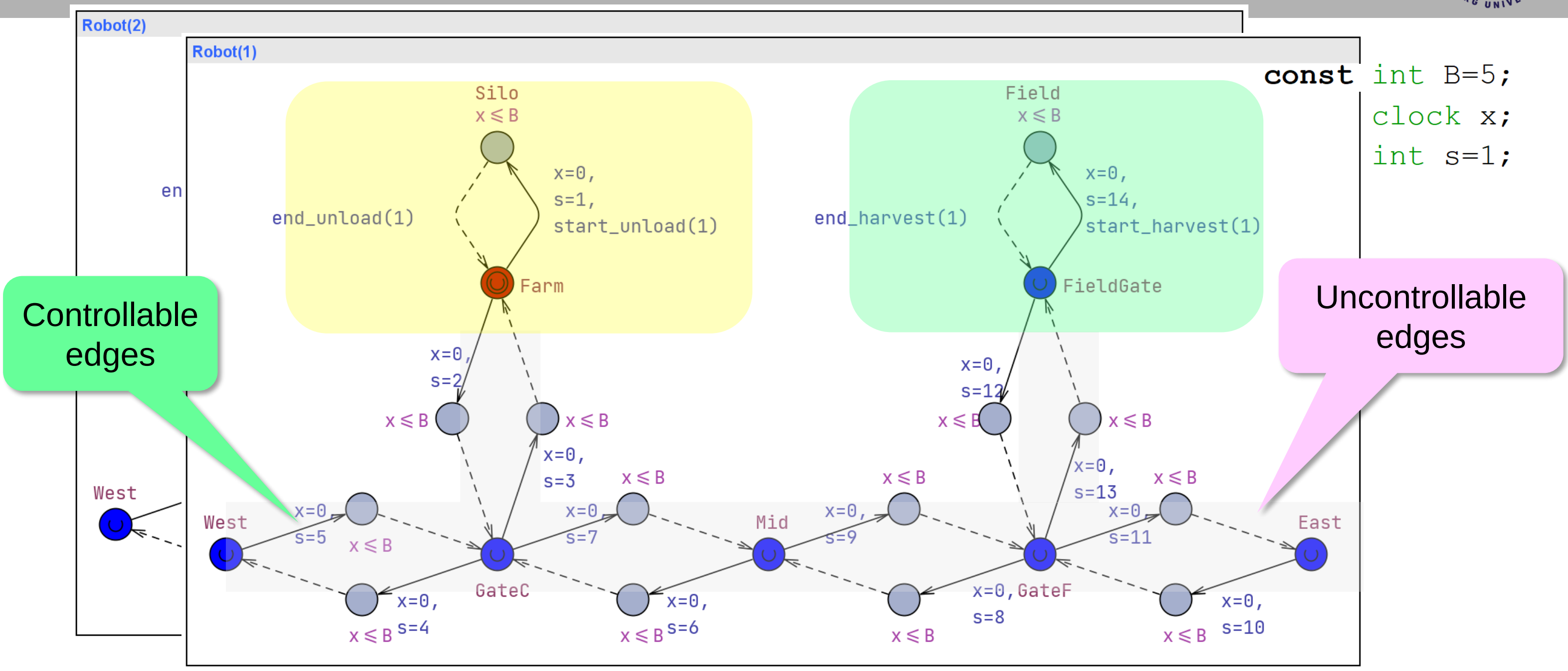
Uniform distribution [0,B]

Pr[<=1000] (<> Robot(1).Field && Robot(1).s==14)

CPSIoT21

Kim Larsen [75]

Smart Farming –Timed Game



```
const int B=5;
clock x;
int s=1;
```

Controllable edges

Uncontrollable edges

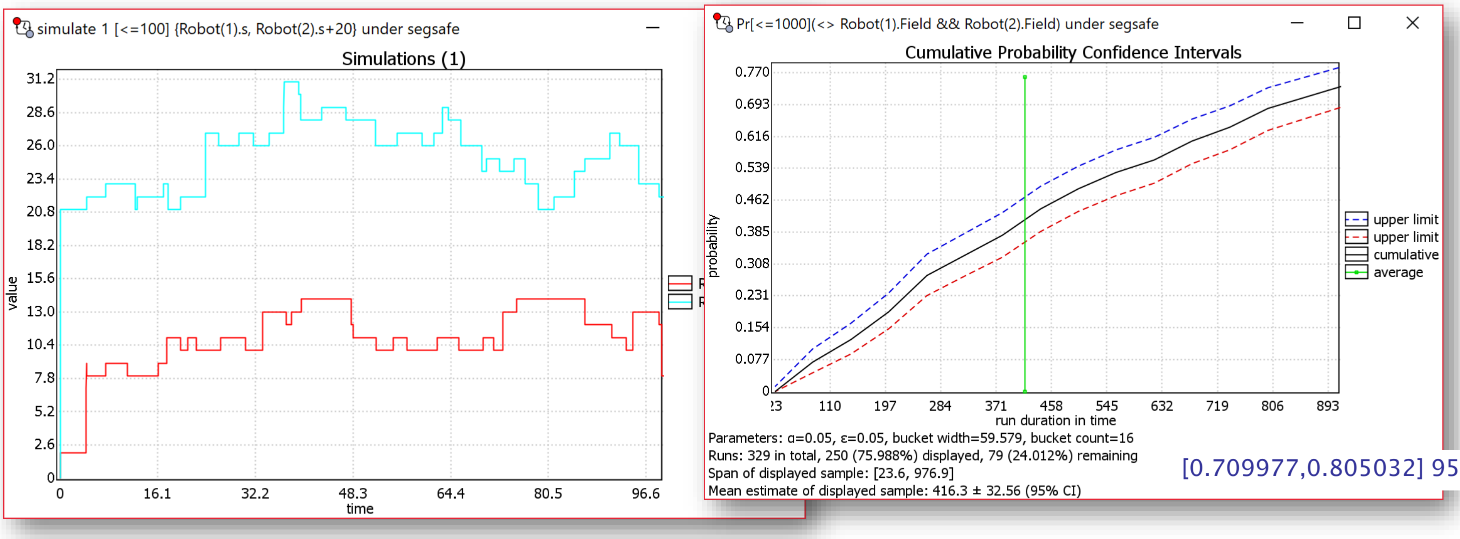
strategy segsafe = control: A[] ! (Robot(1).s>1 && Robot(1).s<14 && Robot(1).s==Robot(2).s)

CPSIoT21

Kim Larsen [76]

©MECO.net

Smart Farming – Timed Games



simulate 1 [<=100] {Robot(1).s, Robot(2).s+20} under segsafe

Simulations (1)

Pr[<=1000](<> Robot(1).Field && Robot(2).Field) under segsafe

Cumulative Probability Confidence Intervals

Parameters: α=0.05, ε=0.05, bucket width=59.579, bucket count=16
Runs: 329 in total, 250 (75.988%) displayed, 79 (24.012%) remaining
Span of displayed sample: [23.6, 976.9]
Mean estimate of displayed sample: 416.3 ± 32.56 (95% CI)

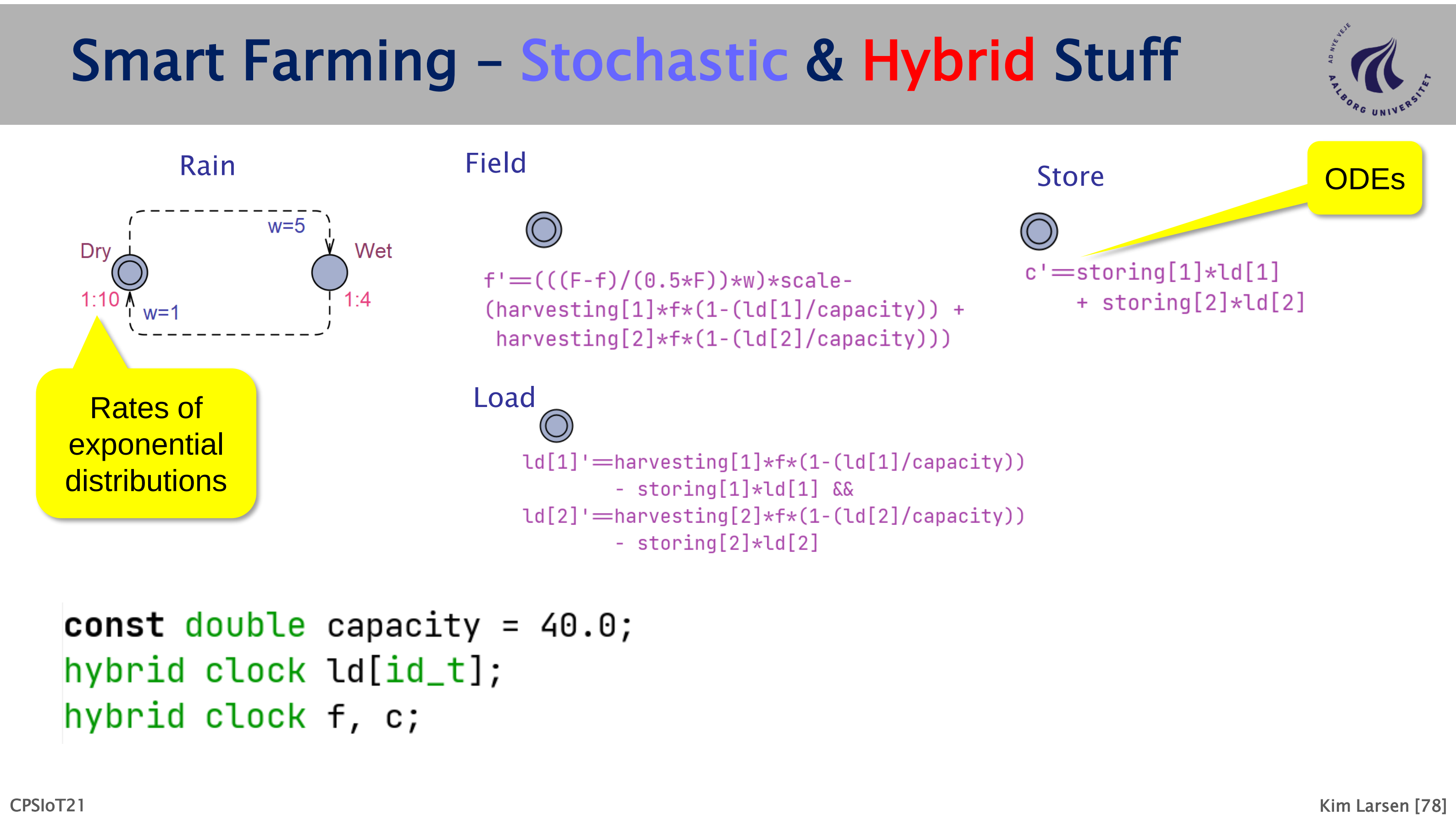
[0.709977,0.805032] 95%

simulate 1 [<=100] {Robot(1).s, Robot(2).s+20} under segsafe

E<> Robot(1).Field && Robot(2).Field under segsafe

E<> Robot(1).s>1 && Robot(1).s<14 && Robot(1).s==Robot(2).s under segsafe

Pr[<=1000] (<> Robot(1).Field && Robot(2).Field==14) under segsafe



Smart Farming – Stochastic & Hybrid Stuff

Rates of exponential distributions

Field

```
f'==(((F-f)/(0.5*F))*w)*scale-
(harvesting[1]*f*(1-(ld[1]/capacity)) +
 harvesting[2]*f*(1-(ld[2]/capacity)))
```

Store

```
c'==storing[1]*ld[1]
    + storing[2]*ld[2]
```

ODEs

Load

```
ld[1]'==harvesting[1]*f*(1-(ld[1]/capacity))
        - storing[1]*ld[1] &&
ld[2]'==harvesting[2]*f*(1-(ld[2]/capacity))
        - storing[2]*ld[2]
```

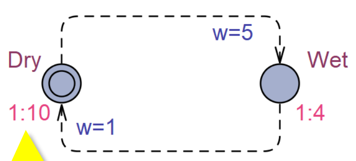
```
const double capacity = 40.0;
hybrid clock ld[id_t];
hybrid clock f, c;
```

CPSIoT21

Kim Larsen [78]

Smart Farming – Stochastic & Hybrid Stuff

Rain



Rates of exponential distributions

Field

```
f'==(((F-f)/(0.5*F))*w)*scale-
(harvesting[1]*f*(1-(ld[1]/capacity)) -
 harvesting[2]*f*(
```

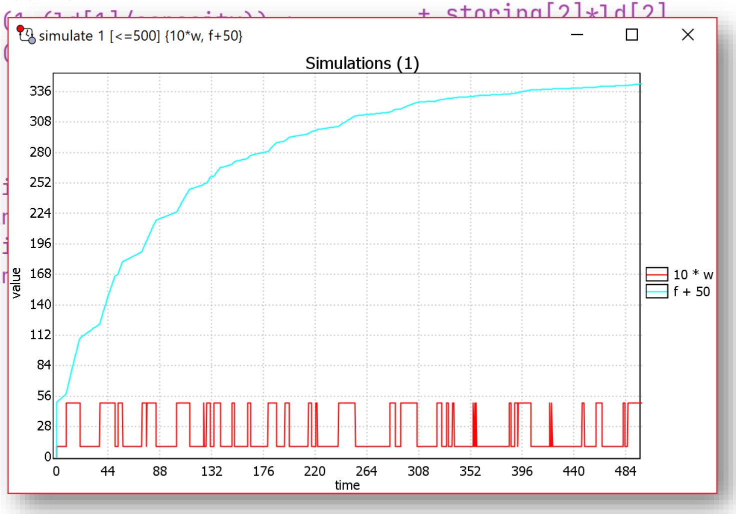
Load

```
ld[1]'==harvesti
        - storir
ld[2]'==harvesti
        - storir
```

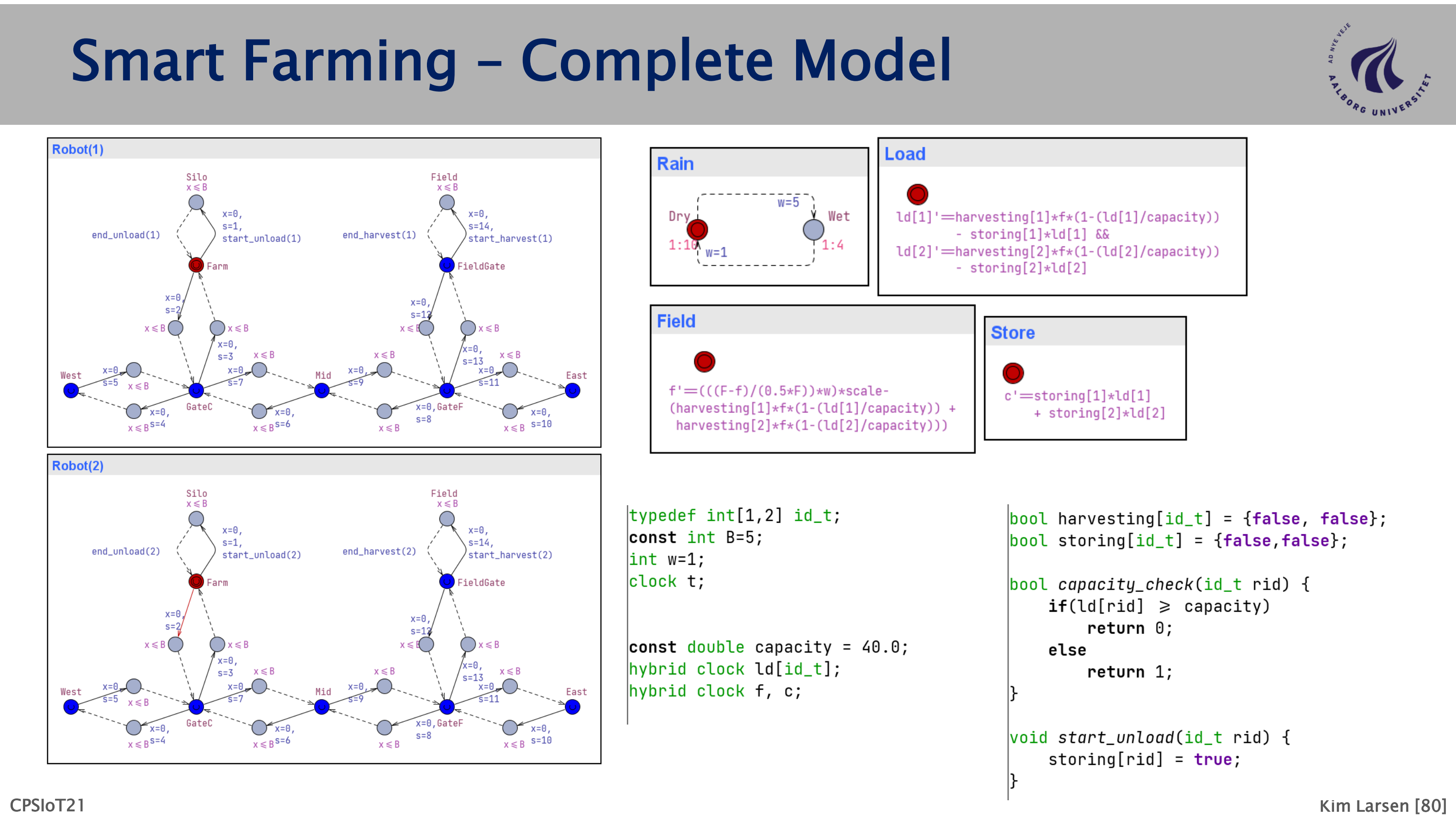
Store

ODEs

```
c'==storing[1]*ld[1]
    + storing[2]*ld[2]
```



```
const double capacity = 40.0;
hybrid clock ld[id_t];
hybrid clock f, c;
```



Smart Farming – Complete Model

```
ld[1]'==harvesting[1]*f*(1-(ld[1]/capacity))
      - storing[1]*ld[1] &&
ld[2]'==harvesting[2]*f*(1-(ld[2]/capacity))
      - storing[2]*ld[2]
```

```
f'==(((F-f)/(0.5*F))*w)*scale-
(harvesting[1]*f*(1-(ld[1]/capacity)) +
 harvesting[2]*f*(1-(ld[2]/capacity)))
```

```
c'==storing[1]*ld[1]
    + storing[2]*ld[2]
```

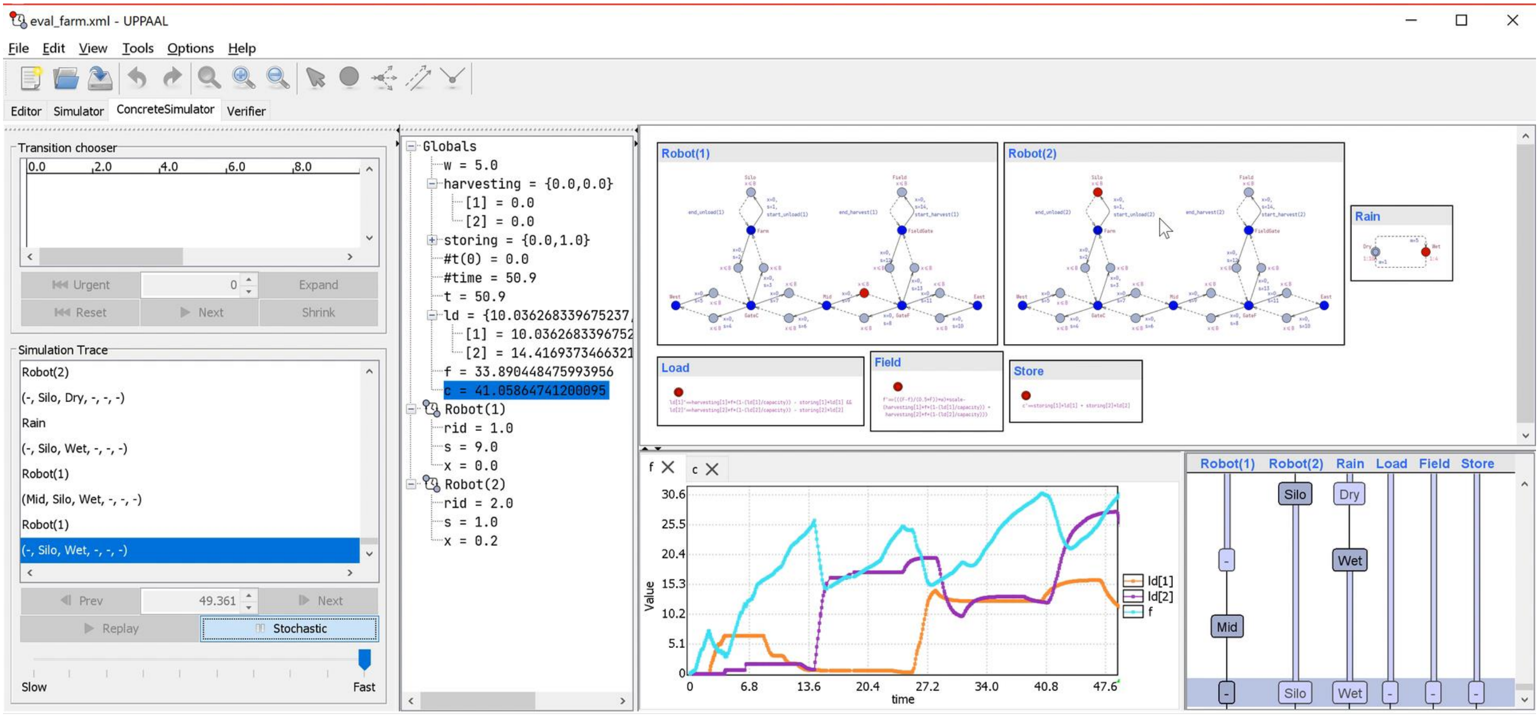
```
typedef int[1,2] id_t;
const int B=5;
int w=1;
clock t;


const double capacity = 40.0;
hybrid clock ld[id_t];
hybrid clock f, c;
```

```
bool harvesting[id_t] = {false, false};
bool storing[id_t] = {false,false};

bool capacity_check(id_t rid) {
    if(ld[rid] ≥ capacity)
        return 0;
    else
        return 1;
}

void start_unload(id_t rid) {
    storing[rid] = true;
}
```

CPSIoT21

Kim Larsen [80]

Farming Benchmark – in Stratego



eval_farm.xml - UPPAAL

Simulation Trace

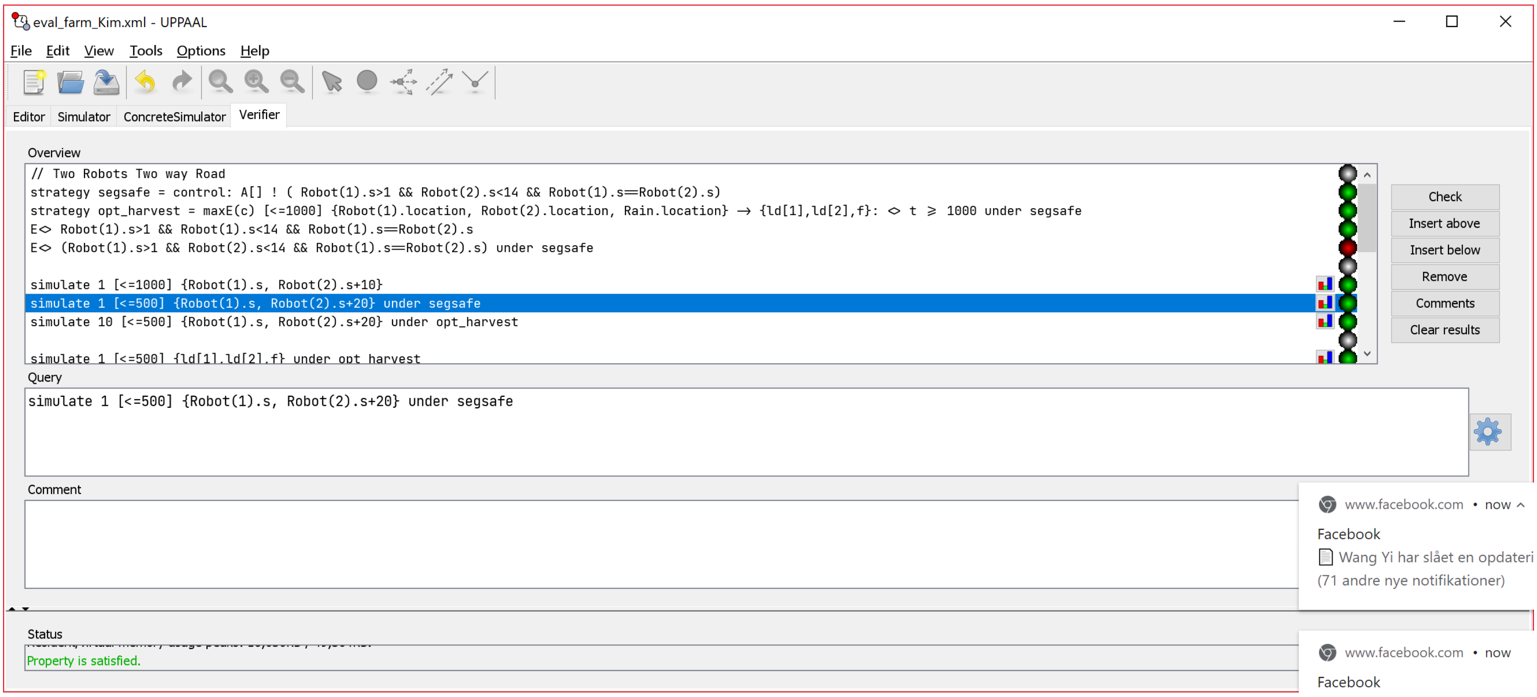
```
Robot(2)
(-, Silo, Dry, -, -, -)
Rain
(-, Silo, Wet, -, -, -)
Robot(1)
(Mid, Silo, Wet, -, -, -)
Robot(1)
(-, Silo, Wet, -, -, -)
```

Prev 49.361 Next

```
Globals
  w = 5.0
  harvesting = {0.0,0.0}
    [1] = 0.0
    [2] = 0.0
  storing = {0.0,1.0}
  #t(0) = 0.0
  #time = 50.9
  t = 50.9
  ld = {10.036268339675237,
    [1] = 10.0362683396752
    [2] = 14.4169373466321
  f = 33.890448475993956
  c = 41.05864741200095
Robot(1)
  rid = 1.0
  s = 9.0
  x = 0.0
Robot(2)
  rid = 2.0
  s = 1.0
  x = 0.2
```

File Edit View Tools Options Help
Editor Simulator ConcreteSimulator Verifier
Transition chooser
0.0 2.0 4.0 6.0 8.0
Urgent 0 Expand
Reset Next Shrink
Replay Stochastic
Slow Fast
Robot(1)
Robot(2)
Silo
Field
Farm
FieldGate
West
GateC
Mid
GateF
East
Rain
Dry
Wet
Load
ld[1]'==harvesting[1]*f*(1-(ld[1]/capacity)) - storing[1]*ld[1] &&
ld[2]'==harvesting[2]*f*(1-(ld[2]/capacity)) - storing[2]*ld[2]
Field
f'==(((F-f)/(0.5*f))*w)*scale-(harvesting[1]*f*(1-(ld[1]/capacity)) + harvesting[2]*f*(1-(ld[2]/capacity)))
Store
c'==storing[1]*ld[1] + storing[2]*ld[2]
f
c
Value
30.6
25.5
20.4
15.3
10.2
5.1
0
0
6.8
13.6
20.4
27.2
34.0
40.8
47.6
time
ld[1]
ld[2]
f
Robot(1) Robot(2) Rain Load Field Store
Silo
Dry
-
Wet
Mid
-
Silo
Wet
-
-
-

Farming Benchmark – in Stratego


eval_farm_Kim.xml - UPPAAL
File Edit View Tools Options Help
Editor Simulator ConcreteSimulator Verifier
Overview
Check
Insert above
Insert below
Remove
Comments
Clear results
Query
Comment
Status
www.facebook.com • now
Facebook
Wang Yi har slået en opdateri
(71 andre nye notifikationer)
www.facebook.com • now
Facebook

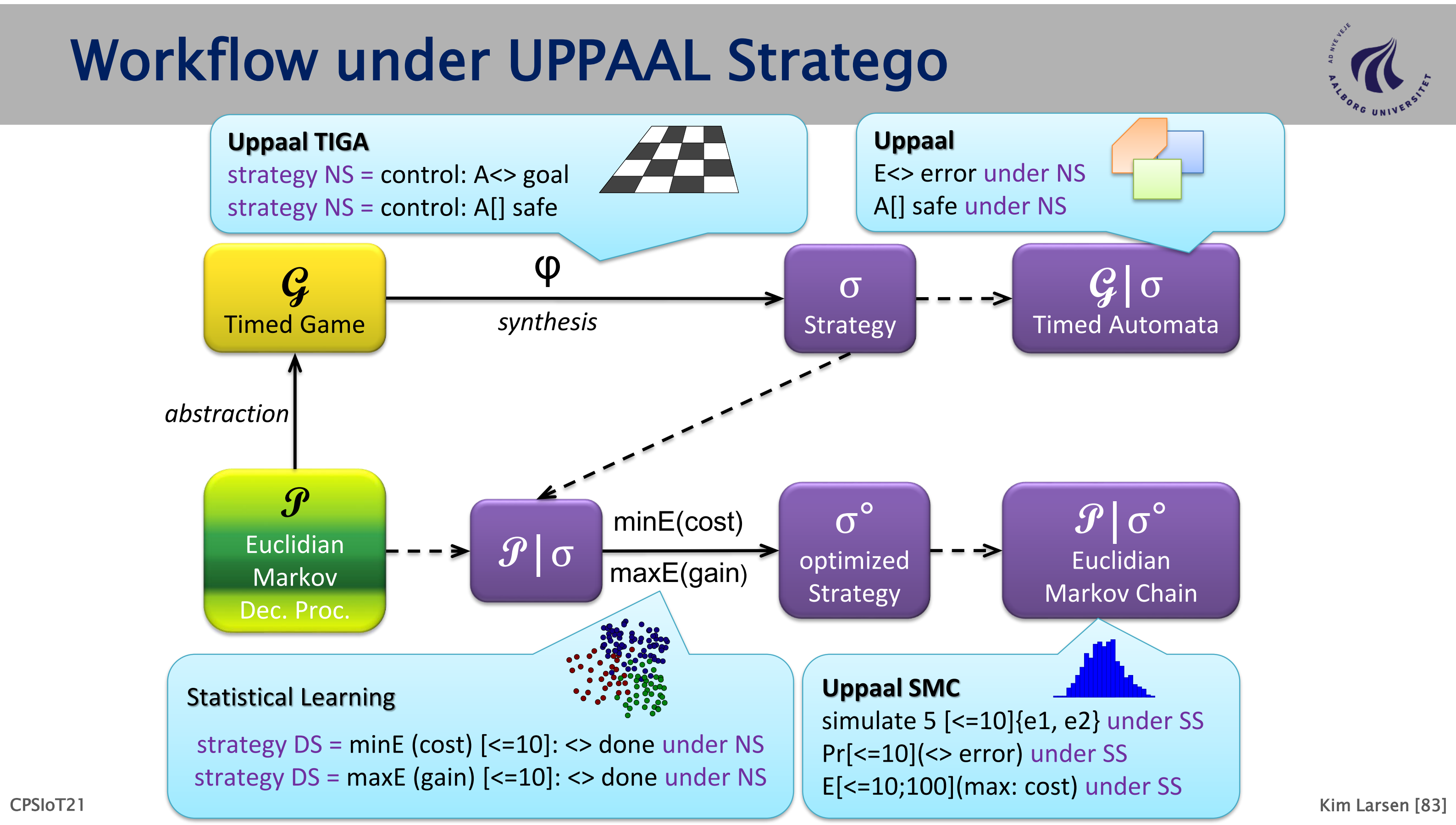
```
// Two Robots Two way Road
strategy segsafe = control: A[] ! ( Robot(1).s>1 && Robot(2).s<14 && Robot(1).s==Robot(2).s)
strategy opt_harvest = maxE(c) [<=1000] {Robot(1).location, Robot(2).location, Rain.location} → {ld[1],ld[2],f}: <> t ≥ 1000 under segsafe
E<> Robot(1).s>1 && Robot(1).s<14 && Robot(1).s==Robot(2).s
E<> (Robot(1).s>1 && Robot(2).s<14 && Robot(1).s==Robot(2).s) under segsafe

simulate 1 [<=1000] {Robot(1).s, Robot(2).s+10}
simulate 1 [<=500] {Robot(1).s, Robot(2).s+20} under segsafe
simulate 10 [<=500] {Robot(1).s, Robot(2).s+20} under opt_harvest

simulate 1 [<=500] {ld[1],ld[2],f} under opt_harvest
```

Query:

```
simulate 1 [<=500] {Robot(1).s, Robot(2).s+20} under segsafe
```

Status:

```
Property is satisfied.
```



Workflow under UPPAAL Stratego

Uppaal TIGA
strategy NS = control: A<> goal
strategy NS = control: A[] safe

Uppaal
E<> error under NS
A[] safe under NS

$\mathcal{G}$ Timed Game
φ
synthesis
σ Strategy
$\mathcal{G} | \sigma$ Timed Automata
abstraction
$\mathcal{P}$ Euclidian Markov Dec. Proc.
$\mathcal{P} | \sigma$
minE(cost)
maxE(gain)
σ° optimized Strategy
$\mathcal{P} | \sigma^\circ$ Euclidian Markov Chain

Statistical Learning
strategy DS = minE (cost) [<=10]: <> done under NS
strategy DS = maxE (gain) [<=10]: <> done under NS

Uppaal SMC
simulate 5 [<=10]{e1, e2} under SS
Pr[<=10](<> error) under SS
E[<=10;100](max: cost) under SS

CPSIoT21

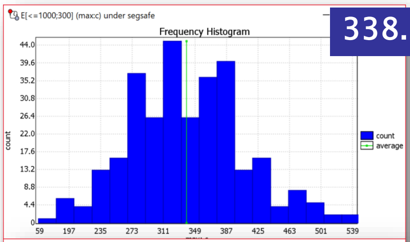
Kim Larsen [83]

Smart Farming

Q1: strategy segsafe = control: A[] ! (Robot(1).s>1 && Robot(1).s<14 && Robot(1).s==Robot(2).s)

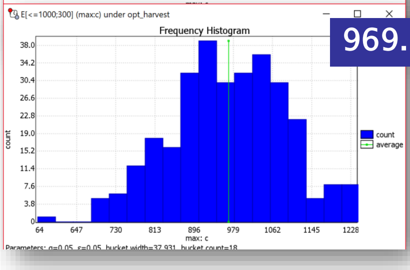
Q2: strategy opt_harvest =
maxE(c) [<=1000] {Robot(1).location, Robot(2).location, Rain.location} -> {ld1,ld2,t}:
<> t >= 1000 under segsafe

Q3: E[<=1000;300] (max:c) under segsafe



338.881 +/− 7.80819

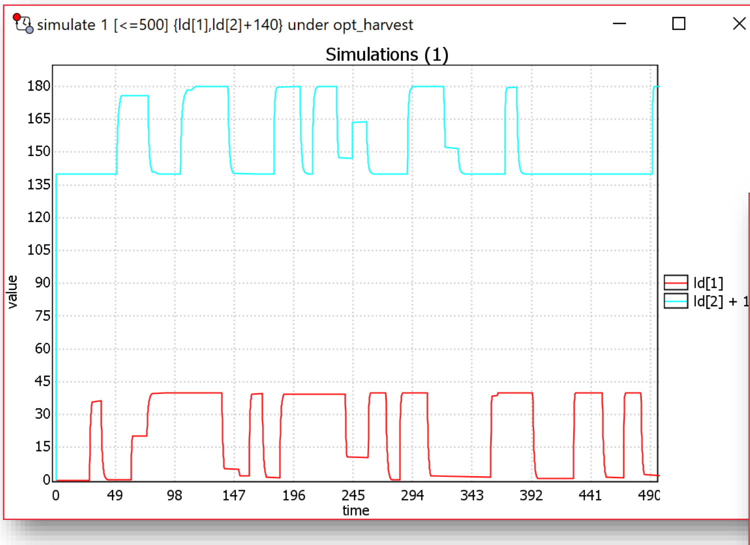
Q4: E[<=1000;300] (max:c) under opt_harvest



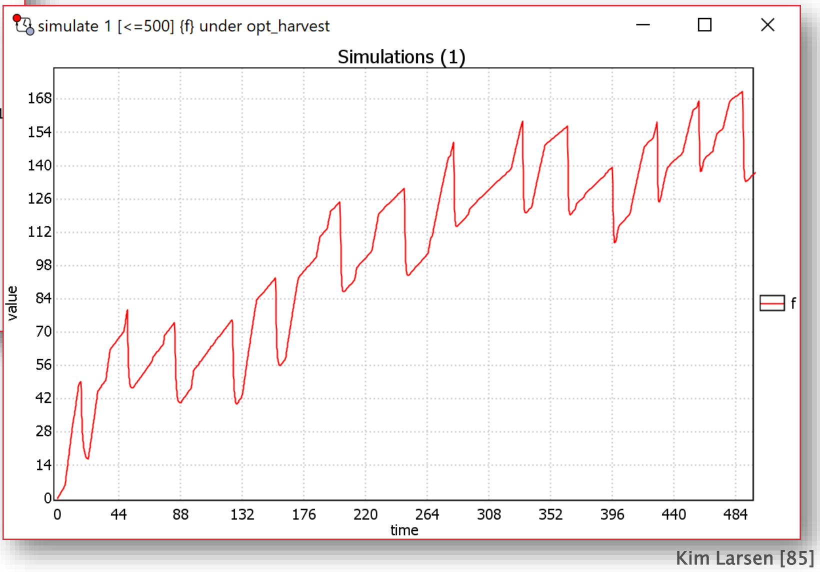
Parameters: α=0.05, ε=0.05, bucket width=37.931, bucket count=18

969.112 +/− 13.8988

ld[1], ld[2] – f

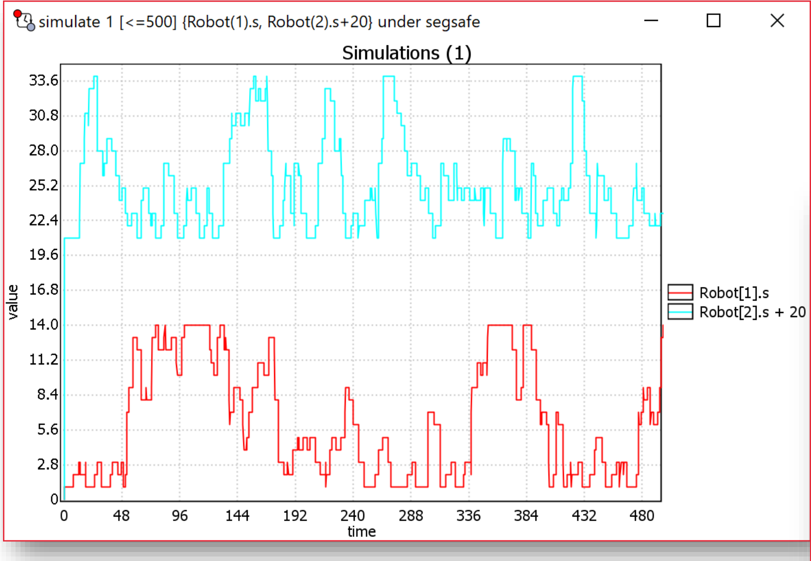


simulate 1 [<=500] {ld[1],ld[2]+140} under opt_harvest

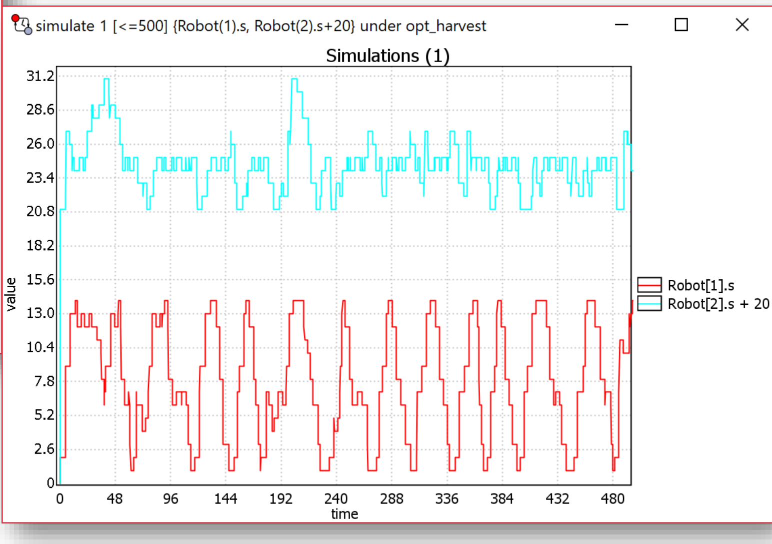


simulate 1 [<=500] {f} under opt_harvest

Robots Movement



simulate 1 [<=500] {Robot(1).s, Robot(2).s+20} under segsafe



simulate 1 [<=500] {Robot(1).s, Robot(2).s+20} under opt_harvest

References: Tools

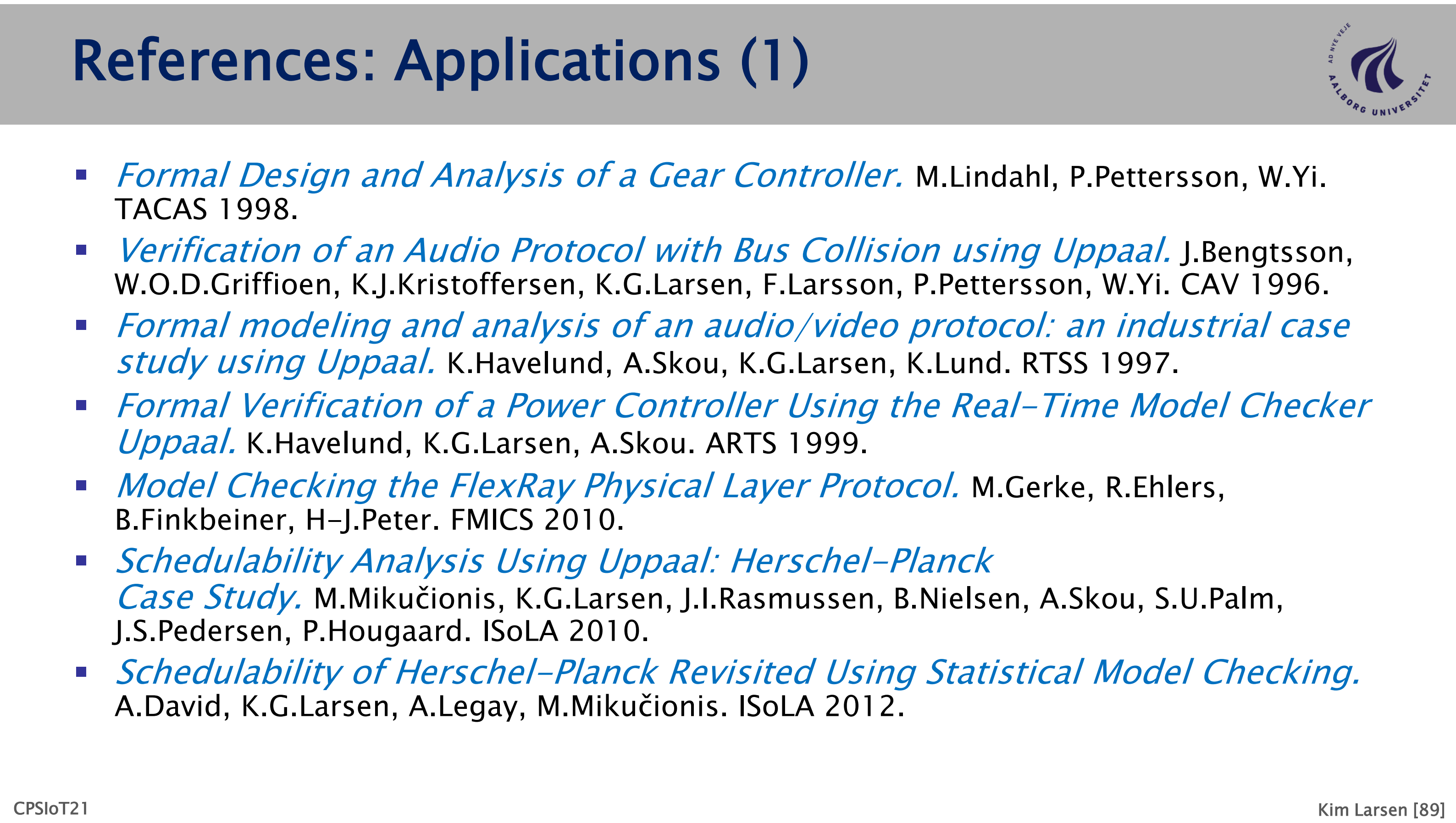
- *Uppaal in a Nutshell.* K.G.Larsen, P.Pettersson, W.Yi. STTT 1997.
- *Priced Timed Automata: Algorithms and Applications.* G.Behrmann, K.G.Larsen, J.I.Rasmussen. FMCO 2014.
- *Online Testing of Real-time Systems Using Uppaal.* K.G.Larsen, M.Mikučionis, B.Nielsen.
- *UPPAAL Tiga: Time for Playing Games.* G.Berhmann, A.Cougnard, A.David, E.Fleury, K.G.Larsen, D.Lime. CAV 2007.
- *Compositional verification of real-time systems using ECDAR.* A.David, K.G.Larsen, A.Legay, M.H.Møller, U.Nyman, A.P.Ravn, A.Skou,, A.Wąsowski, STTT 2012.
- *UPPAAL-SMC: Statistical Model Checking for Priced Timed Automata.* P.Bulychev, A.David, K.G.Larsen, M.Mikučionis, D.B.Poulsen, A.Legay, Z.Wang. QAPL 2012.
- *Uppaal Stratego.* A.David, P.G.Jensen, K.G.Larsen, M.Mikučionis, J.H.Taankvist. TACAS 2015.

CPSIoT21

Kim Larsen [87]

References: Tutorials and Overviews

- *A Tutorial on Uppaal.* G.Behrmann, A.David, K.G.Larsen. SFM-RT 2004.
- *Uppaal SMC Tutorial.* A.David, K.G.Larsen, A.Legay, M.Mikučionis, D.B.Poulsen. STTT 2015.
- *20 Years of Real Real Time Model Validation.* K.G.Larsen, F.Lorber, B.Nielsen. FM 2018.

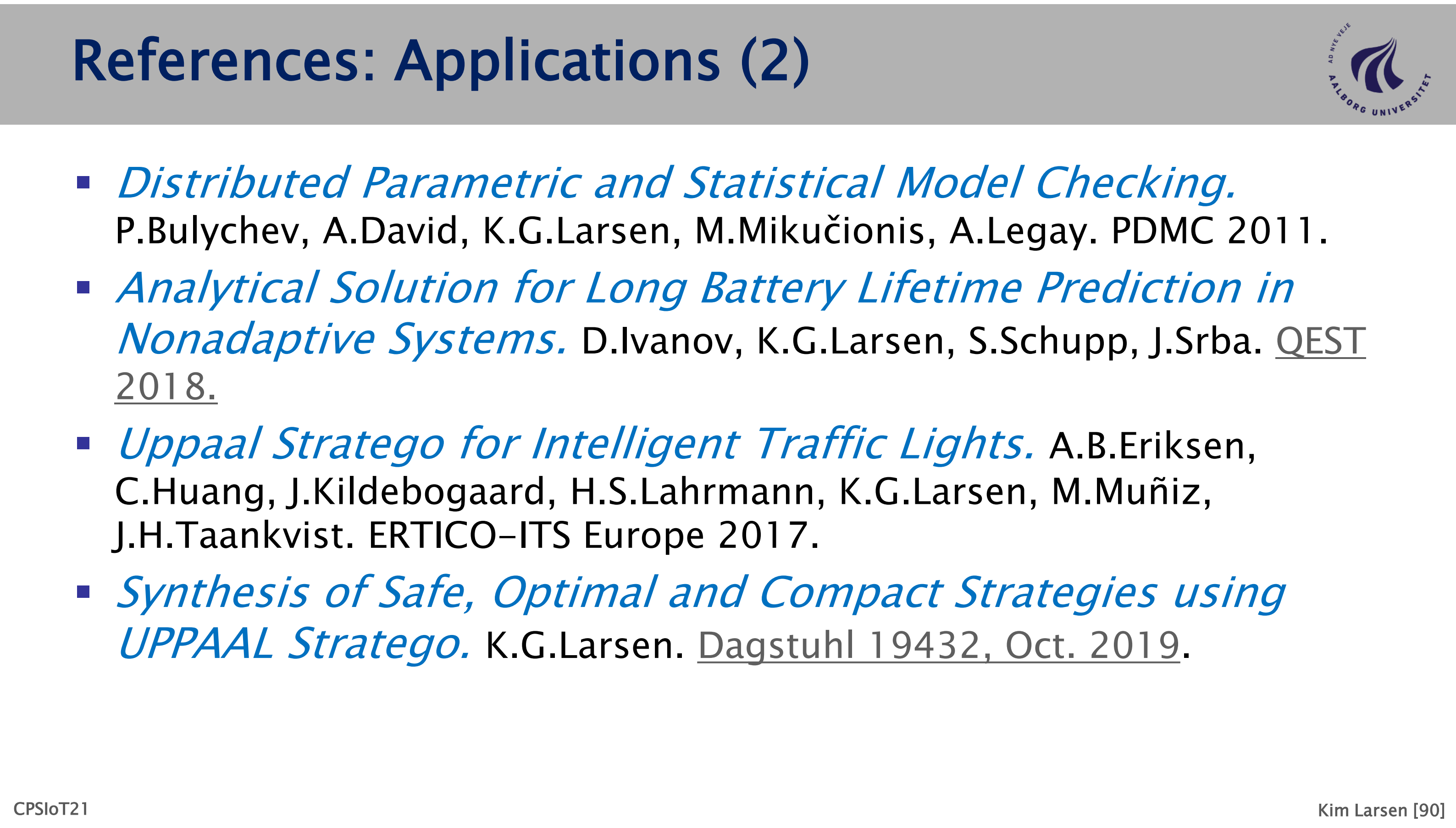


References: Applications (1)

- *Formal Design and Analysis of a Gear Controller.* M.Lindahl, P.Pettersson, W.Yi. TACAS 1998.
- *Verification of an Audio Protocol with Bus Collision using Uppaal.* J.Bengtsson, W.O.D.Griffioen, K.J.Kristoffersen, K.G.Larsen, F.Larsson, P.Pettersson, W.Yi. CAV 1996.
- *Formal modeling and analysis of an audio/video protocol: an industrial case study using Uppaal.* K.Havelund, A.Skou, K.G.Larsen, K.Lund. RTSS 1997.
- *Formal Verification of a Power Controller Using the Real-Time Model Checker Uppaal.* K.Havelund, K.G.Larsen, A.Skou. ARTS 1999.
- *Model Checking the FlexRay Physical Layer Protocol.* M.Gerke, R.Ehlers, B.Finkbeiner, H-J.Peter. FMICS 2010.
- *Schedulability Analysis Using Uppaal: Herschel-Planck Case Study.* M.Mikučionis, K.G.Larsen, J.I.Rasmussen, B.Nielsen, A.Skou, S.U.Palm, J.S.Pedersen, P.Hougaard. ISoLA 2010.
- *Schedulability of Herschel-Planck Revisited Using Statistical Model Checking.* A.David, K.G.Larsen, A.Legay, M.Mikučionis. ISoLA 2012.

CPSIoT21

Kim Larsen [89]



References: Applications (2)

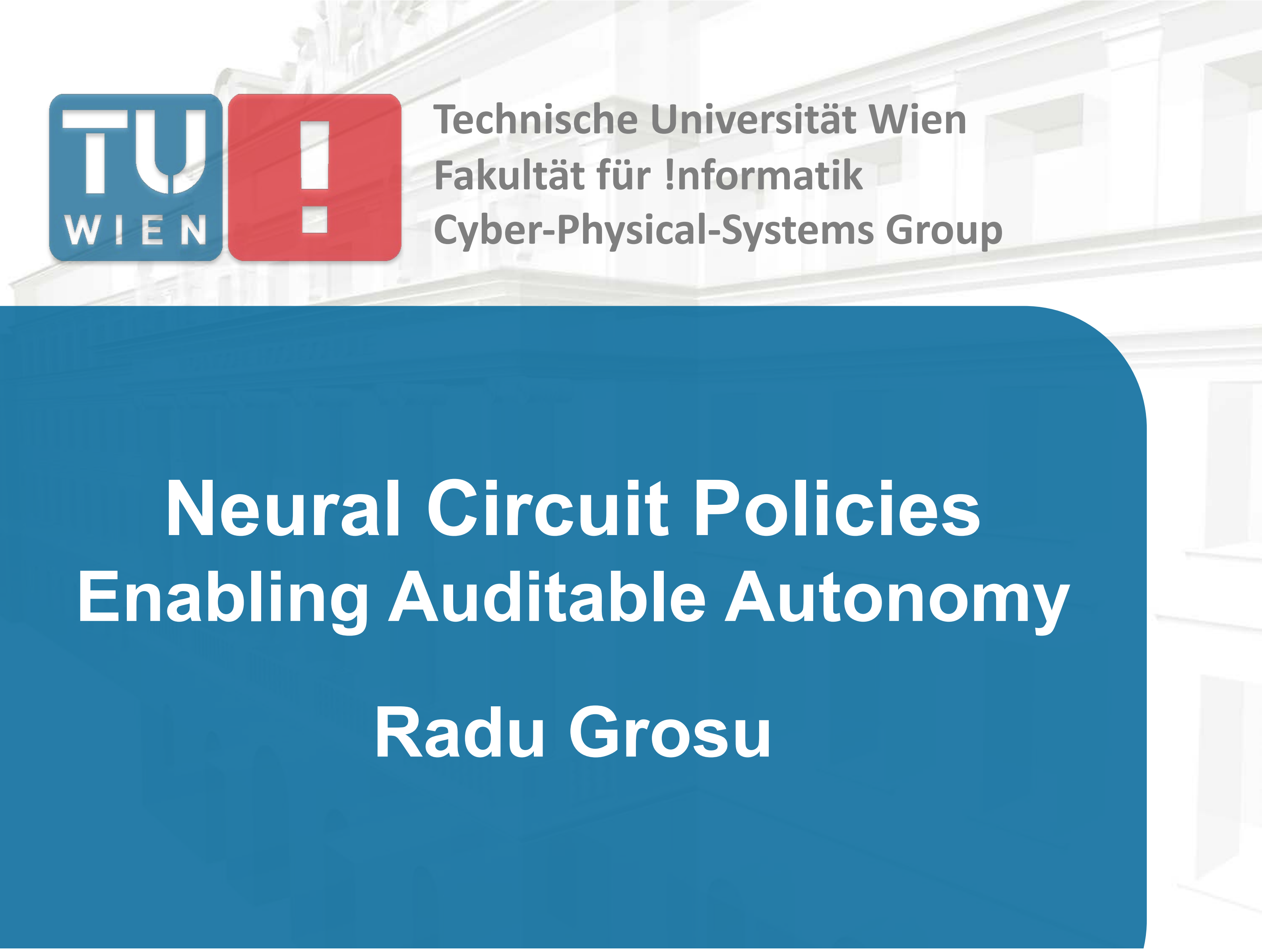
- *Distributed Parametric and Statistical Model Checking.* P.Bulychev, A.David, K.G.Larsen, M.Mikučionis, A.Legay. PDMC 2011.
- *Analytical Solution for Long Battery Lifetime Prediction in Nonadaptive Systems.* D.Ivanov, K.G.Larsen, S.Schupp, J.Srba. QEST 2018.
- *Uppaal Stratego for Intelligent Traffic Lights.* A.B.Eriksen, C.Huang, J.Kildebogaard, H.S.Lahrmann, K.G.Larsen, M.Muñiz, J.H.Taankvist. ERTICO-ITS Europe 2017.
- *Synthesis of Safe, Optimal and Compact Strategies using UPPAAL Stratego.* K.G.Larsen. Dagstuhl 19432, Oct. 2019.

CPSIoT21

Kim Larsen [90]

References: Other Applications

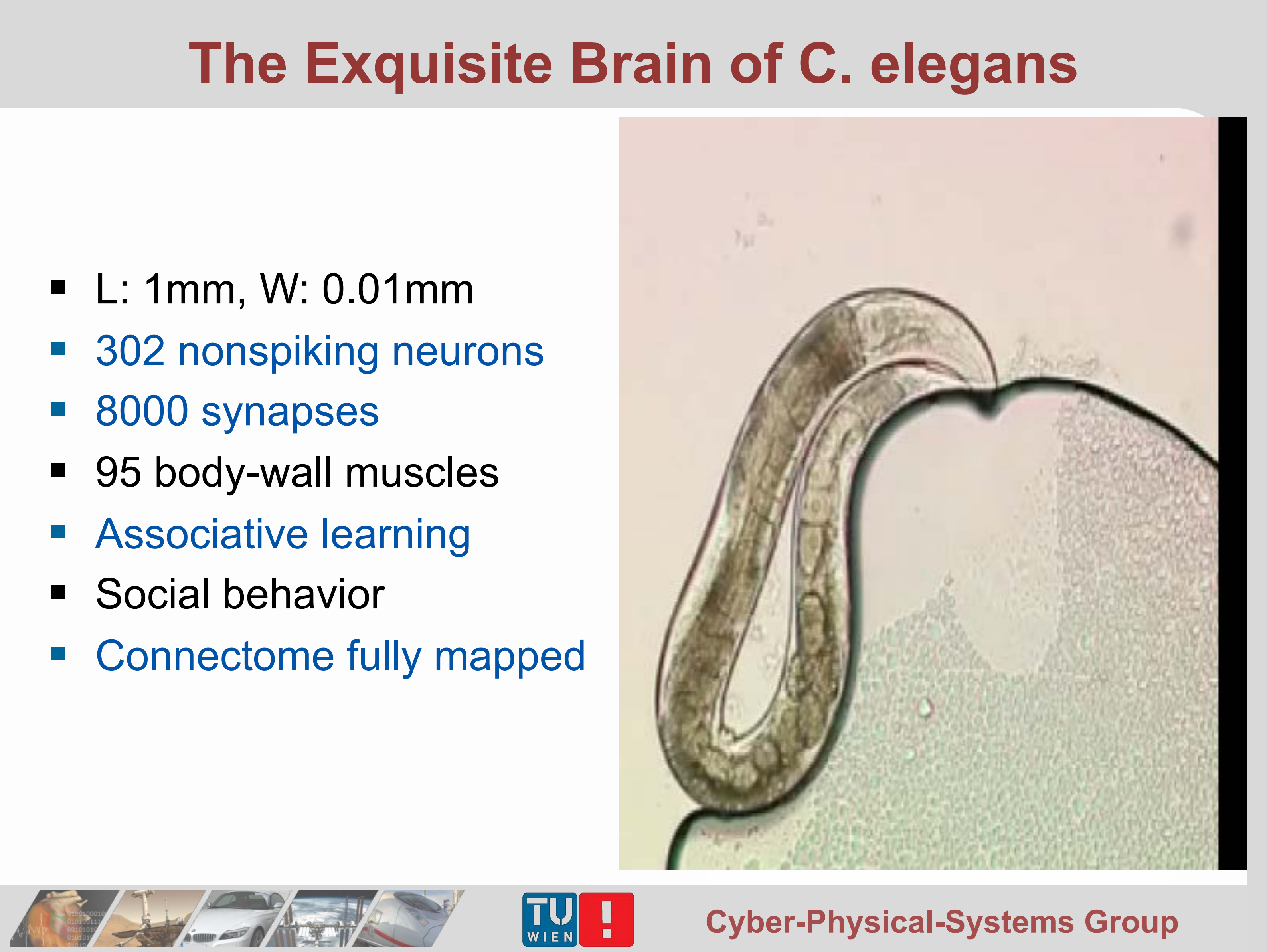
- *Formal analysis of a ZigBee-based routing protocol for smart grids using UPPAAL.* A.Rashid, O.Hasan, K.Saghar. HONET 2015.
- *Synthesizing power management strategies for wireless sensor networks with Uppaal-Stratego.* S.Dai, M.Hong, B.Guo. IJDSN 2017.
- *Optimizing Control Strategy Using Statistical Model Checking.* A.David, D.H.Du, K.G.Larsen, A.Legay, M.Mikučionis. NFM 2013.
- *Fluid Model-Checking in Uppaal for Covid-19.* P.G.Jensen, K.Y.Jørgensen, K.G.Larsen, M.Mikučionis, M.Muñiz, D.B.Poulsen. ISoLA 2020.



Technische Universität Wien
Fakultät für !nformatik
Cyber-Physical-Systems Group

Neural Circuit Policies Enabling Auditable Autonomy

Radu Grosu

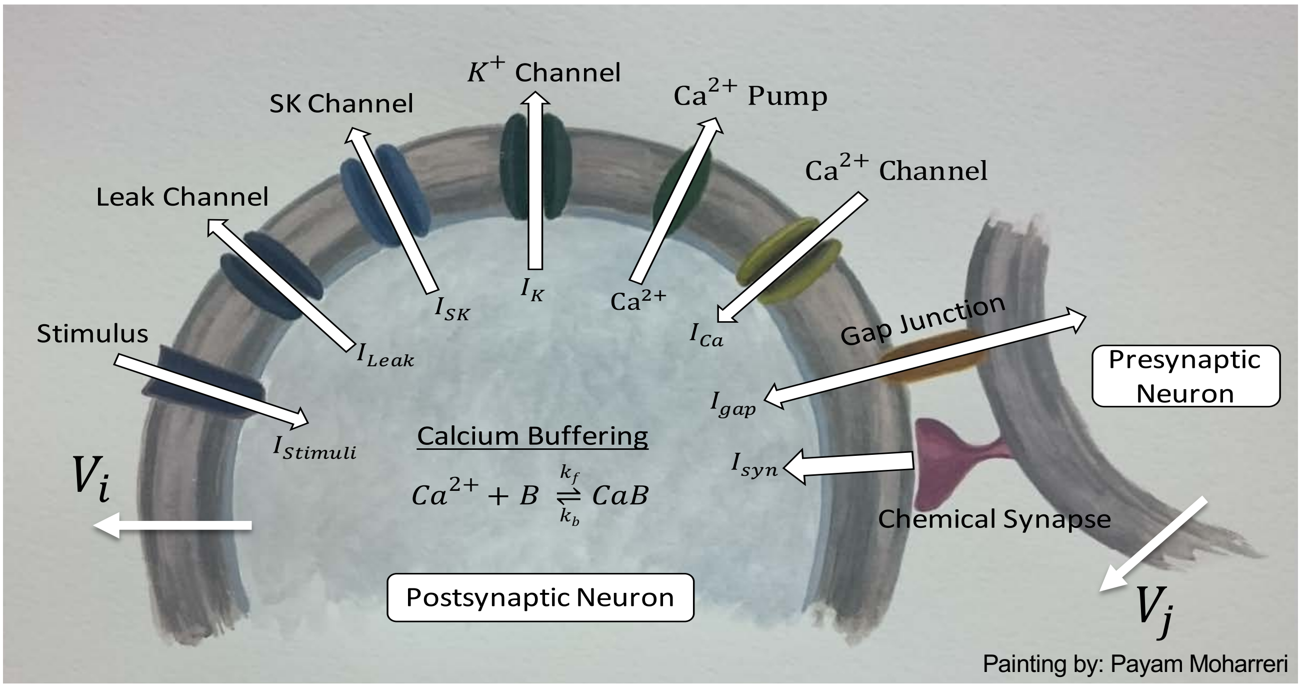


The Exquisite Brain of C. elegans

- L: 1mm, W: 0.01mm
- 302 nonspiking neurons
- 8000 synapses
- 95 body-wall muscles
- Associative learning
- Social behavior
- Connectome fully mapped

Cyber-Physical-Systems Group

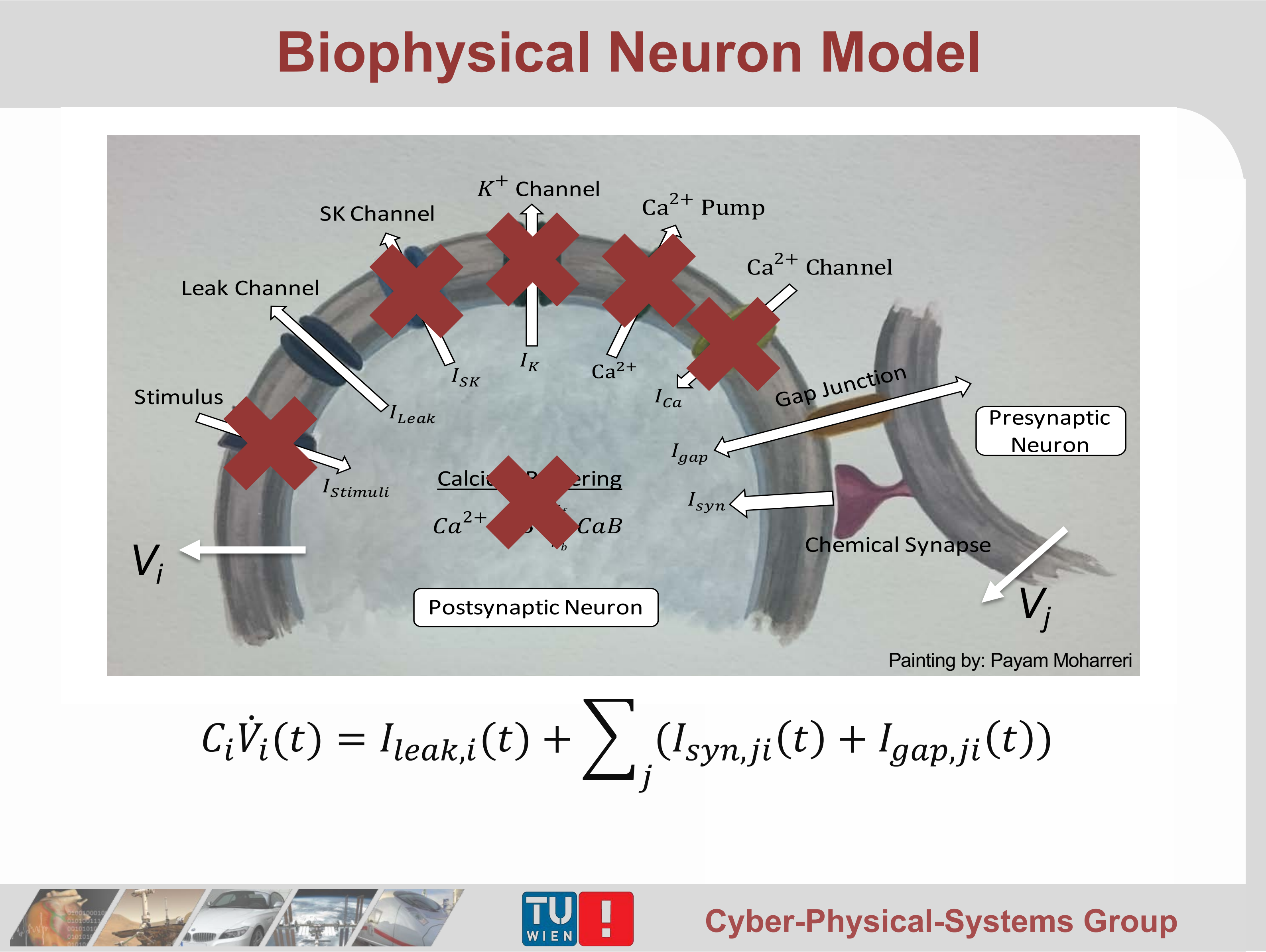
Biophysical Neuron Model



Painting by: Payam Moharreri

$$C_i \dot{V}_i = -\left(I_{Ca} + I_K + I_{SK} + I_{leak,i}\right) + I_{stim,i} + \sum_j I_{syn,ji} + I_{gap,ji}$$

Cyber-Physical-Systems Group

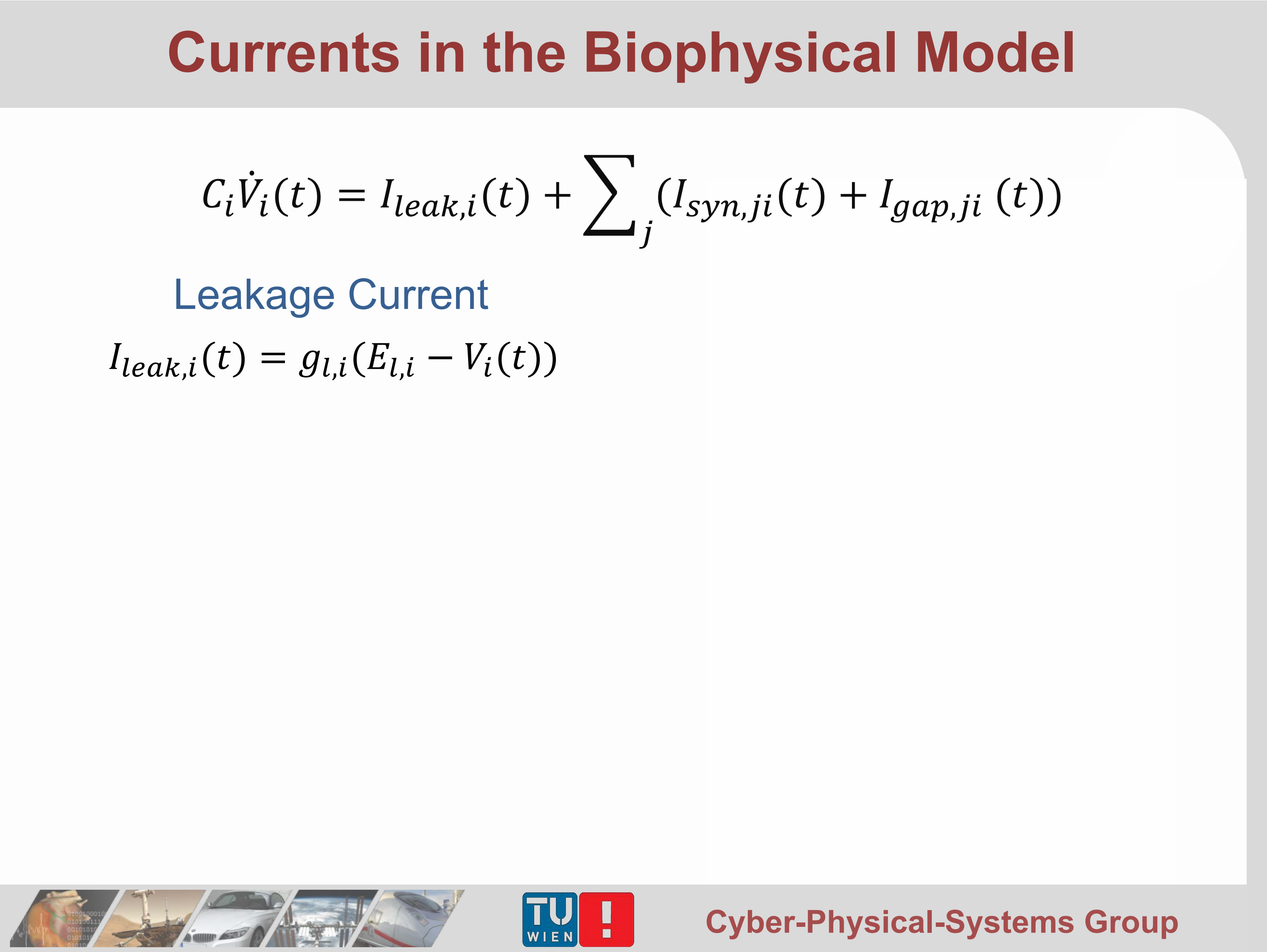


Biophysical Neuron Model

Painting by: Payam Moharreri

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum\nolimits_j (I_{syn,ji}(t) + I_{gap,ji}(t))$$

Cyber-Physical-Systems Group



Currents in the Biophysical Model

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\,(t))$$

Leakage Current

$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

TU WIEN
Cyber-Physical-Systems Group

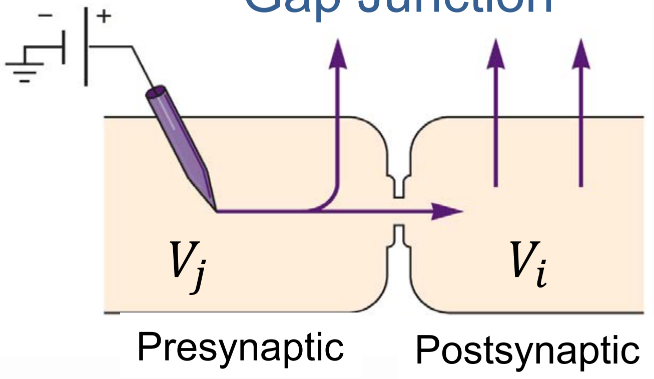
Currents in the Biophysical Model

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\ (t))$$

Leakage Current

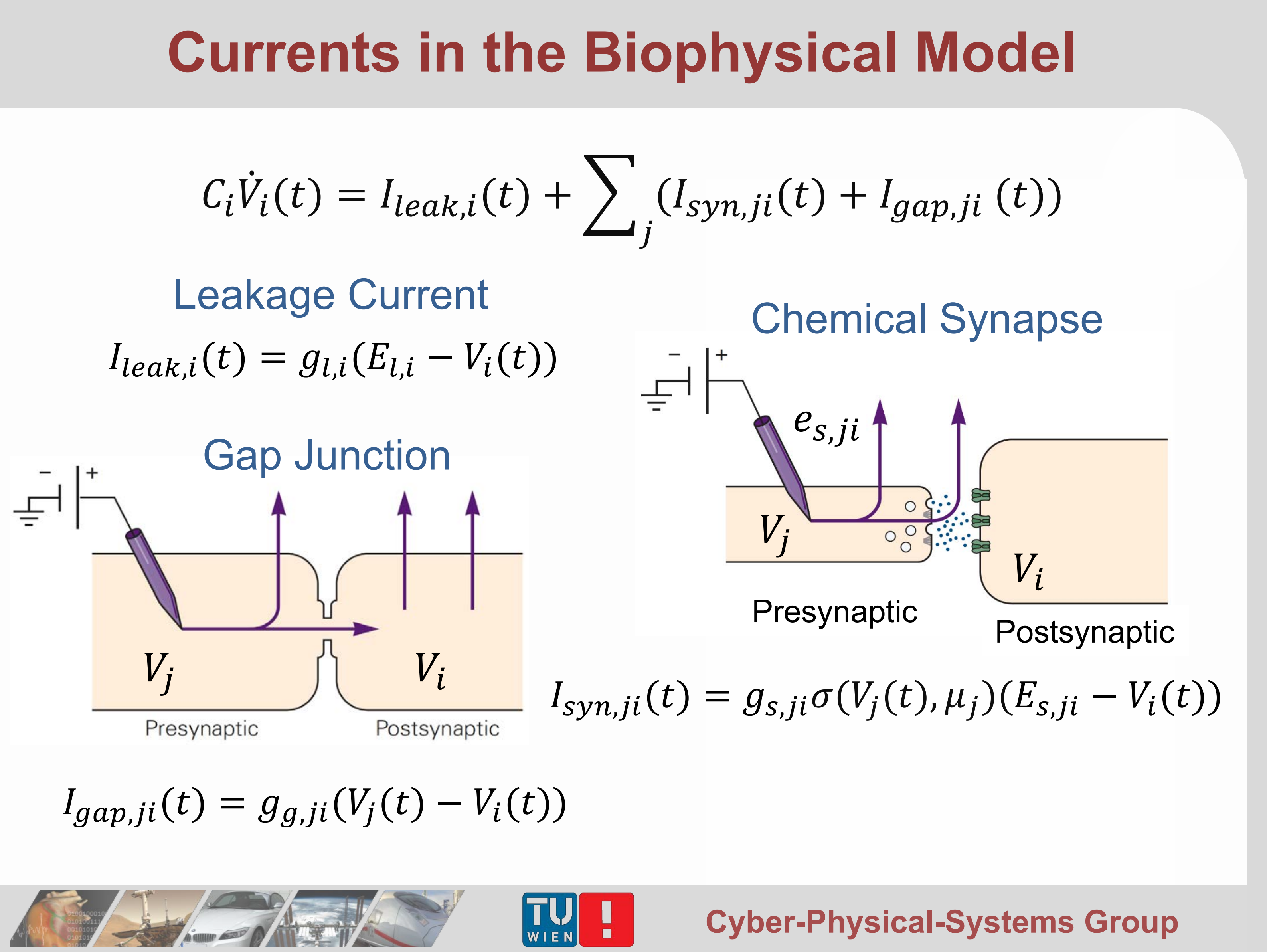
$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

Gap Junction



$$I_{gap,ji}(t) = g_{g,ji}(V_j(t) - V_i(t))$$

Cyber-Physical-Systems Group



Currents in the Biophysical Model

$$C_i \dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\ (t))$$

Leakage Current

$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

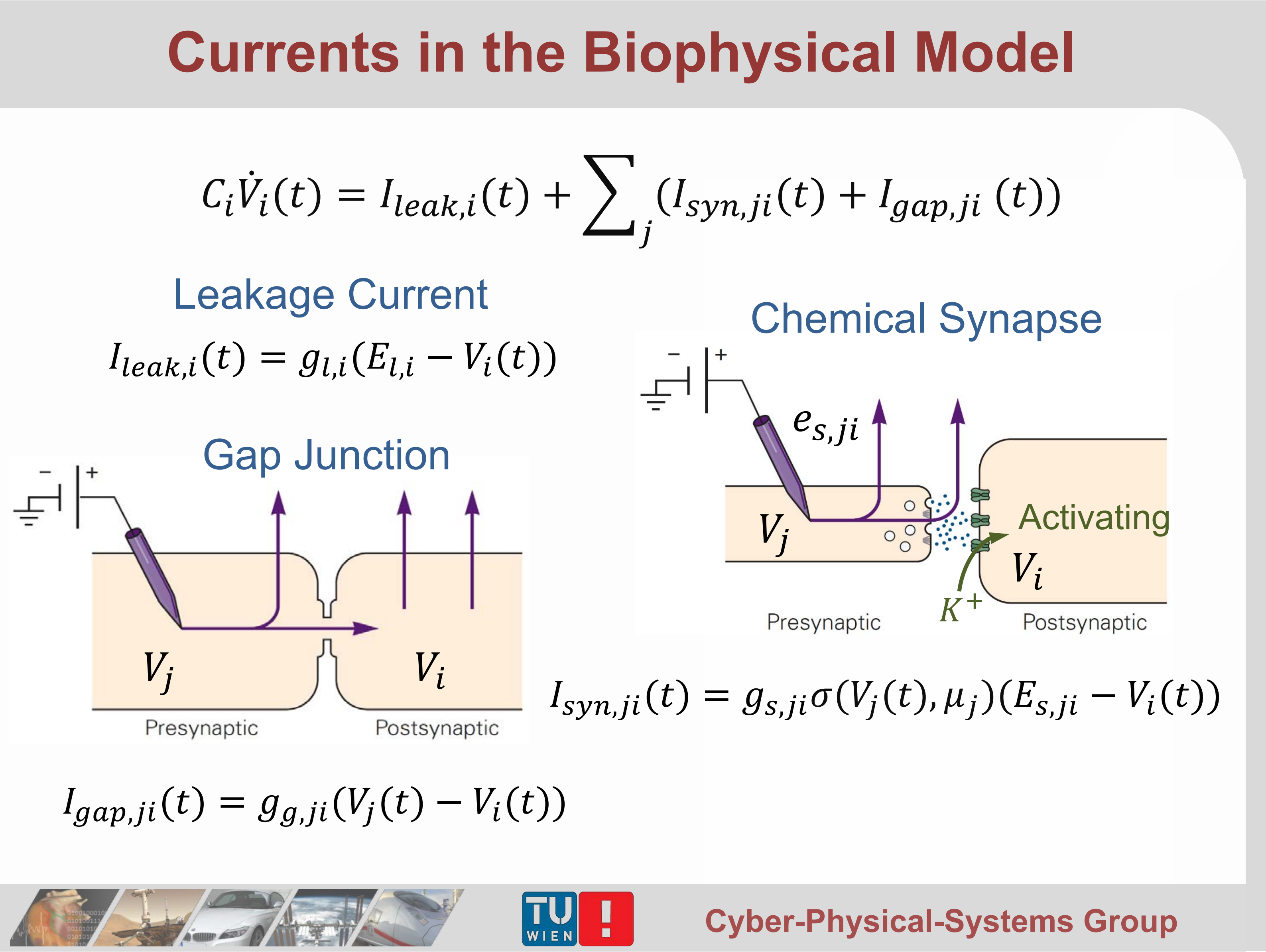
Gap Junction

$$I_{gap,ji}(t) = g_{g,ji}(V_j(t) - V_i(t))$$

Chemical Synapse

$$I_{syn,ji}(t) = g_{s,ji}\sigma(V_j(t), \mu_j)(E_{s,ji} - V_i(t))$$

Cyber-Physical-Systems Group



Currents in the Biophysical Model

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\ (t))$$

Leakage Current

$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

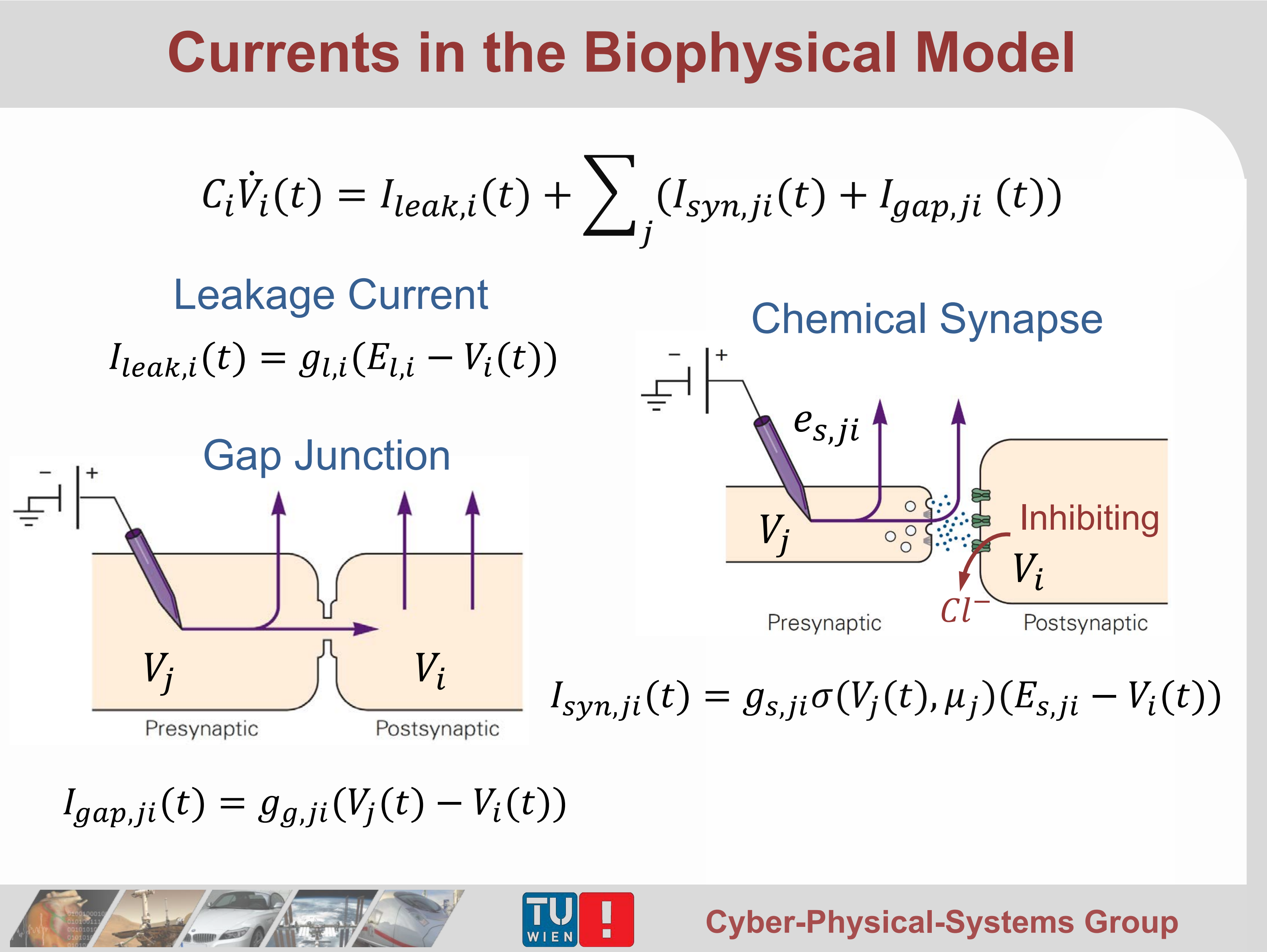
Gap Junction

$$I_{gap,ji}(t) = g_{g,ji}(V_j(t) - V_i(t))$$

Chemical Synapse

$$I_{syn,ji}(t) = g_{s,ji}\sigma(V_j(t), \mu_j)(E_{s,ji} - V_i(t))$$

Cyber-Physical-Systems Group



Currents in the Biophysical Model

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\ (t))$$

Leakage Current

$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

Gap Junction

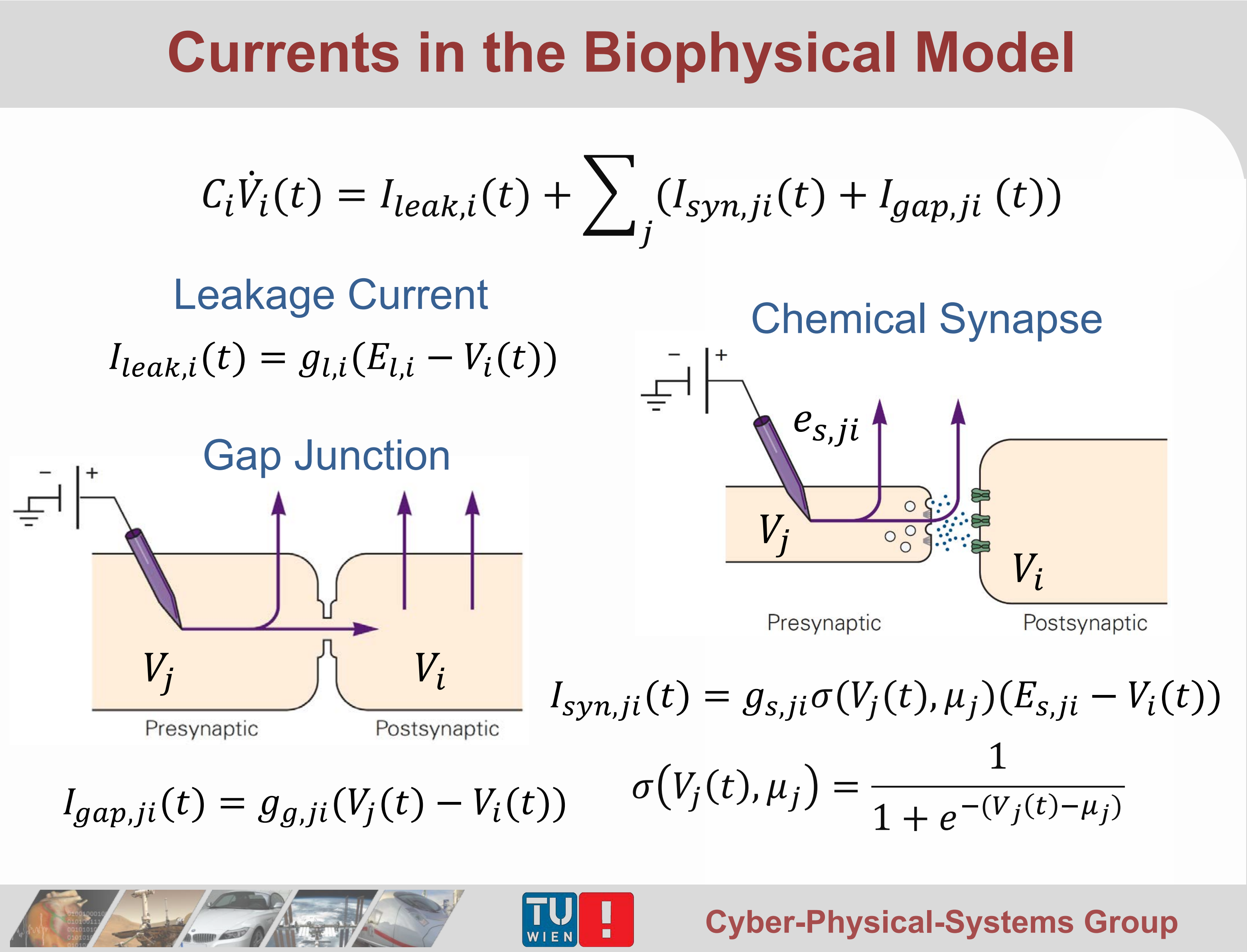
$$I_{gap,ji}(t) = g_{g,ji}(V_j(t) - V_i(t))$$

Chemical Synapse

$$I_{syn,ji}(t) = g_{s,ji}\sigma(V_j(t), \mu_j)(E_{s,ji} - V_i(t))$$

TU WIEN

Cyber-Physical-Systems Group



Currents in the Biophysical Model

$$C_i\dot{V}_i(t) = I_{leak,i}(t) + \sum_j (I_{syn,ji}(t) + I_{gap,ji}\,(t))$$

Leakage Current

$$I_{leak,i}(t) = g_{l,i}(E_{l,i} - V_i(t))$$

Gap Junction

$$I_{gap,ji}(t) = g_{g,ji}(V_j(t) - V_i(t))$$

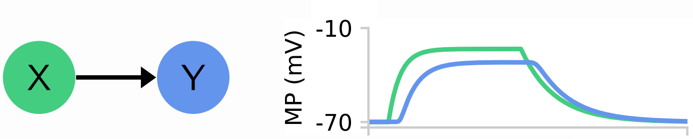
Chemical Synapse

$$I_{syn,ji}(t) = g_{s,ji}\sigma(V_j(t),\mu_j)(E_{s,ji} - V_i(t))$$

$$\sigma\big(V_j(t),\mu_j\big) = \frac{1}{1 + e^{-(V_j(t)-\mu_j)}}$$

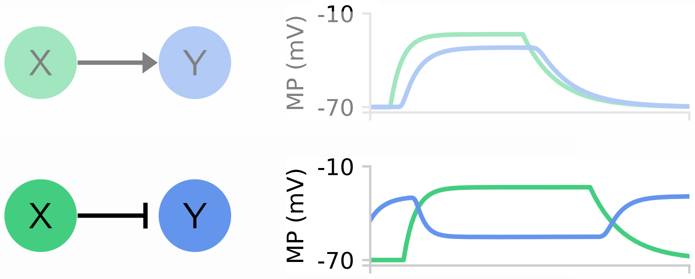
Cyber-Physical-Systems Group

Primitive Policy Motifs



Excitation

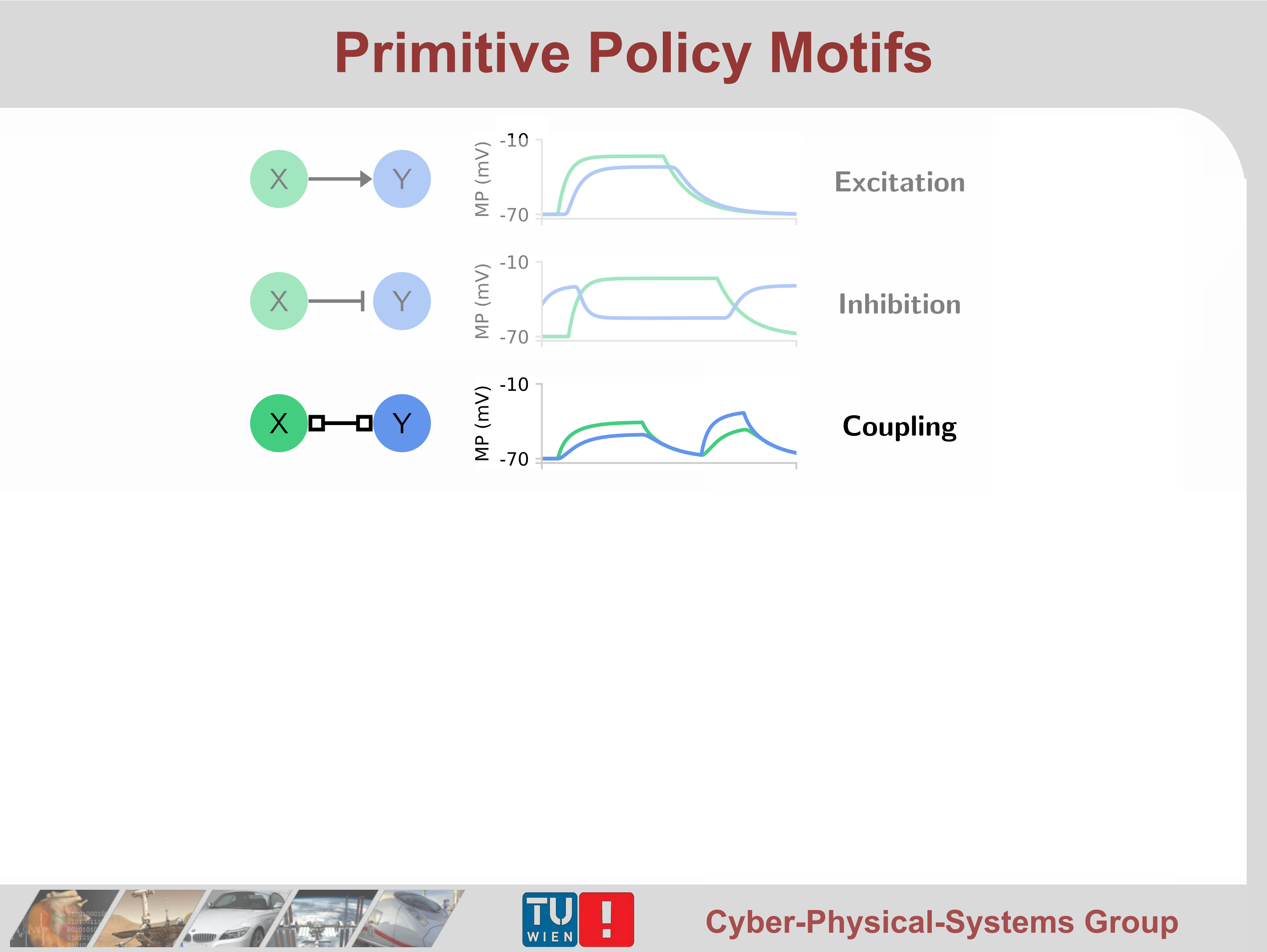
Primitive Policy Motifs



Excitation

Inhibition

Cyber-Physical-Systems Group



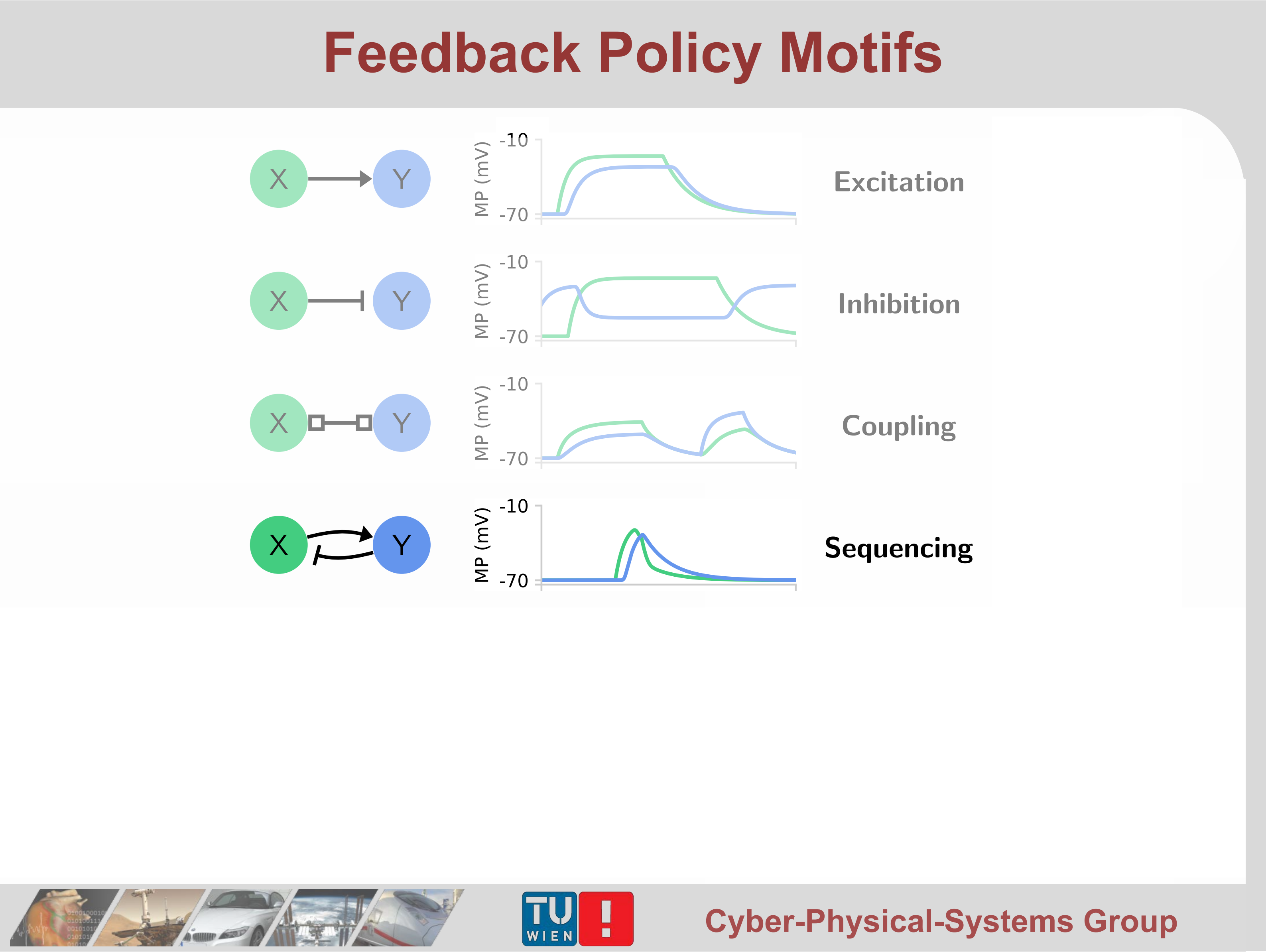
Primitive Policy Motifs

Excitation

Inhibition

Coupling

Cyber-Physical-Systems Group



Feedback Policy Motifs

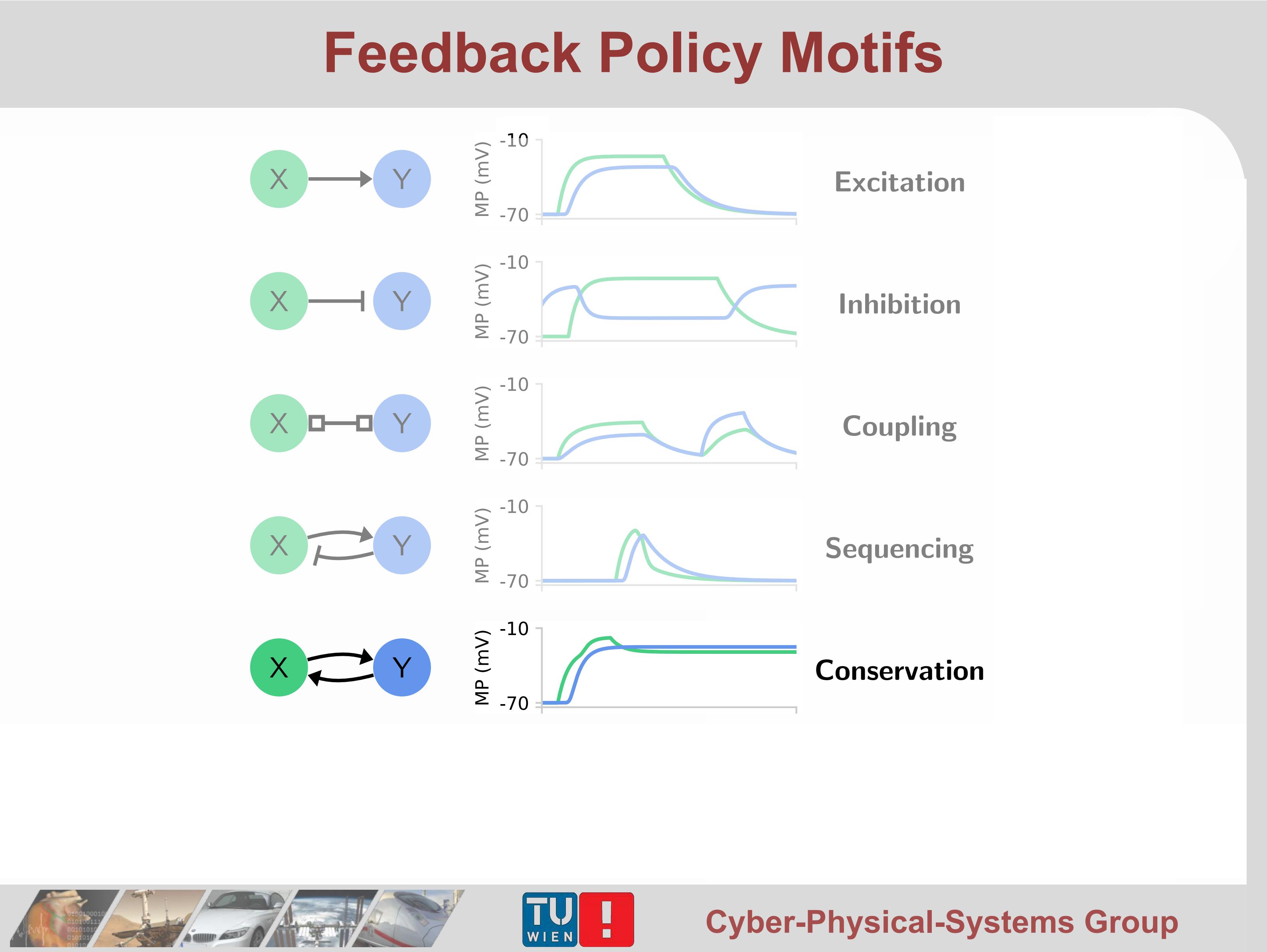
Excitation

Inhibition

Coupling

Sequencing

Cyber-Physical-Systems Group



Feedback Policy Motifs

Excitation

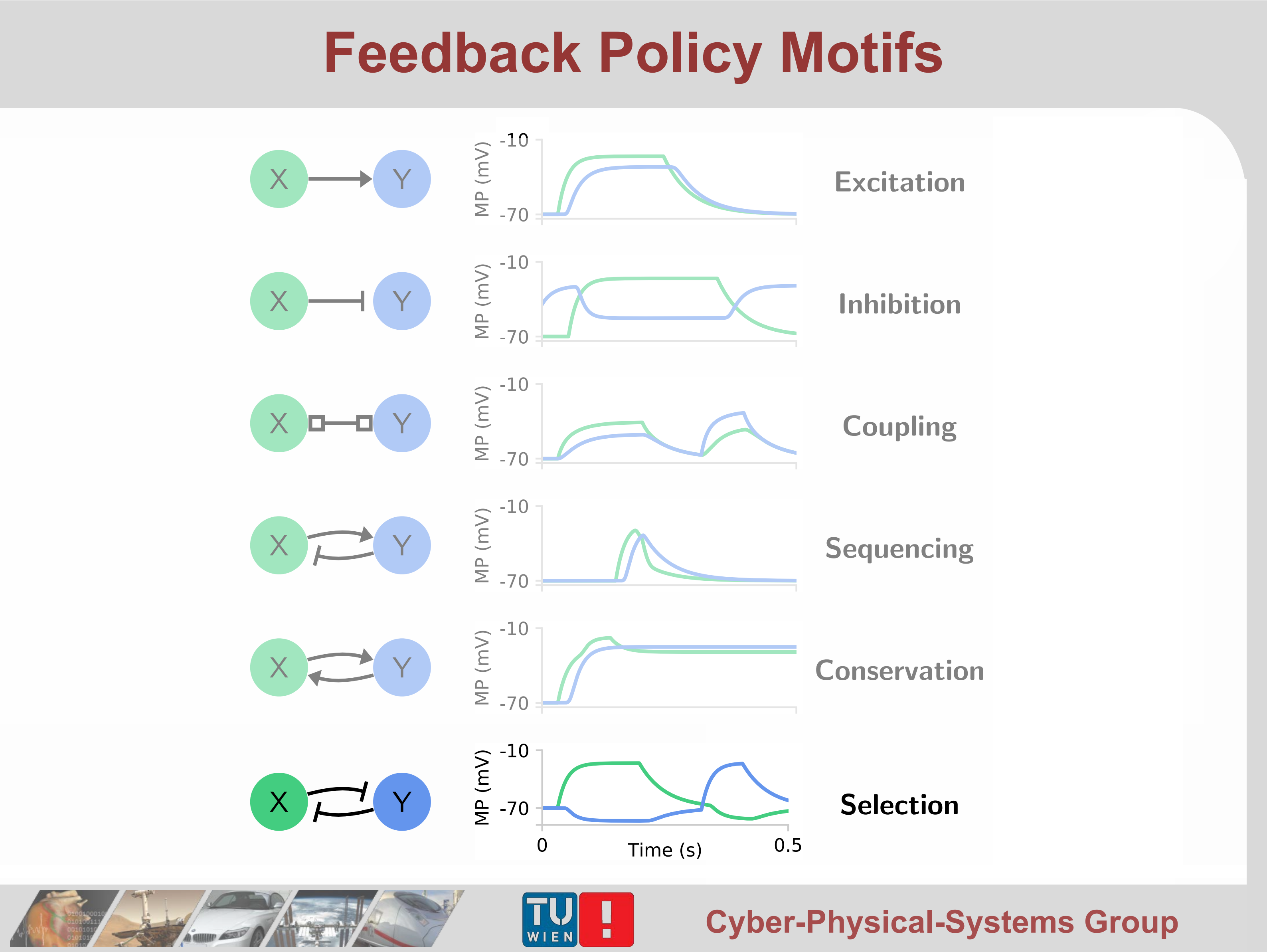
Inhibition

Coupling

Sequencing

Conservation

Cyber-Physical-Systems Group



Feedback Policy Motifs

Excitation

Inhibition

Coupling

Sequencing

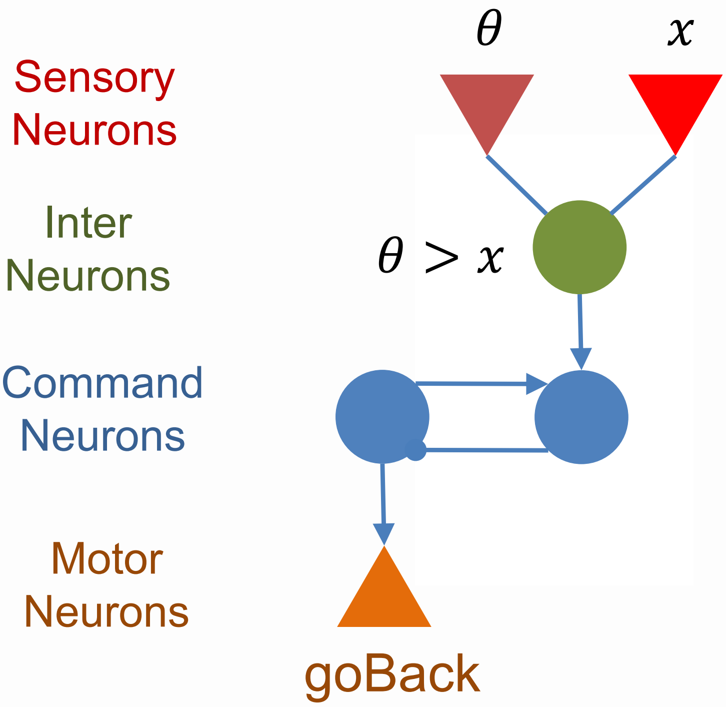
Conservation

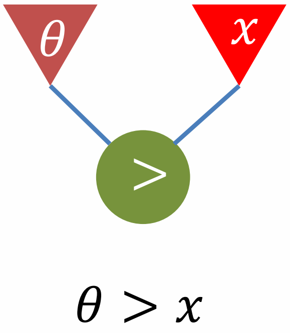
Selection

Cyber-Physical-Systems Group

©MECO.net

Policy Motifs: Example



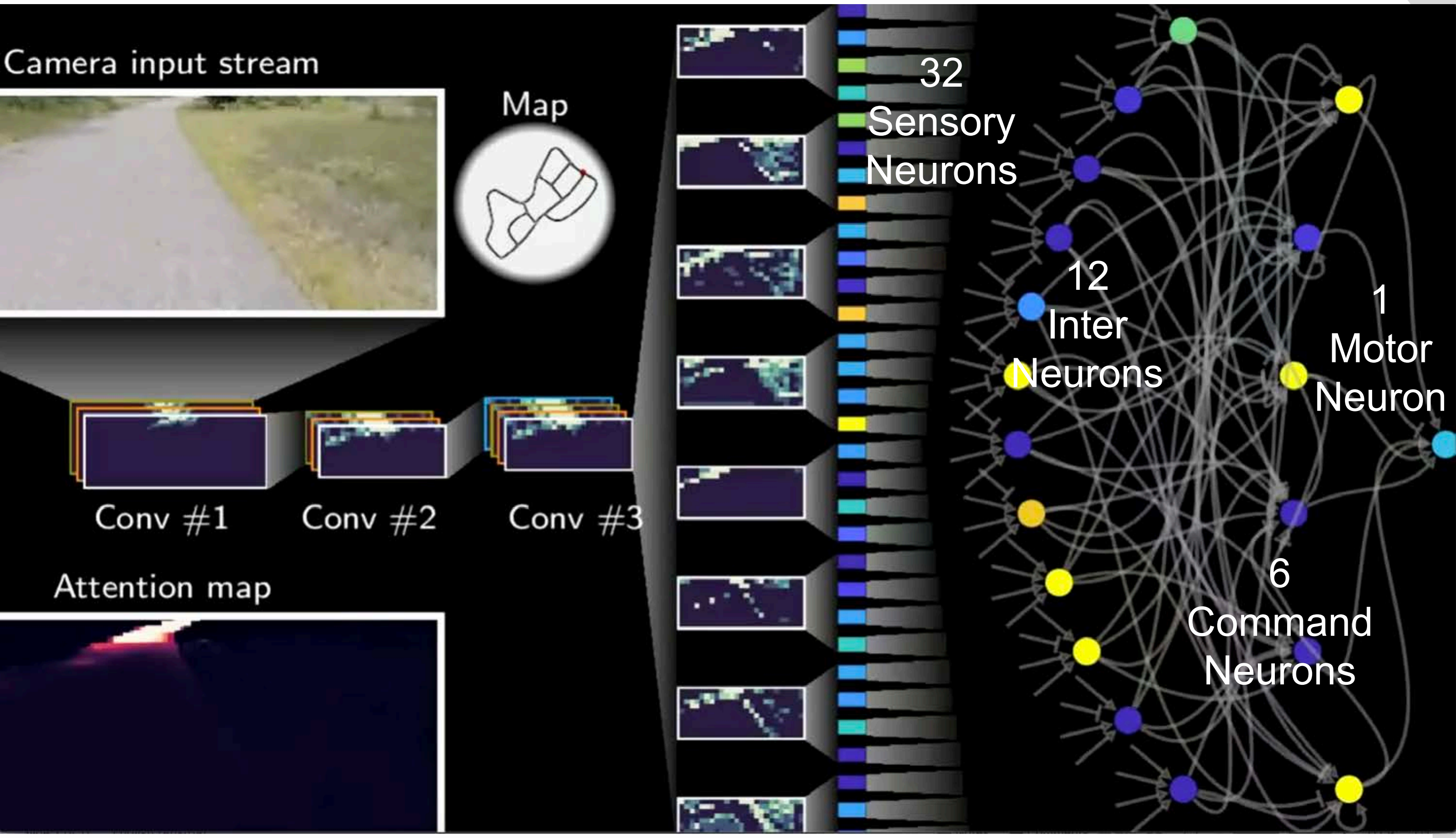


while $(\theta \leq x)$
goBack

Cyber-Physical-Systems Group

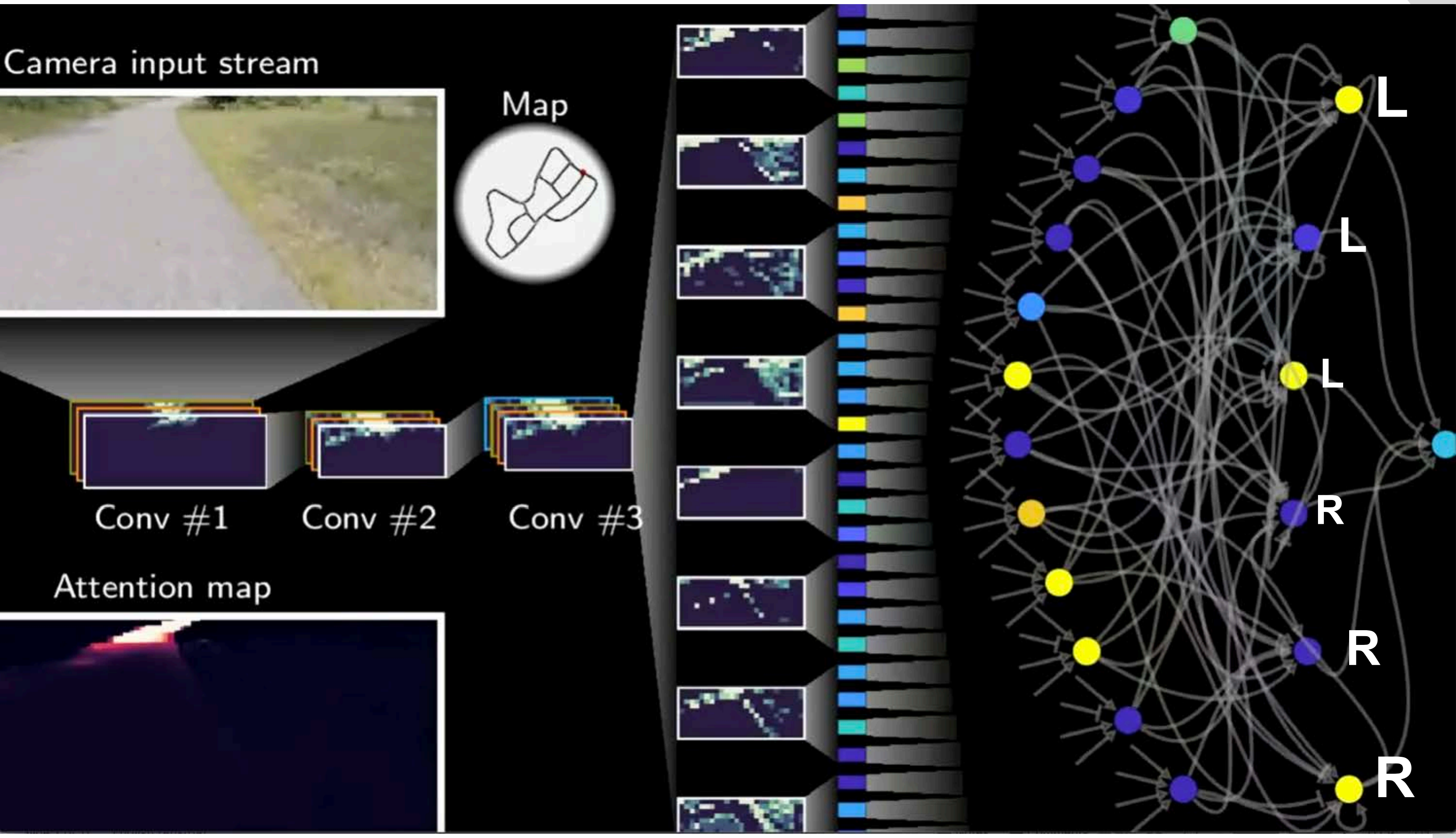
©MECO.net

NCP Architecture for Lane Keeping

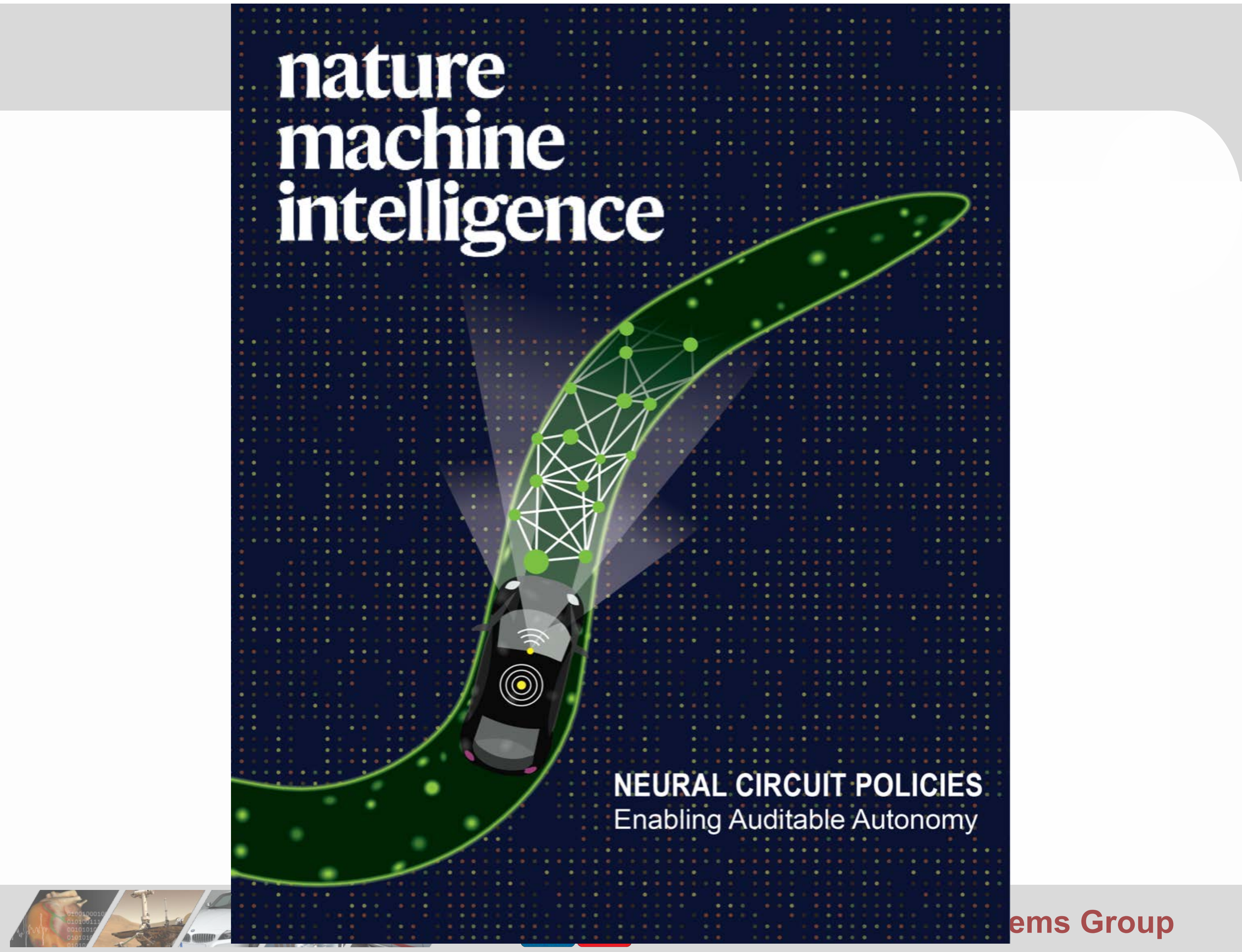


Cyber-Physical-Systems Group

NCP Architecture for Lane Keeping



Cyber-Physical-Systems Group



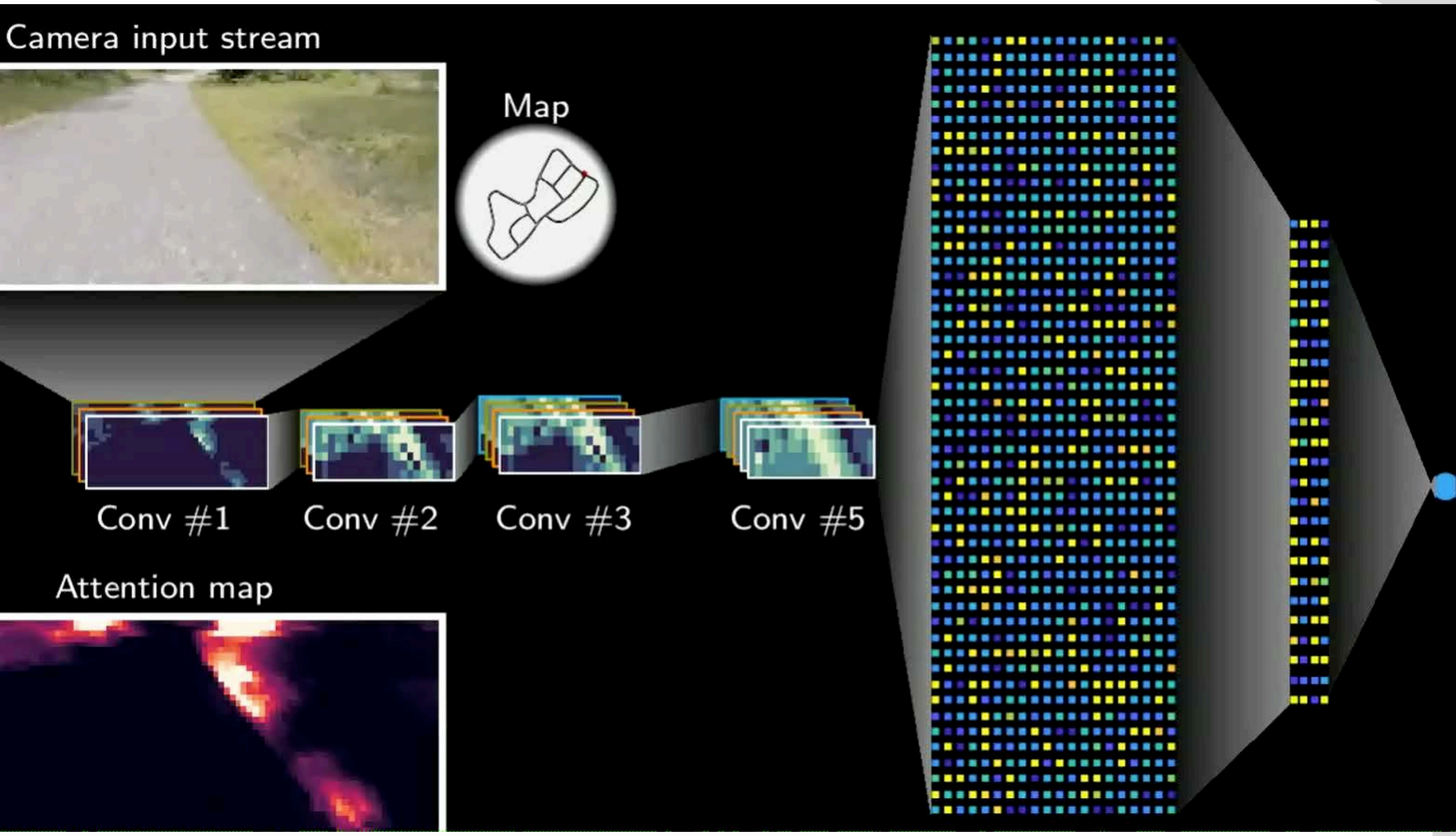
nature machine intelligence

NEURAL CIRCUIT POLICIES

Enabling Auditable Autonomy

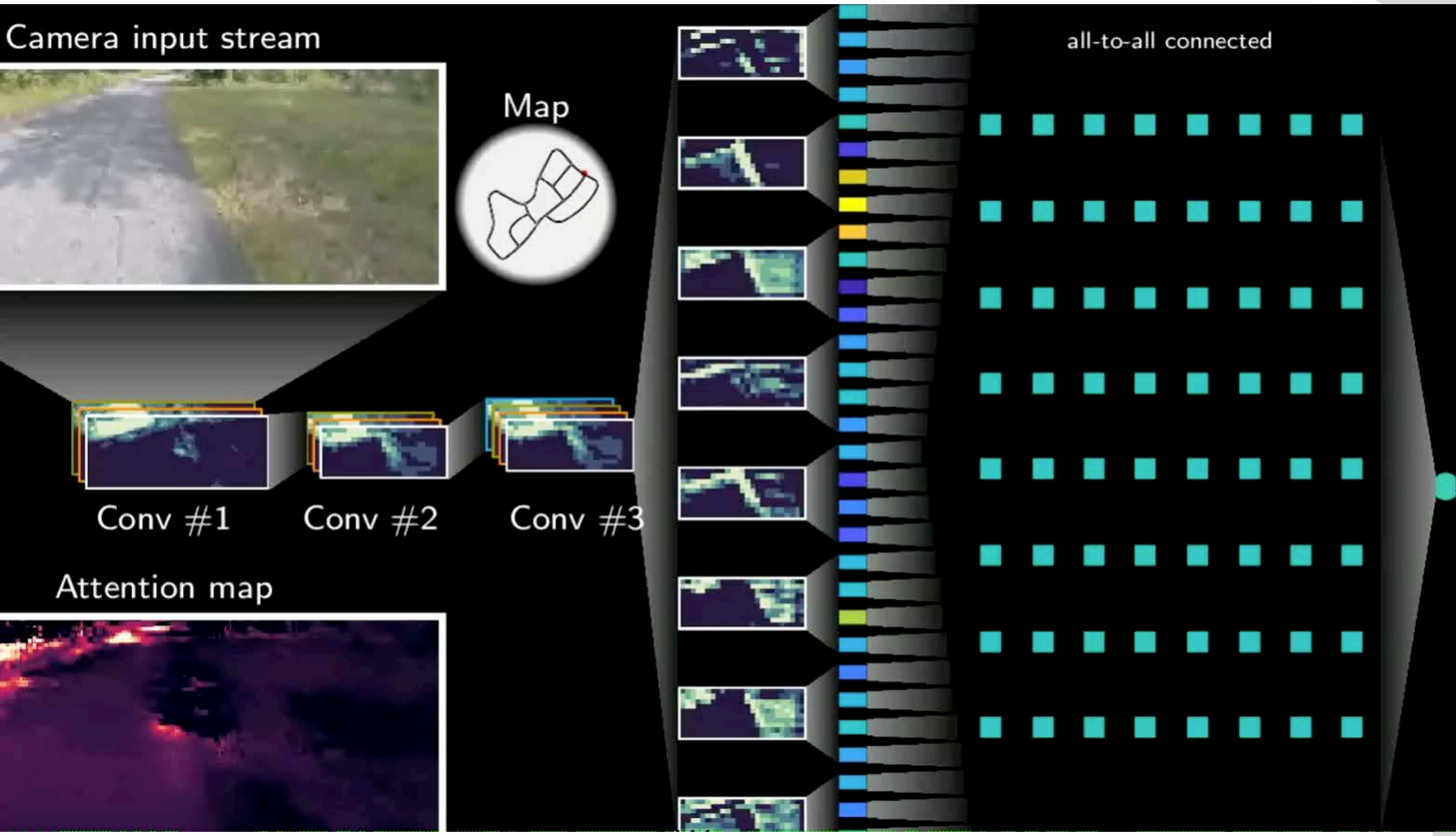
ems Group

Convolutional Neural Networks in Action



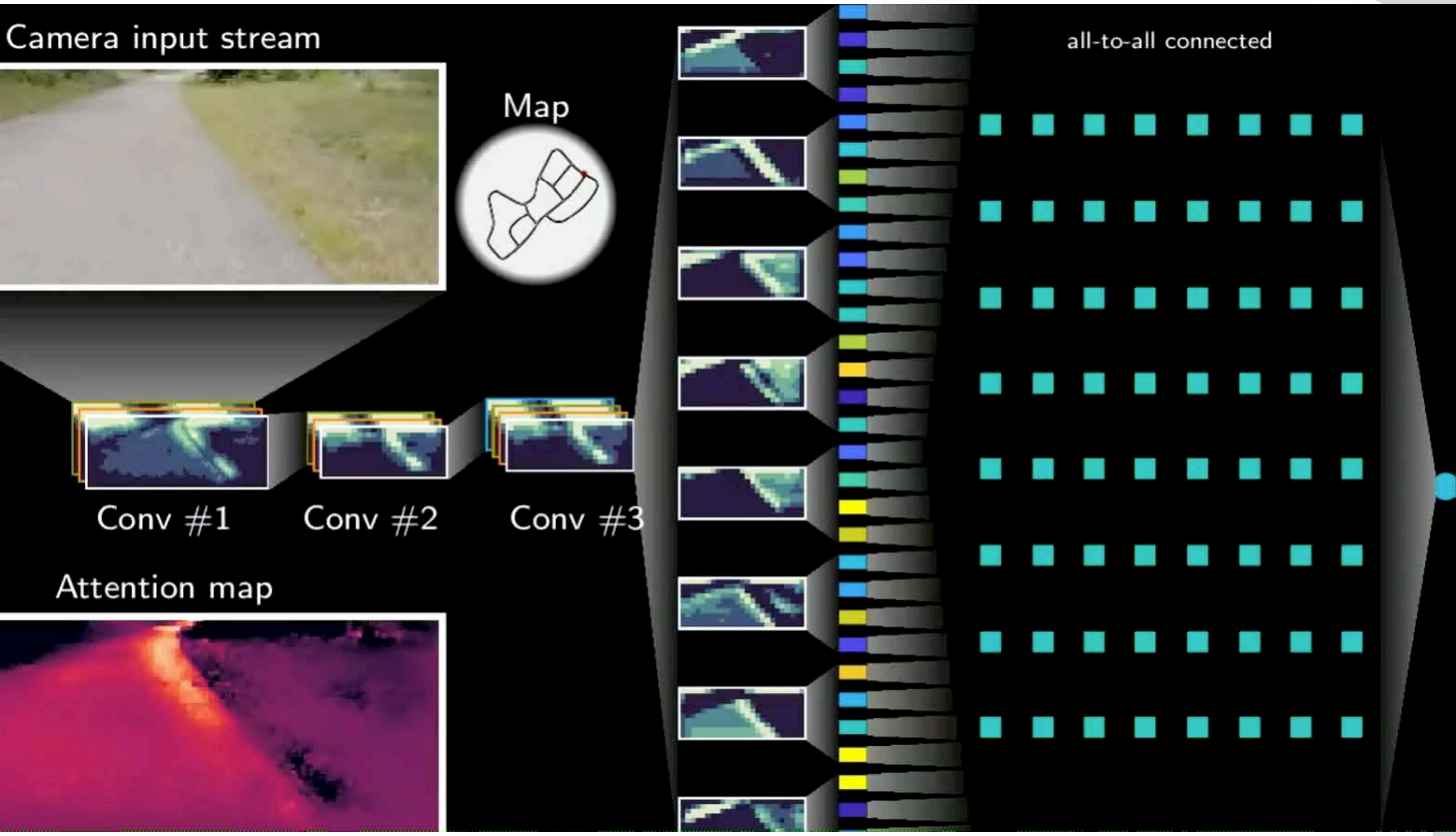
Cyber-Physical-Systems Group

Continuous-Time RNNs in Action



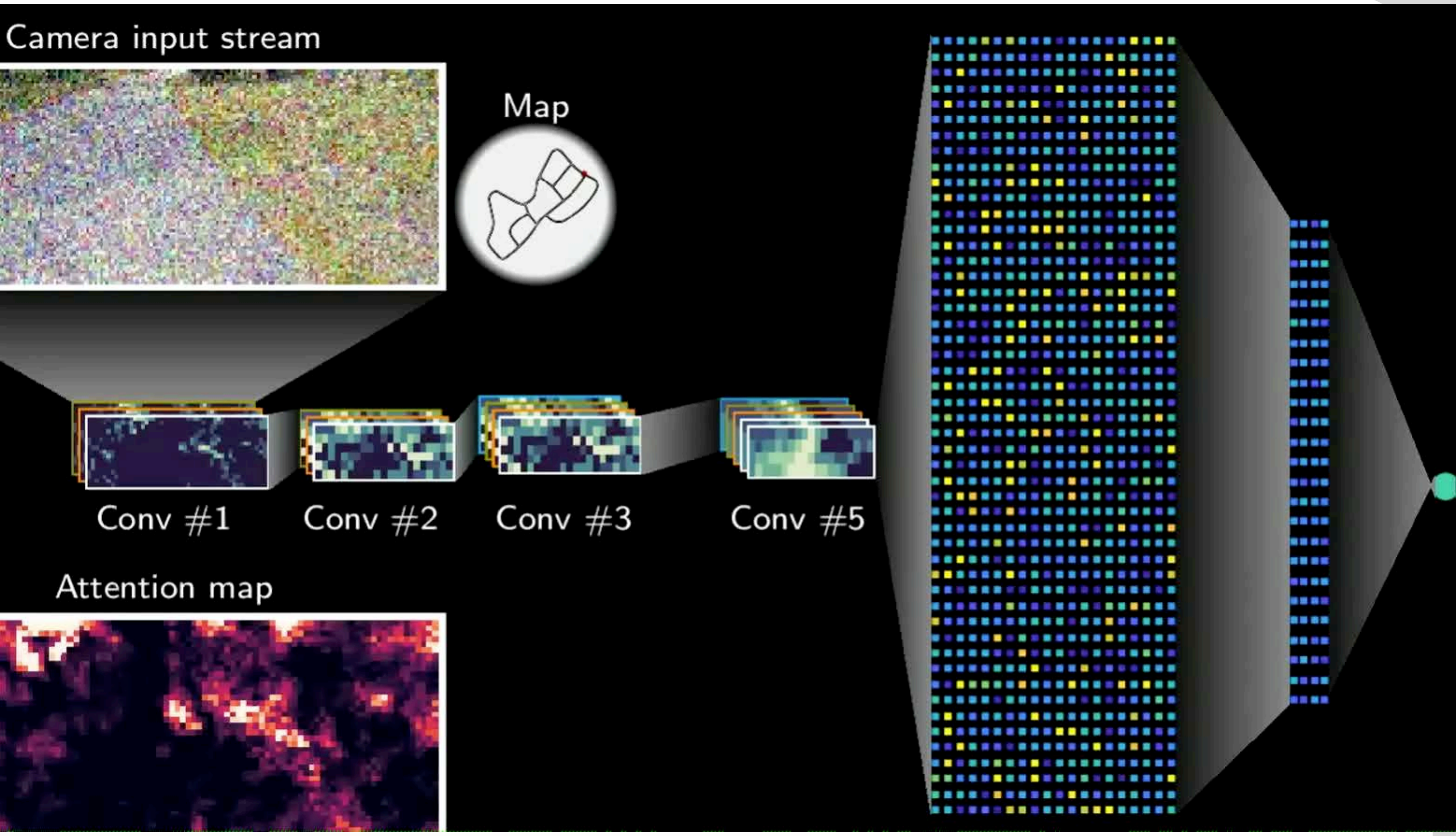
Cyber-Physical-Systems Group

Long-Short-Term-Memory NNs in Action



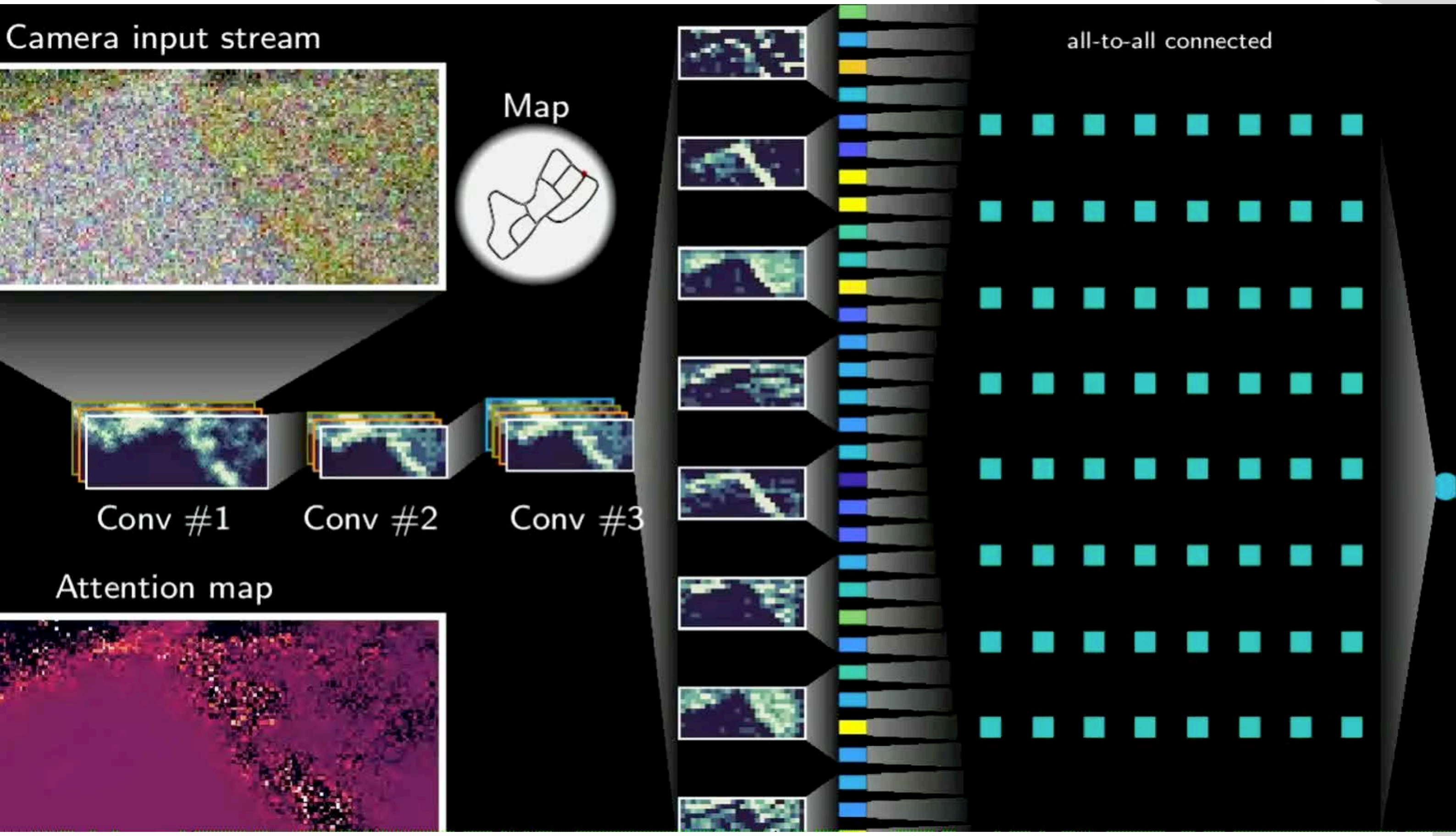
Cyber-Physical-Systems Group

Convolutional Neural Networks: Noisy Input



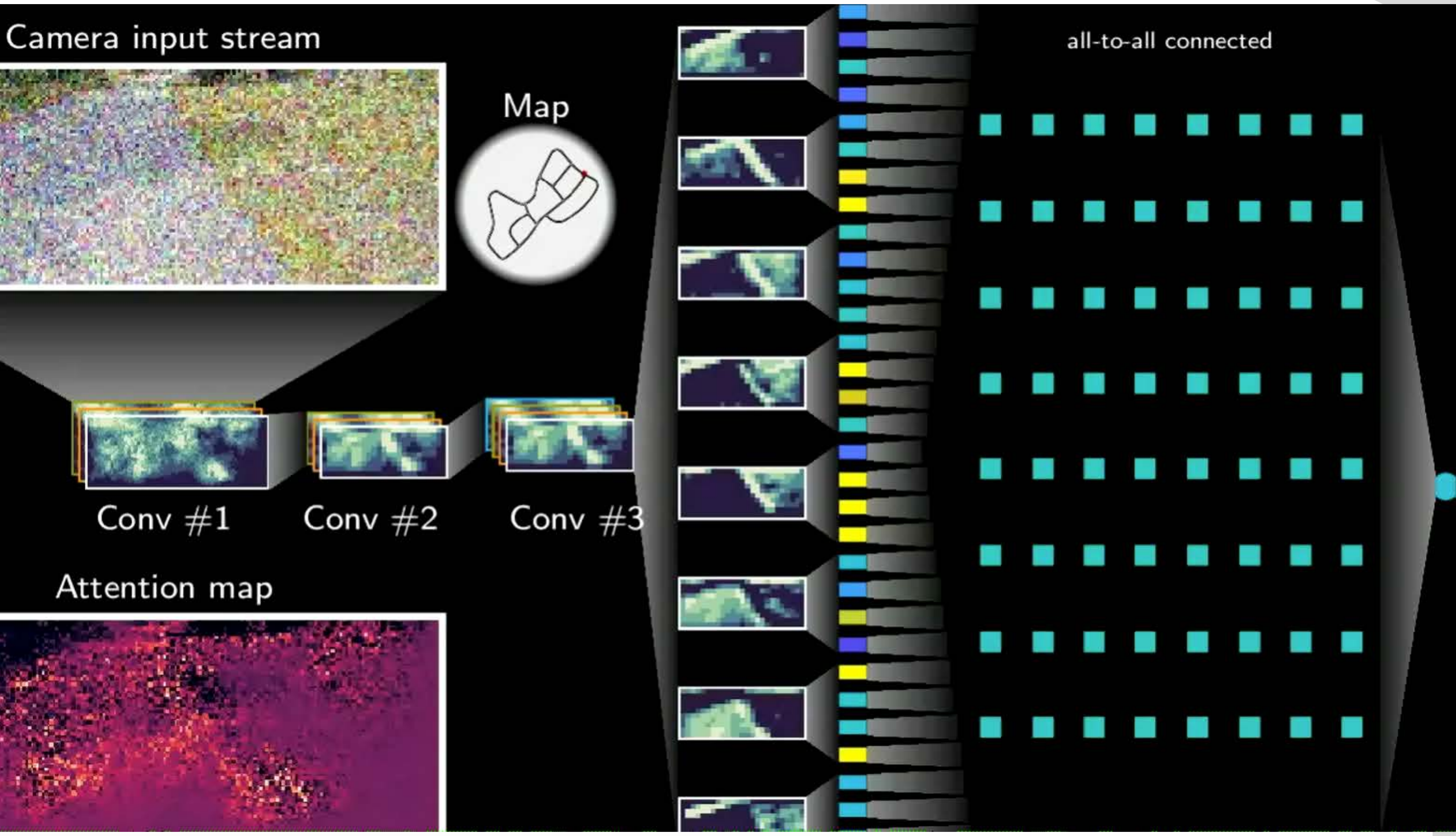
Cyber-Physical-Systems Group

Continuous-Time RNNs: Noisy Input

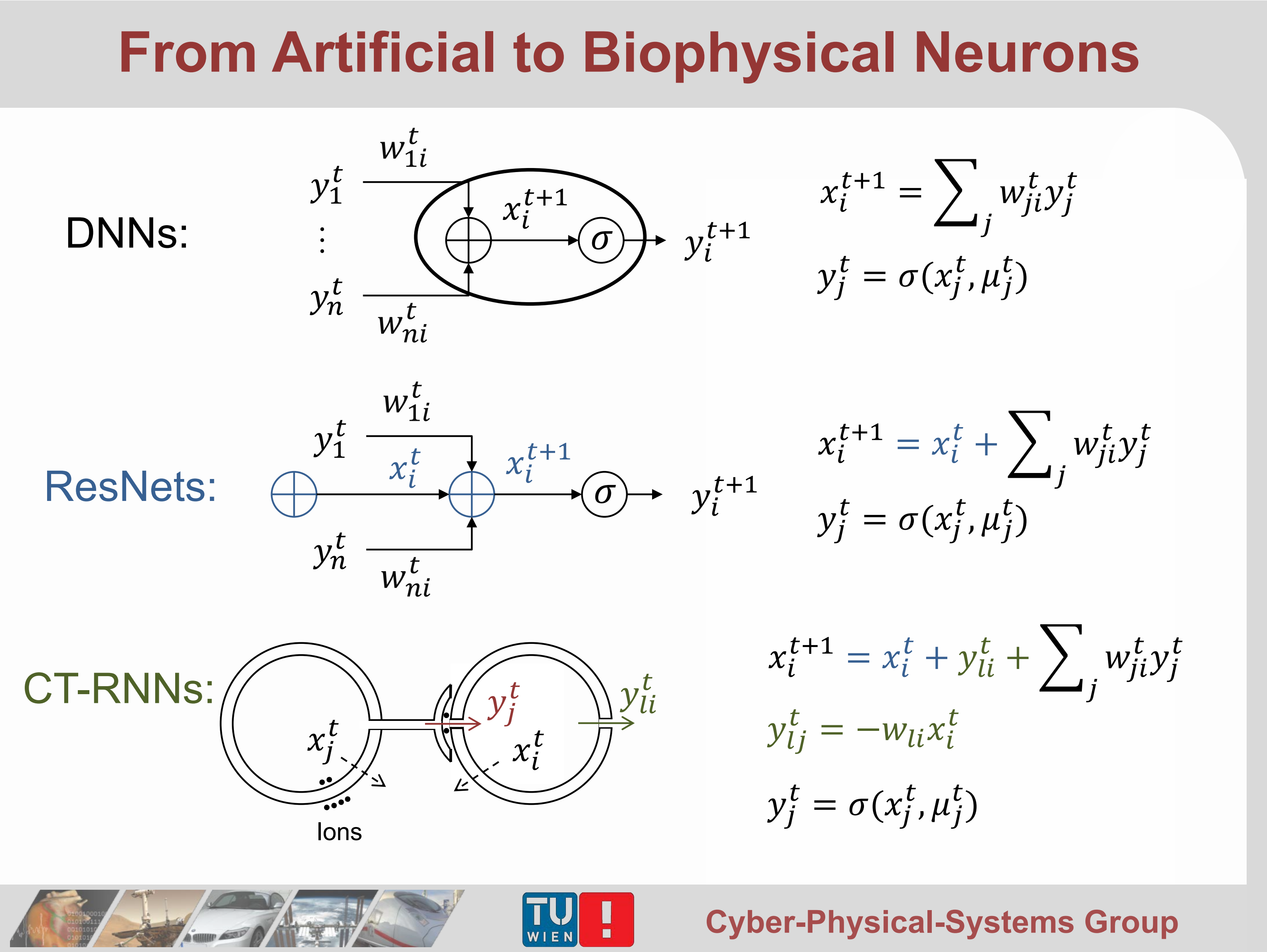


Cyber-Physical-Systems Group

Long-Short-Term-Memory NNs: Noisy Input



Cyber-Physical-Systems Group



From Artificial to Biophysical Neurons

DNNs:

$$x_i^{t+1} = \sum_j w_{ji}^t y_j^t$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)$$

ResNets:

$$x_i^{t+1} = x_i^t + \sum_j w_{ji}^t y_j^t$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)$$

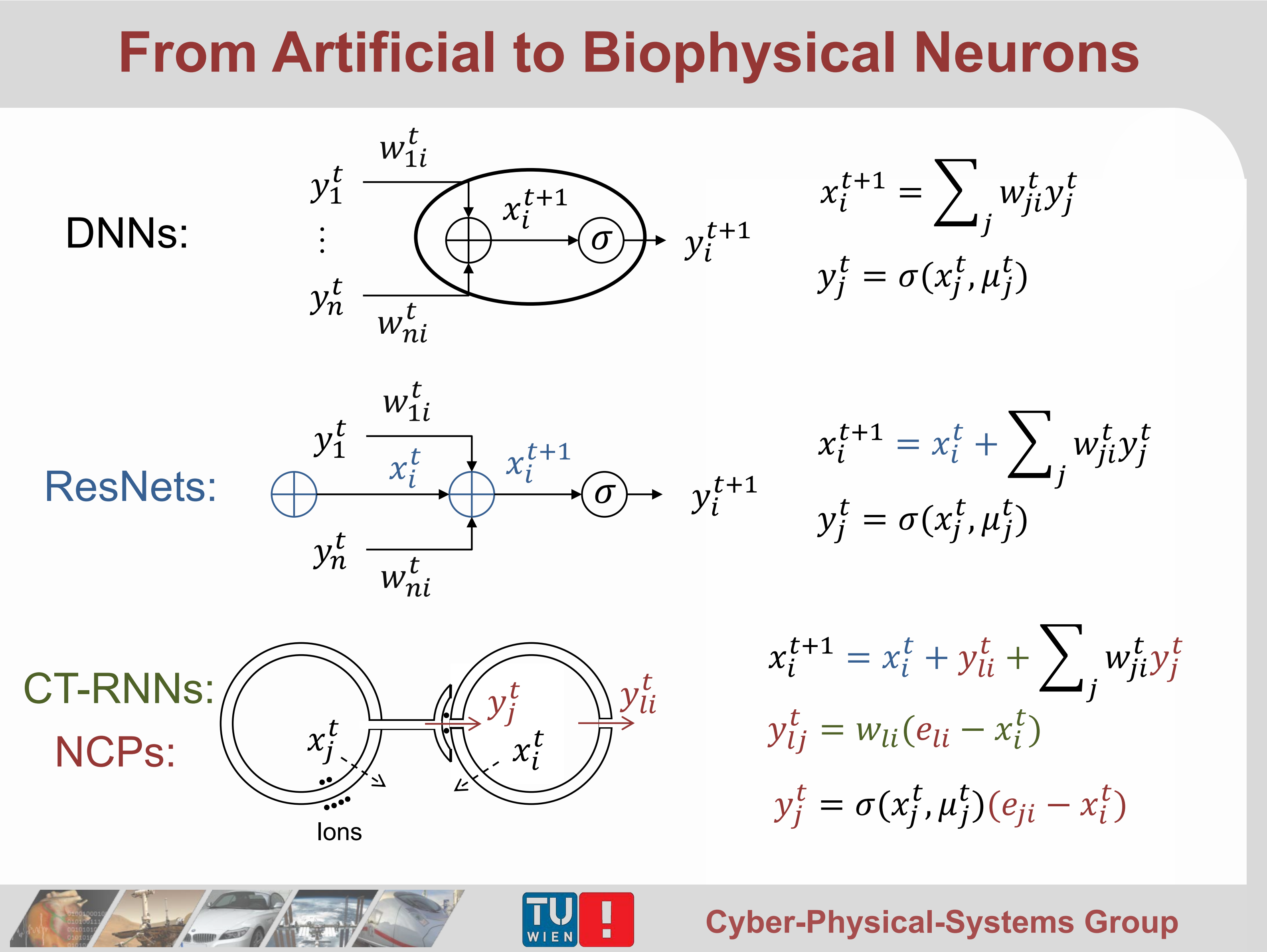
CT-RNNs:

$$x_i^{t+1} = x_i^t + y_{li}^t + \sum_j w_{ji}^t y_j^t$$

$$y_{lj}^t = -w_{li} x_i^t$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)$$

Cyber-Physical-Systems Group



From Artificial to Biophysical Neurons

DNNs:

$$x_i^{t+1} = \sum_j w_{ji}^t y_j^t$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)$$

ResNets:

$$x_i^{t+1} = x_i^t + \sum_j w_{ji}^t y_j^t$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)$$

CT-RNNs:

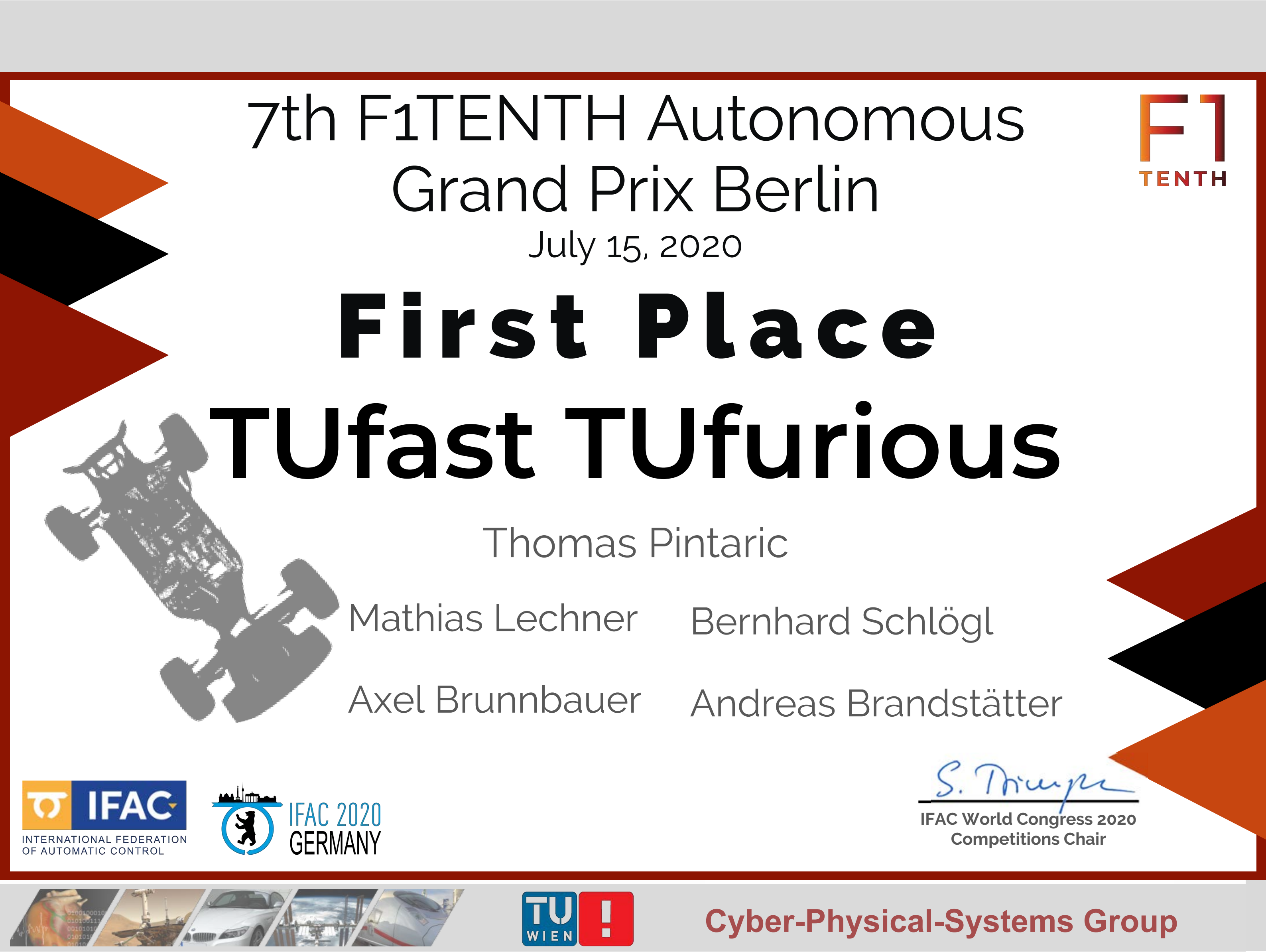
NCPs:

$$x_i^{t+1} = x_i^t + y_{li}^t + \sum_j w_{ji}^t y_j^t$$

$$y_{lj}^t = w_{li}(e_{li} - x_i^t)$$

$$y_j^t = \sigma(x_j^t, \mu_j^t)(e_{ji} - x_i^t)$$

Cyber-Physical-Systems Group



7th F1TENTH Autonomous Grand Prix Berlin

July 15, 2020

F1 TENTH

First Place

TUfast TUfurious

Thomas Pintaric

Mathias Lechner

Bernhard Schlögl

Axel Brunnbauer

Andreas Brandstätter

IFAC INTERNATIONAL FEDERATION OF AUTOMATIC CONTROL

IFAC 2020 GERMANY

IFAC World Congress 2020
Competitions Chair

TU WIEN

Cyber-Physical-Systems Group

IFAC World Congress, Berlin Grand PRX

Virtual Autonomous Racing

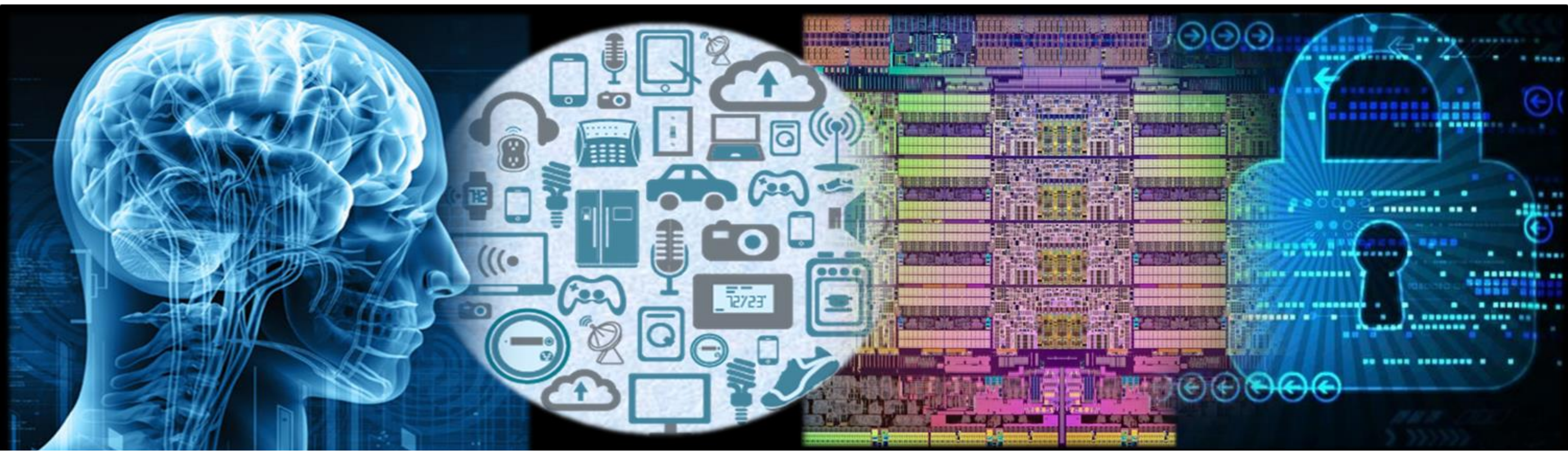
TUW Winner Team: TUfast TUfurious

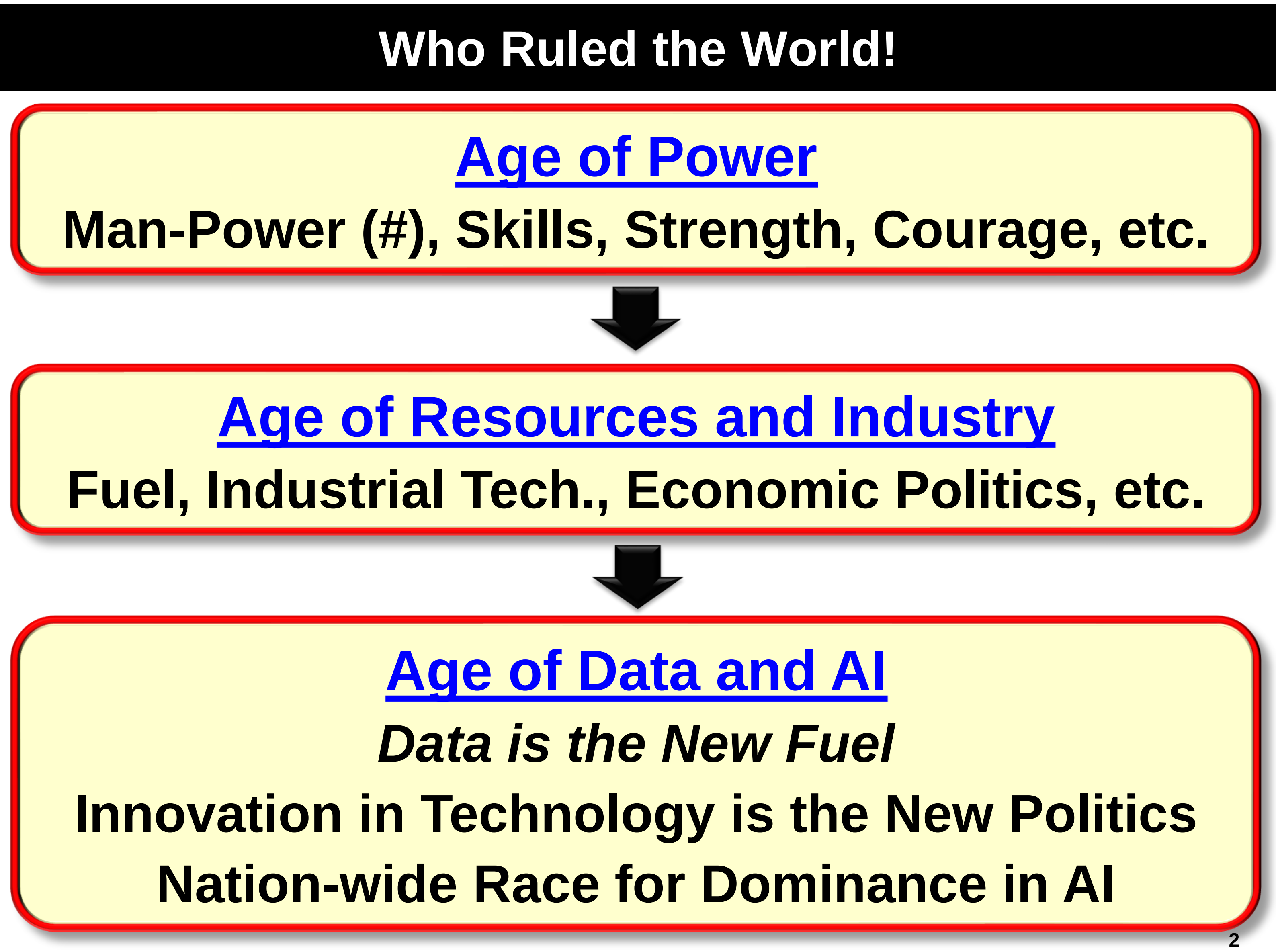
جامعة نيويورك أبوظبي NYU ABU DHABI
NYU TANDON SCHOOL OF ENGINEERING
CENTER FOR CYBER SECURITY sites.nyuad.nyu.edu/ccs-ad/
CARE Tech Computer Architecture and Robust, Energy-Efficient Technologies Group
TU WIEN

Energy-Efficiency and Security for Edge-AI:

Challenges and Opportunities

A. Marchisio, M. A. Hanif, M. Shafique
Vienna University of Technology (TU Wien), Austria
New York University Abu Dhabi (NYUAD), UAE





Who Ruled the World!

Age of Power

Man-Power (#), Skills, Strength, Courage, etc.

Age of Resources and Industry

Fuel, Industrial Tech., Economic Politics, etc.

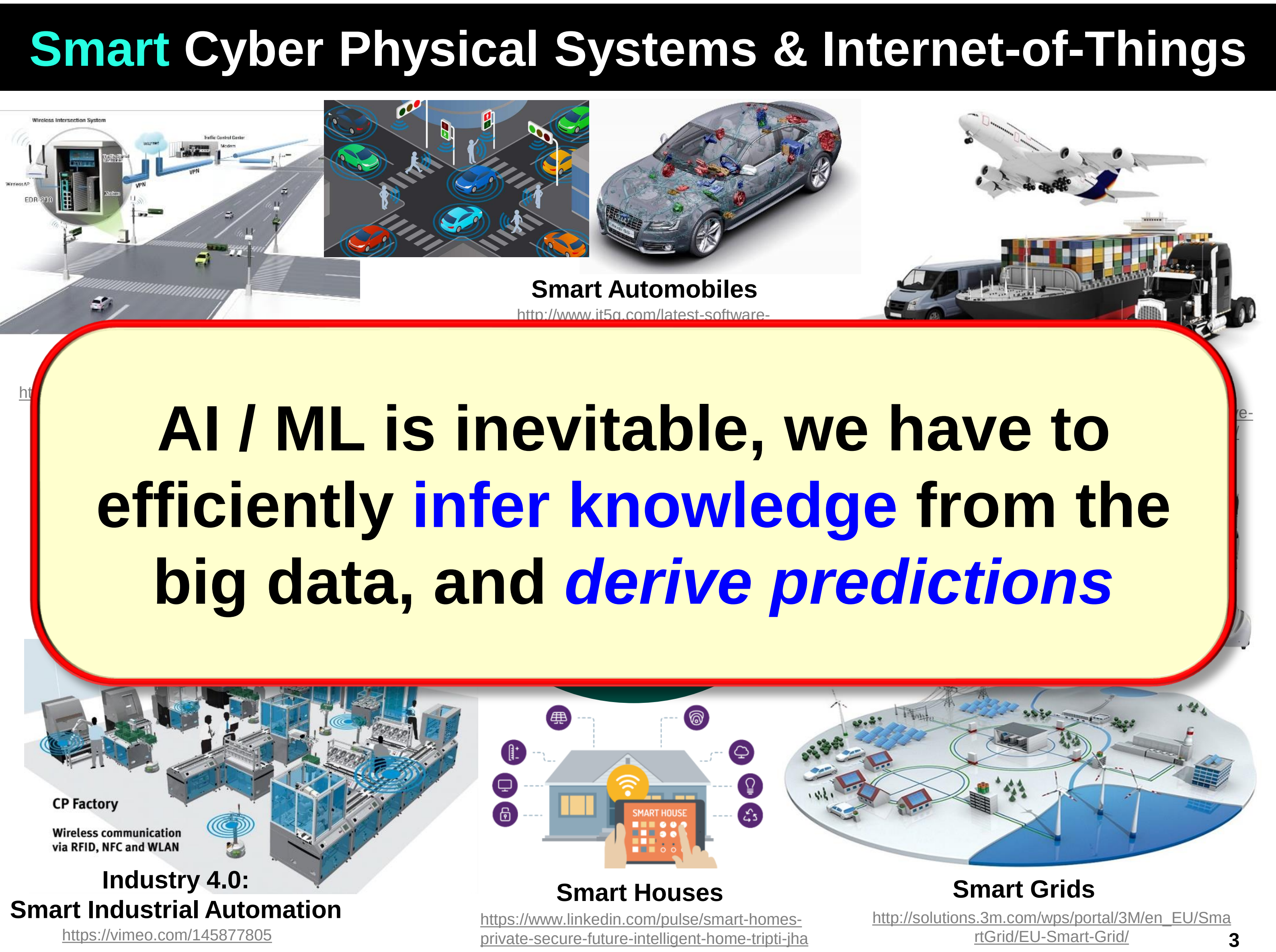
Age of Data and AI

Data is the New Fuel

Innovation in Technology is the New Politics

Nation-wide Race for Dominance in AI

2


Wireless Intersection System
CP Factory
Wireless communication via RFID, NFC and WLAN
SMART HOUSE

Smart Cyber Physical Systems & Internet-of-Things

Smart Automobiles

http://www.it5g.com/latest-software-

ht

re-

AI / ML is inevitable, we have to efficiently *infer knowledge* from the big data, and *derive predictions*

Industry 4.0:
Smart Industrial Automation
https://vimeo.com/145877805

Smart Houses
https://www.linkedin.com/pulse/smart-homes-private-secure-future-intelligent-home-tripti-jha

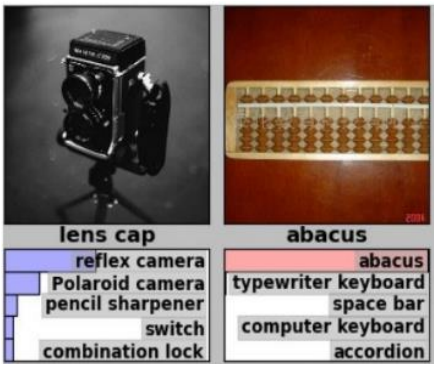
Smart Grids
http://solutions.3m.com/wps/portal/3M/en_EU/SmartGrid/EU-Smart-Grid/

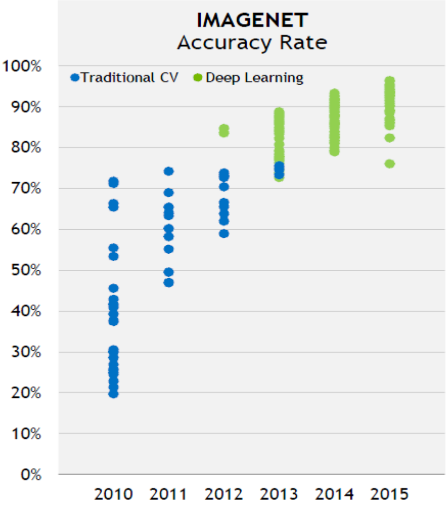
3

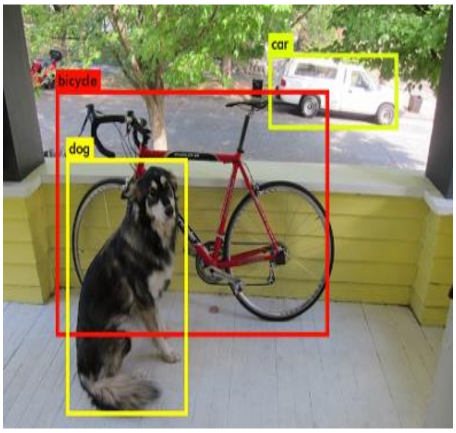
AI / ML Applications => require High Efficiency Gains

Autonomous Driving

Image Classification







Object Detection & Localization

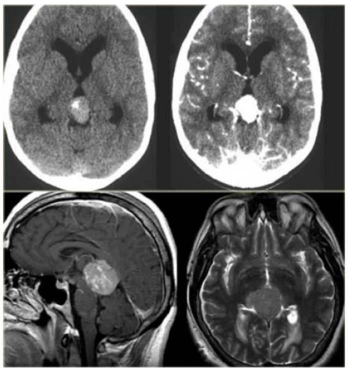
Machine Translation

Natural Language Processing

nature
At last – a computer program that can beat a champion Go player
ALL SYSTEMS GO

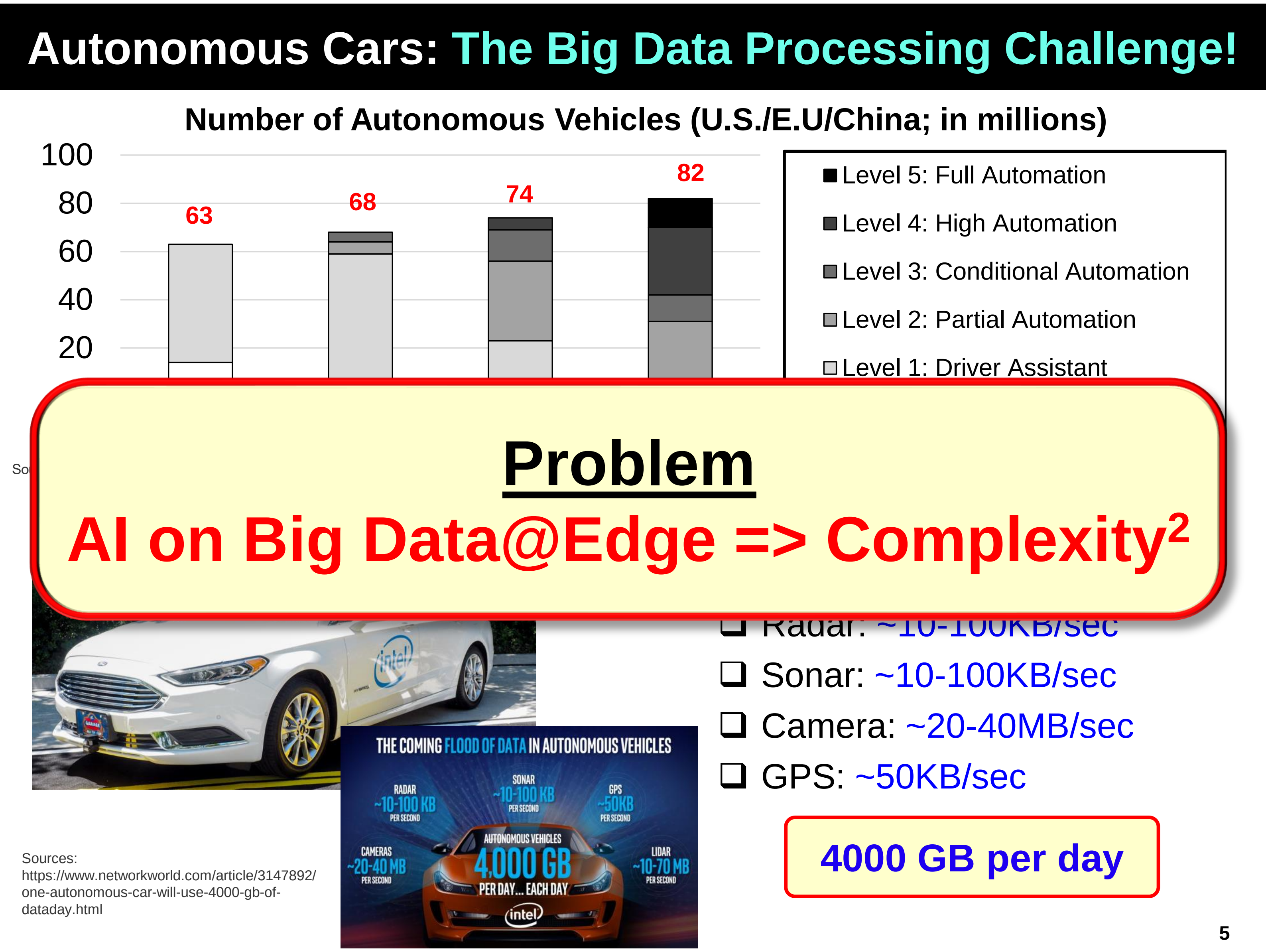
Strategy Games

Forex/Stocks Trading 4



Cancer Detection

©MECO.net



Autonomous Cars: The Big Data Processing Challenge!

Number of Autonomous Vehicles (U.S./E.U/China; in millions)

100
80
60
40
20
63
68
74
82
■ Level 5: Full Automation
■ Level 4: High Automation
■ Level 3: Conditional Automation
■ Level 2: Partial Automation
□ Level 1: Driver Assistant
So

Problem

AI on Big Data@Edge => Complexity²

❑ Radar: ~10-100KB/sec

❑ Sonar: ~10-100KB/sec

❑ Camera: ~20-40MB/sec

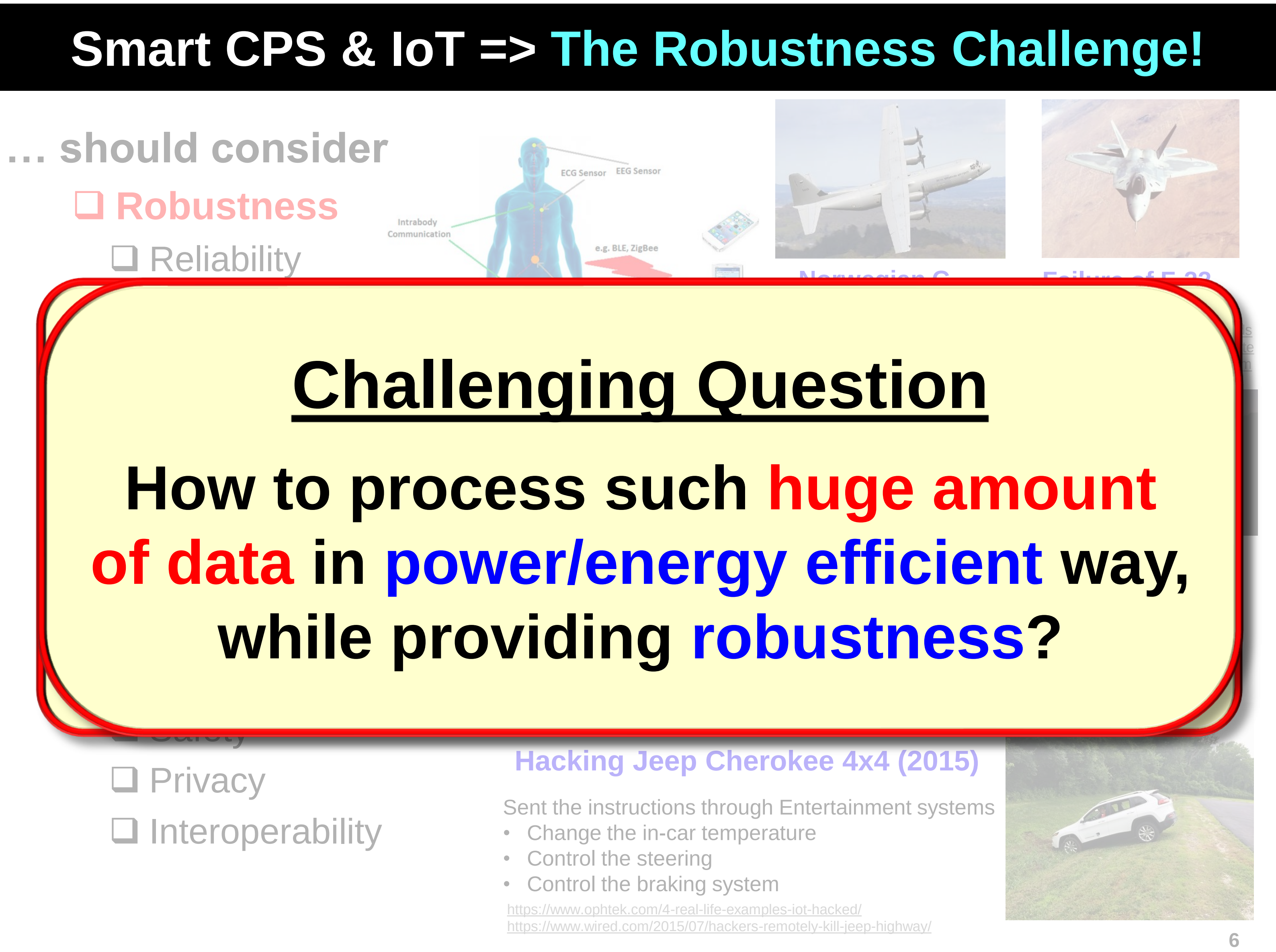
❑ GPS: ~50KB/sec

4000 GB per day

THE COMING FLOOD OF DATA IN AUTONOMOUS VEHICLES
RADAR ~10-100 KB PER SECOND
SONAR ~10-100 KB PER SECOND
GPS ~50KB PER SECOND
CAMERAS ~20-40 MB PER SECOND
AUTONOMOUS VEHICLES 4,000 GB PER DAY... EACH DAY
LIDAR ~10-70 MB PER SECOND
intel

Sources: https://www.networkworld.com/article/3147892/one-autonomous-car-will-use-4000-gb-of-dataday.html

5



Smart CPS & IoT => The Robustness Challenge!

… should consider

❑ Robustness

❑ Reliability

❑ Safety

❑ Privacy

❑ Interoperability

ECG Sensor
EEG Sensor
Intrabody Communication
e.g. BLE, ZigBee

Challenging Question

How to process such huge amount of data in power/energy efficient way, while providing robustness?

Hacking Jeep Cherokee 4x4 (2015)

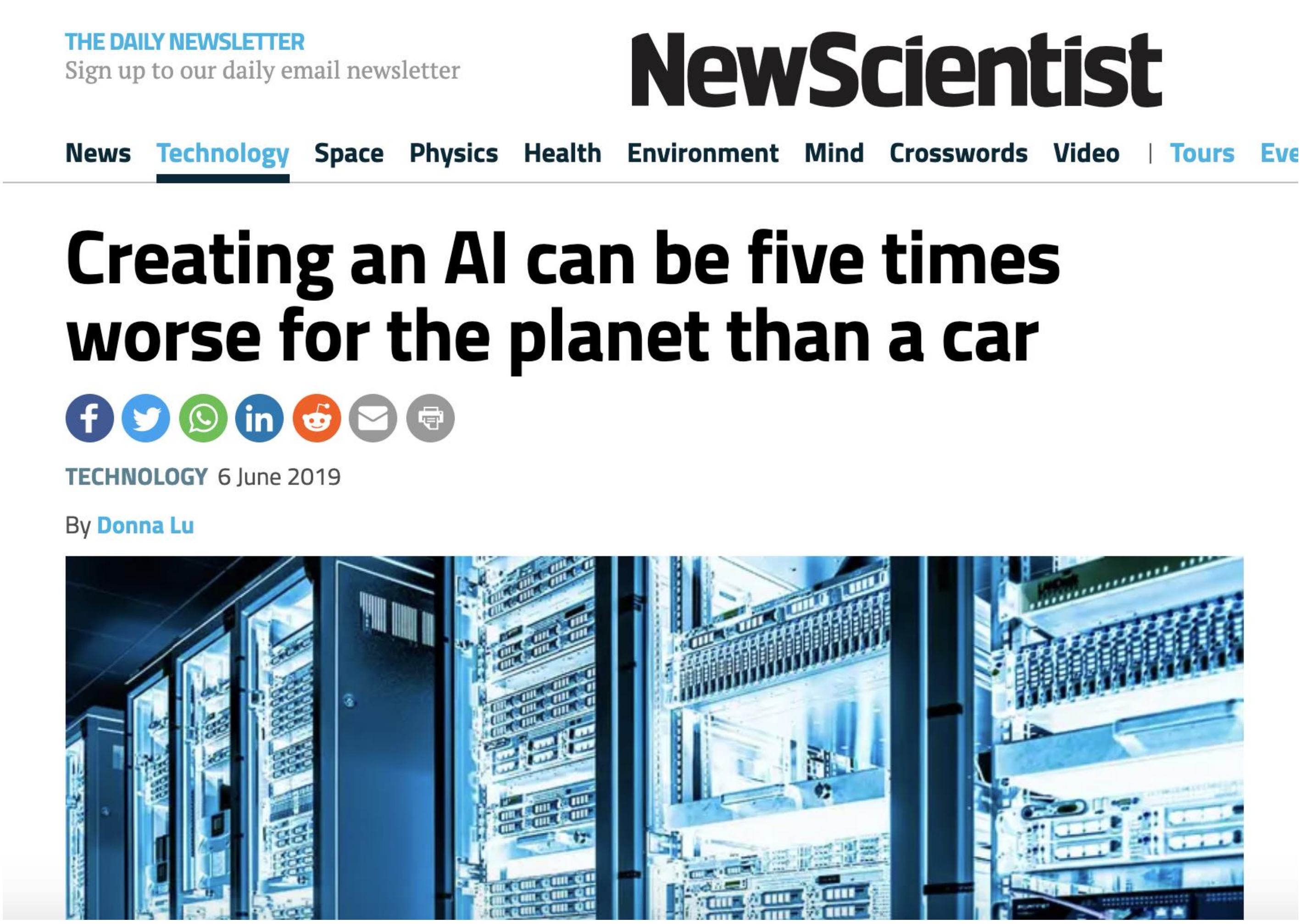
Sent the instructions through Entertainment systems
- Change the in-car temperature
- Control the steering
- Control the braking system

https://www.ophtek.com/4-real-life-examples-iot-hacked/
https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

6

The Low-Power Challenge in ML Training?

High Power => High Cost and CO_2 Emissions



THE DAILY NEWSLETTER
Sign up to our daily email newsletter

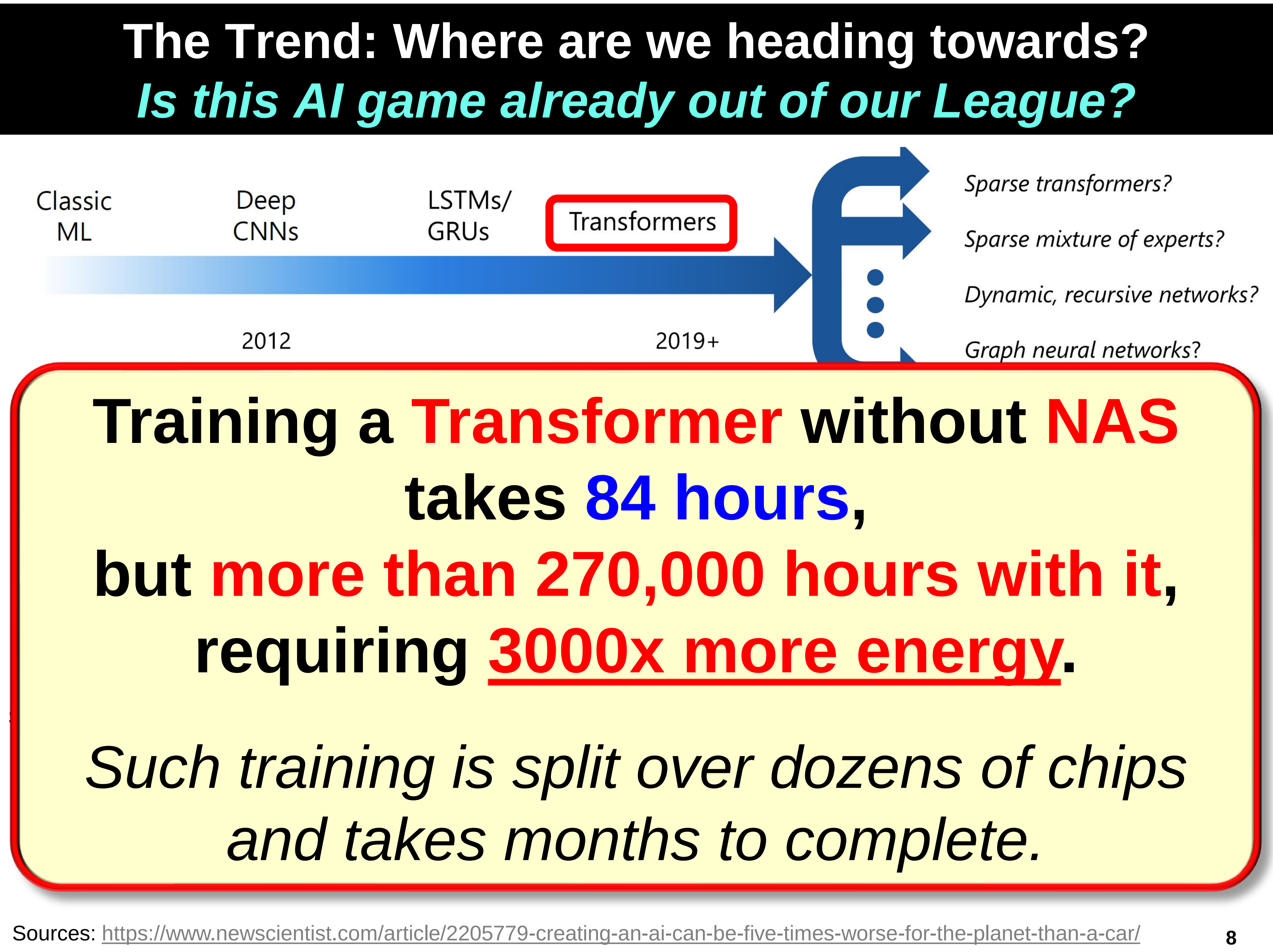
NewScientist

Creating an AI can be five times worse for the planet than a car

TECHNOLOGY 6 June 2019

By Donna Lu

7



The Trend: Where are we heading towards?

Is this AI game already out of our League?

Classic ML
Deep CNNs
LSTMs/ GRUs
Transformers
2012
2019+
Sparse transformers?
Sparse mixture of experts?
Dynamic, recursive networks?
Graph neural networks?

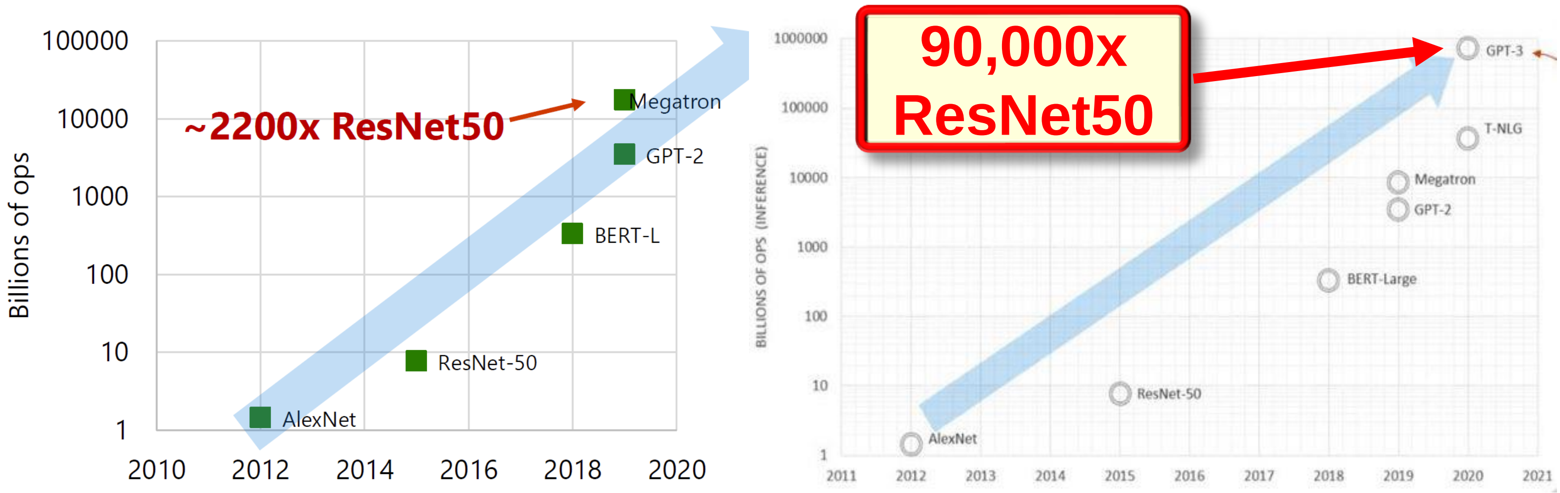
Training a Transformer without NAS takes 84 hours, but more than 270,000 hours with it, requiring 3000x more energy.

Such training is split over dozens of chips and takes months to complete.

Sources: https://www.newscientist.com/article/2205779-creating-an-ai-can-be-five-times-worse-for-the-planet-than-a-car/

8

Complexity: Exponential Growth in Model Sizes!



~2200x ResNet50

90,000x ResNet50

Source: Eric Chung, "Accelerating Microsoft's AI Ambitions", Microsoft, Azure AI and Advanced Architectures Group, 2019.

Source: https://www.microsoft.com/en-us/research/blog/a-microsoft-custom-data-type-for-efficient-inference/.

Megatron is a **8.3 billion parameter transformer** language model with trained on **512 V100 GPUs**, making it the largest transformer model ever!

Google TPU-v3 vs. Nvidia's DGX Supercomputers

Google TPU-v3 supercomputer

288 kW of power

(https://www.nextplatform.com/2018/05/10/tearing-apart-googles-tpu-3-0-ai-coprocessor/)

Nvidia's Selene supercomputer (DGX-SuperPod)

1125 kW of power

(https://developer.nvidia.com/blog/dgx-superpod-world-record-supercomputing-enterprise/)

Figure sources: https://www.eetimes.com/nvidia-google-both-claim-mlperf-training-crown/#

10

Today's ML Training Chip?

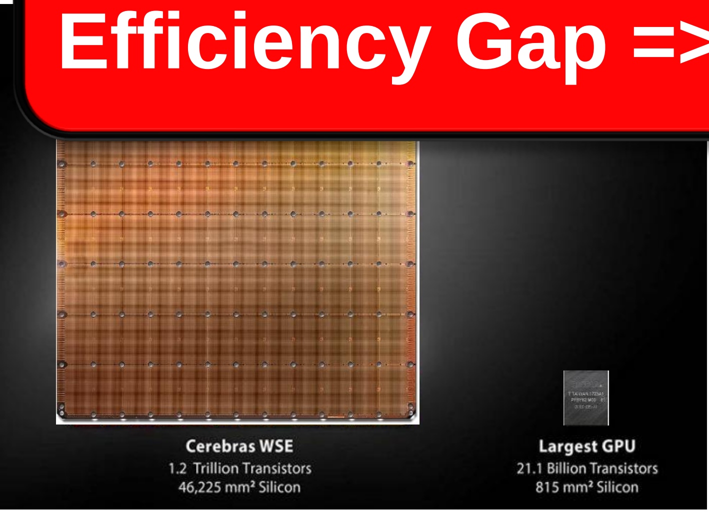
Cerebras 2nd Generation Wafer Scale Engine

Cerebras Wafer Scale Engine (WSE)

The Most Powerful Processor for AI

400,000 AI-optimized cores

46,225 mm² silicon



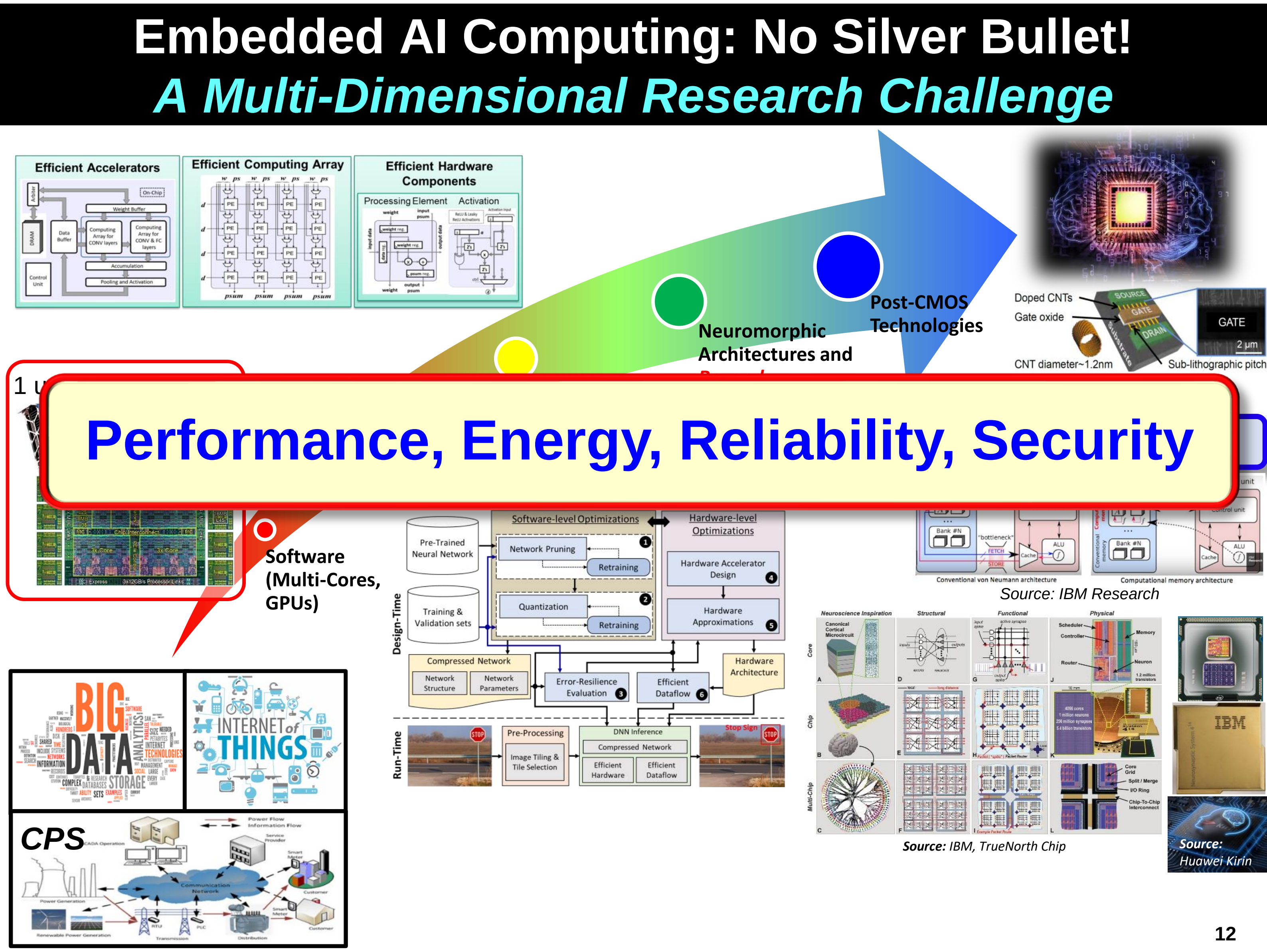
Human Brain => 20W

Efficiency Gap => 1,000x → 100,000x!!!

push to the chip through 12x 4 kW power supplies

Figure sources:

1. https://www.anandtech.com/show/16000/342-transistors-for-every-person-in-the-world-cerebras-2nd-gen-wafer-scale-engine-teased
2. https://www.cerebras.net/



Embedded AI Computing: No Silver Bullet!

A Multi-Dimensional Research Challenge

Performance, Energy, Reliability, Security

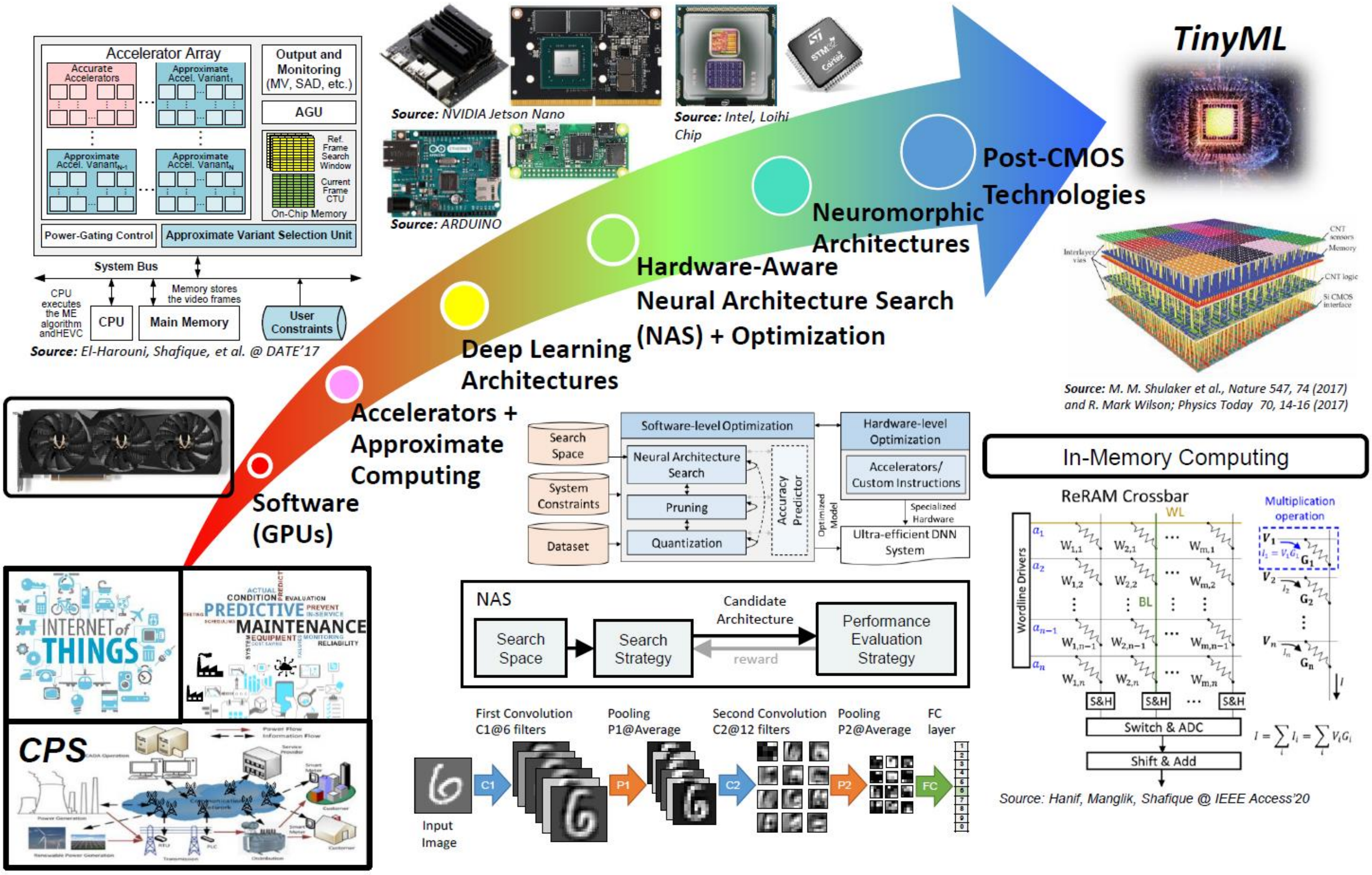
Source: IBM Research

Source: IBM, TrueNorth Chip

Source: Huawei Kirin

12

TinyML: Research Roadmap



Software (GPUs)

Accelerators + Approximate Computing

Deep Learning Architectures

Hardware-Aware Neural Architecture Search (NAS) + Optimization

Neuromorphic Architectures

Post-CMOS Technologies

TinyML

Source: El-Harouni, Shafique, et al. @ DATE'17

Source: NVIDIA Jetson Nano

Source: ARDUINO

Source: Intel, Loihi Chip

Source: M. M. Shulaker et al., Nature 547, 74 (2017) and R. Mark Wilson; Physics Today 70, 14-16 (2017)

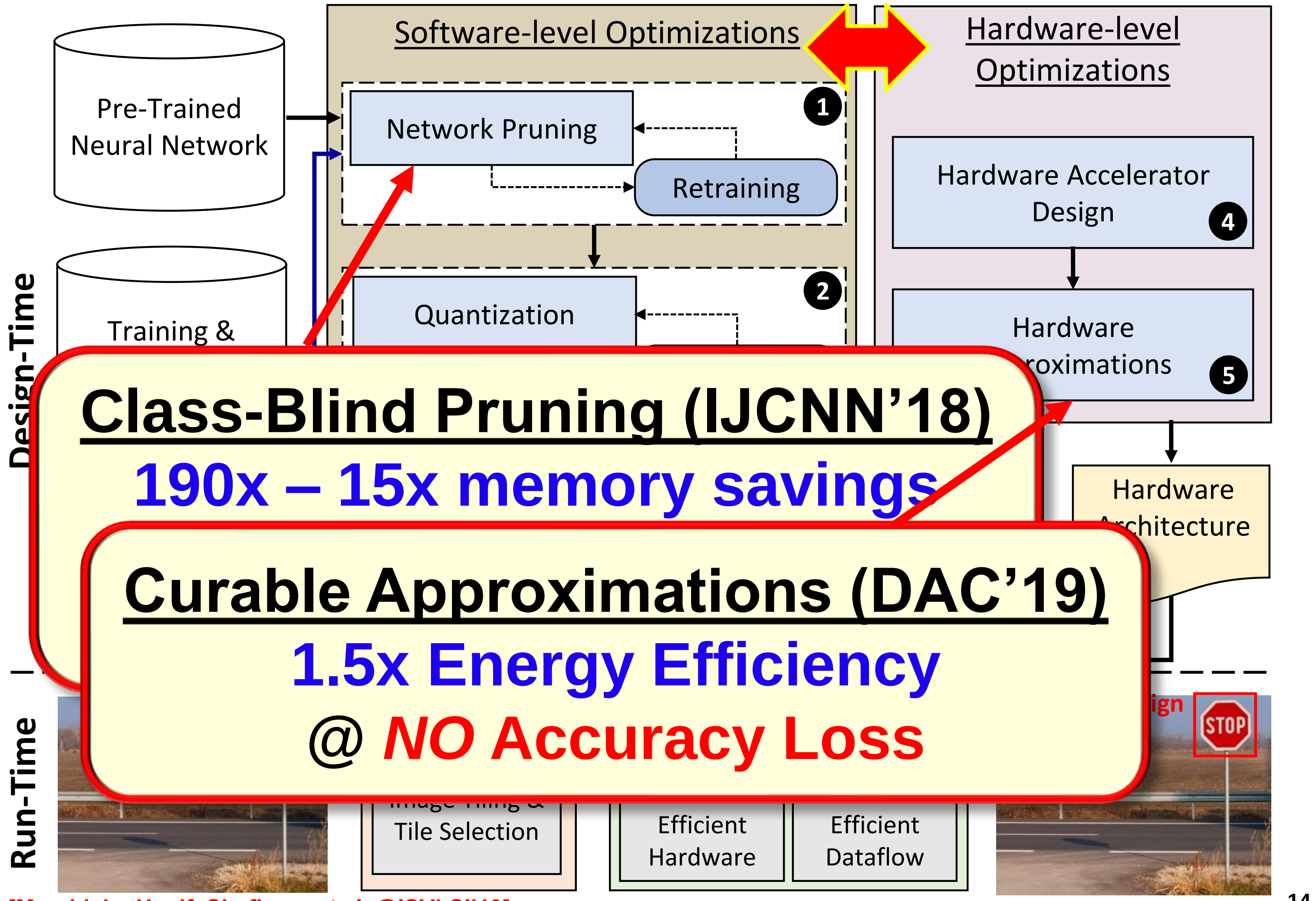
In-Memory Computing

Source: Hanif, Manglik, Shafique @ IEEE Access'20

[Shafique, et al. @DAC'21]

13

Our Cross-Layer Framework for Embedded Deep Learning



Class-Blind Pruning (IJCNN'18)

190x – 15x memory savings

Curable Approximations (DAC'19)

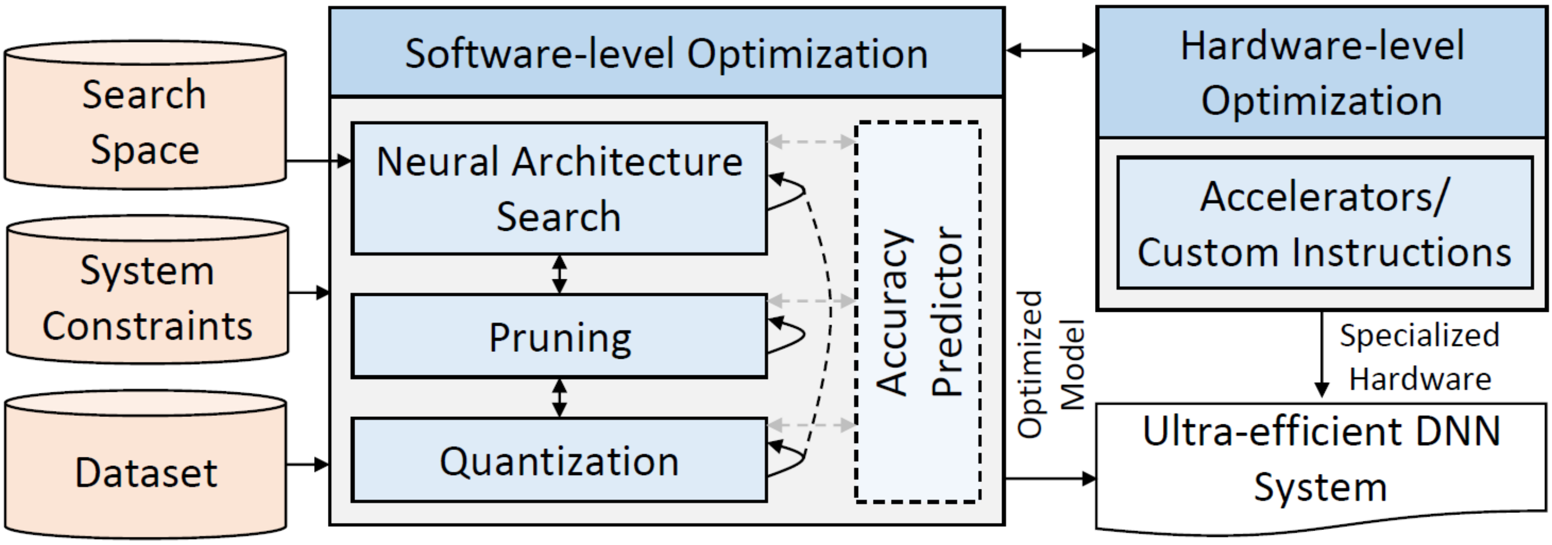
1.5x Energy Efficiency

@ *NO Accuracy Loss*

[Marchisio, Hanif, Shafique, et al. @ISVLSI'19]

14

Our Cross-Layer Design Flow for TinyML

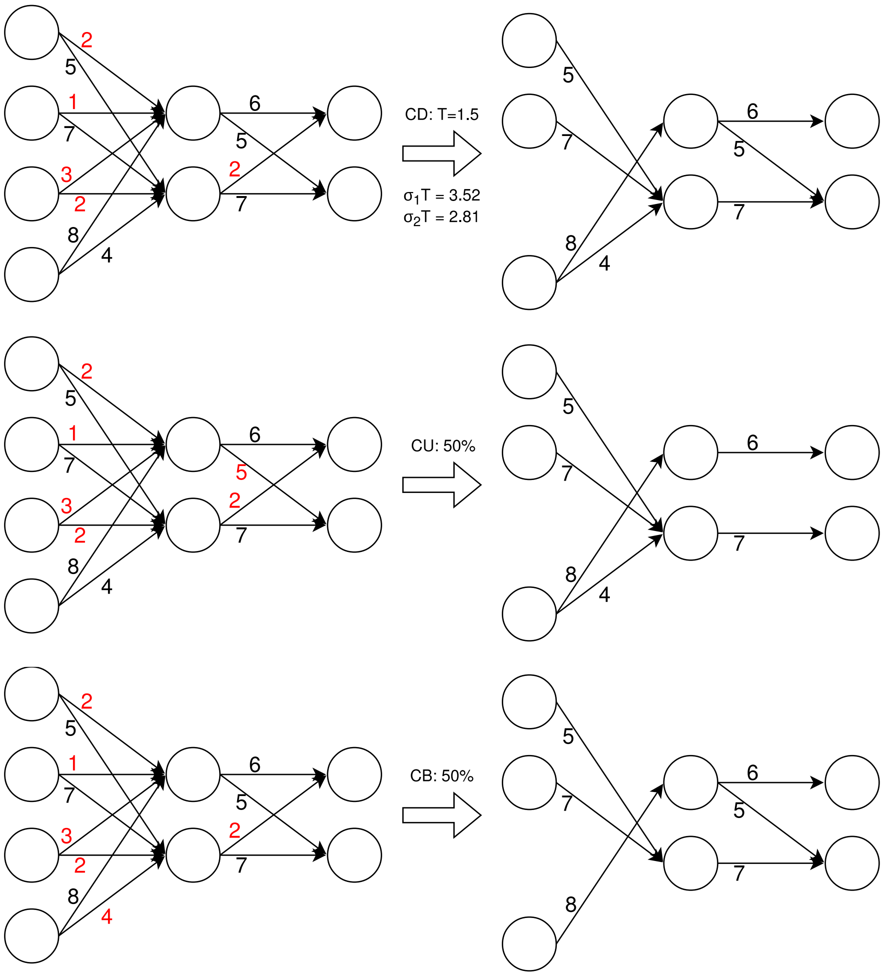

Search Space
System Constraints
Dataset
Software-level Optimization
Neural Architecture Search
Pruning
Quantization
Accuracy Predictor
Optimized Model
Hardware-level Optimization
Accelerators/ Custom Instructions
Specialized Hardware
Ultra-efficient DNN System

[Shafique, et al. @DAC'21]

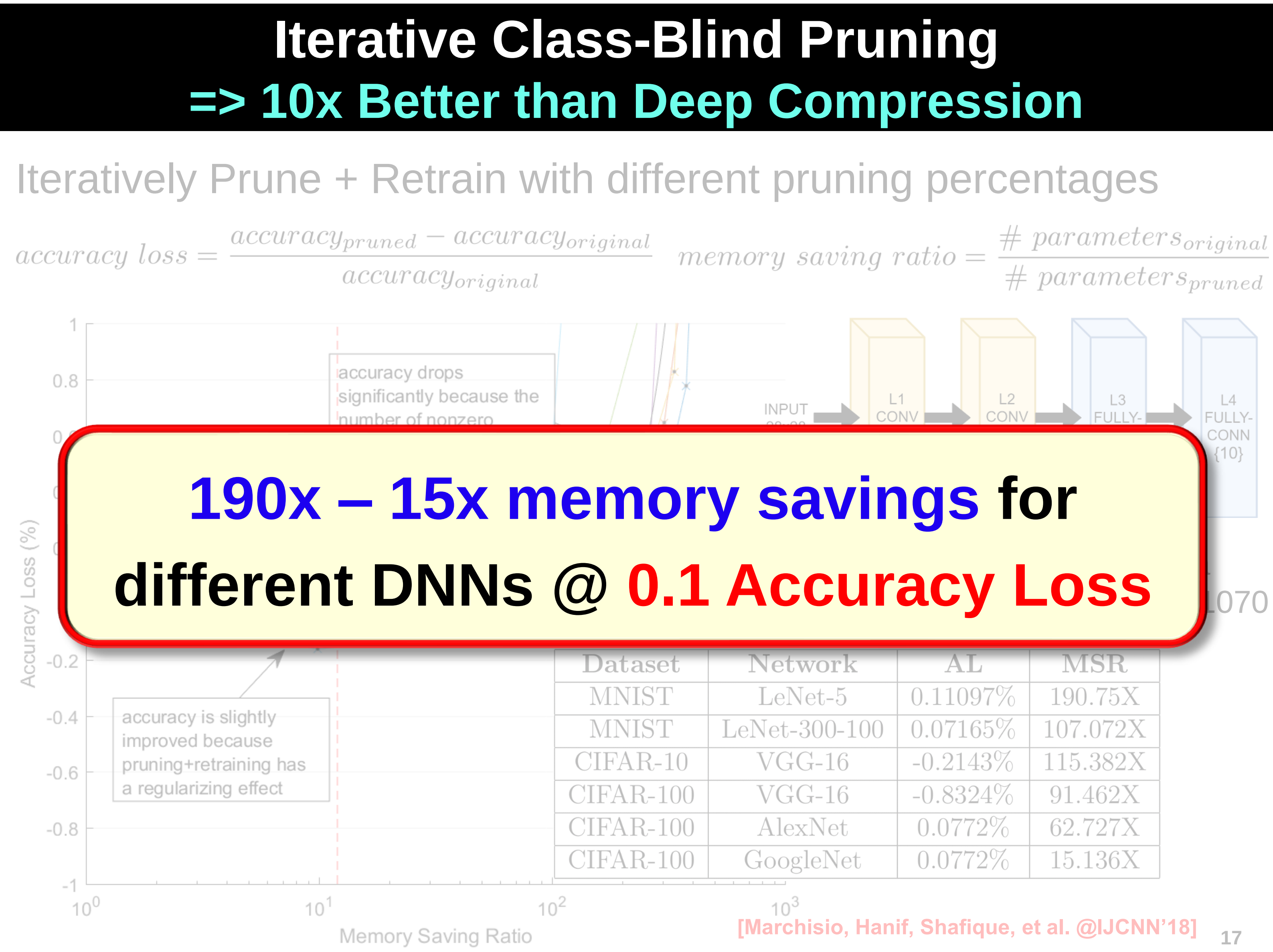
15

DNN Pruning: Methods & Comparison

- ❑ **Class-Distribution (CD):** a certain threshold T is selected and, for every layer, all the parameters below σT are pruned, where σ is the standard deviation.
- ❑ **Class-Uniform (CU):** a certain percentage x is selected and, for every layer, the smallest x% parameters are pruned.
- ❑ **Class-Blind (CB):** a certain percentage x is selected and the smallest x% parameters of the entire model are pruned, without keeping uniform sparsity for each layer.



[Marchisio, Hanif, Shafique, et al. @IJCNN'18]



Iterative Class-Blind Pruning
=> 10x Better than Deep Compression

Iteratively Prune + Retrain with different pruning percentages

$$accuracy\ loss = \frac{accuracy_{pruned} - accuracy_{original}}{accuracy_{original}} \qquad memory\ saving\ ratio = \frac{\#\ parameters_{original}}{\#\ parameters_{pruned}}$$

1
0.8
0
0
0
-0.2
-0.4
-0.6
-0.8
-1
Accuracy Loss (%)
10^0
10^1
10^2
10^3
Memory Saving Ratio
accuracy drops significantly because the number of nonzero
accuracy is slightly improved because pruning+retraining has a regularizing effect
INPUT
L1 CONV
L2 CONV
L3 FULLY-
L4 FULLY-CONN {10}

Dataset	Network	AL	MSR
MNIST	LeNet-5	0.11097%	190.75X
MNIST	LeNet-300-100	0.07165%	107.072X
CIFAR-10	VGG-16	-0.2143%	115.382X
CIFAR-100	VGG-16	-0.8324%	91.462X
CIFAR-100	AlexNet	0.0772%	62.727X
CIFAR-100	GoogleNet	0.0772%	15.136X

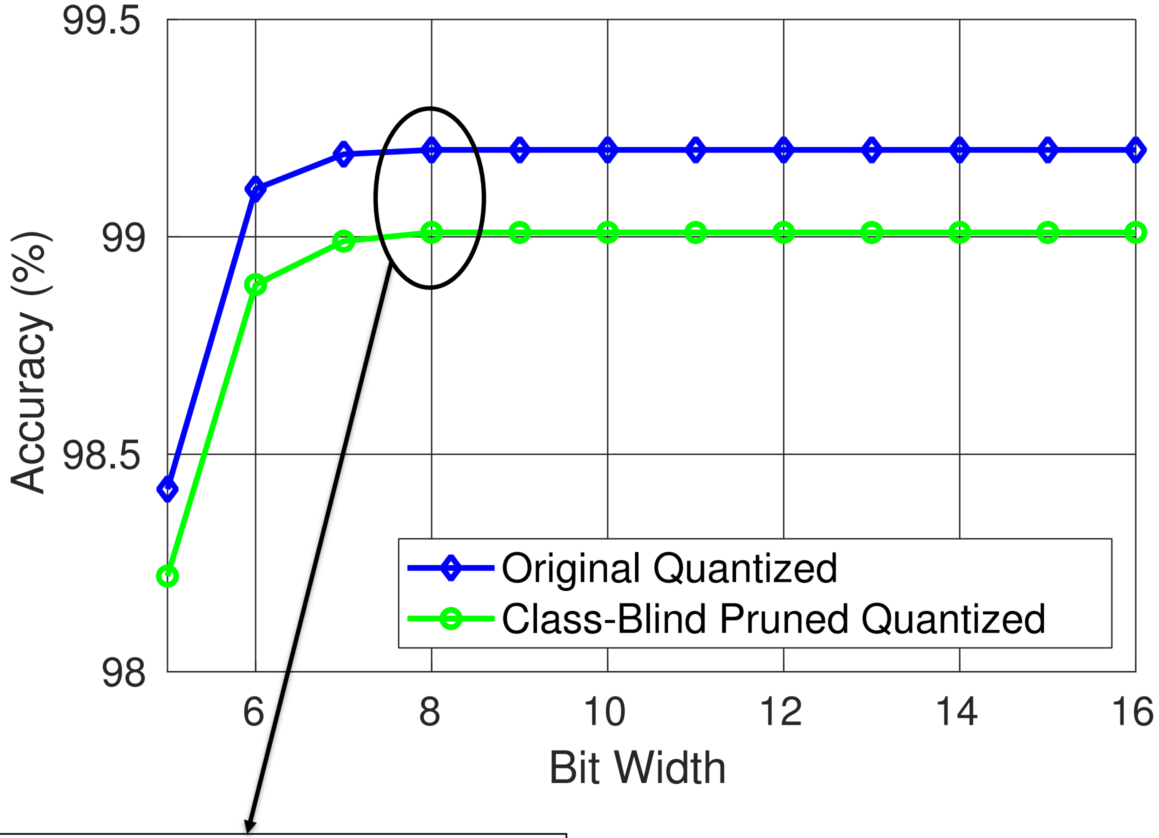
190x – 15x memory savings for different DNNs @ 0.1 Accuracy Loss

[Marchisio, Hanif, Shafique, et al. @IJCNN’18]

17

DNN Quantization: Method and Experiments

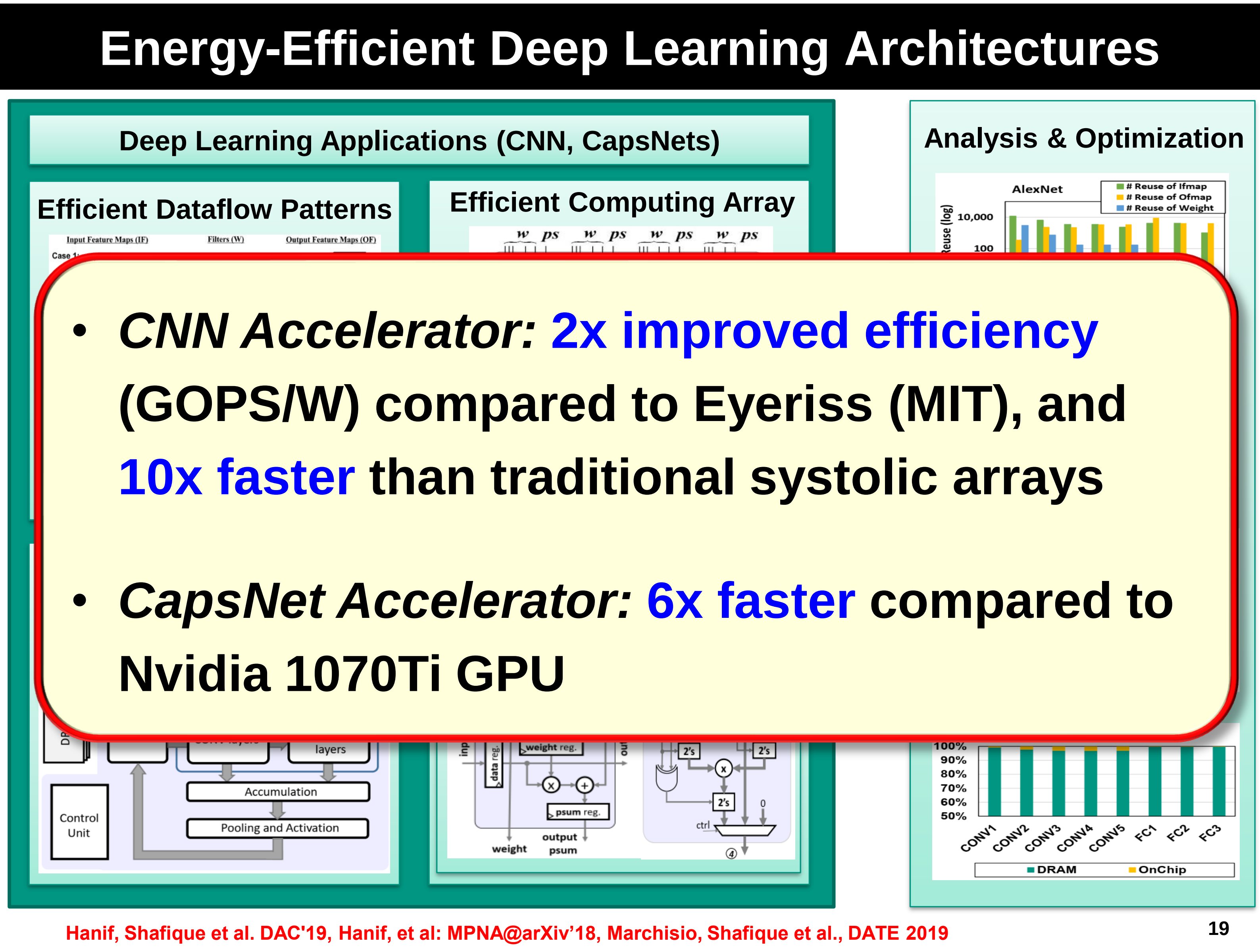
32bit floating-point => fixed-point => reduce bit-width



✓ Same accuracy as full precision
✓ Low memory footprint

[Marchisio, Hanif, Shafique, et al. INTESA@ESWeek'18]

18



Energy-Efficient Deep Learning Architectures

Deep Learning Applications (CNN, CapsNets)

Efficient Dataflow Patterns

Efficient Computing Array

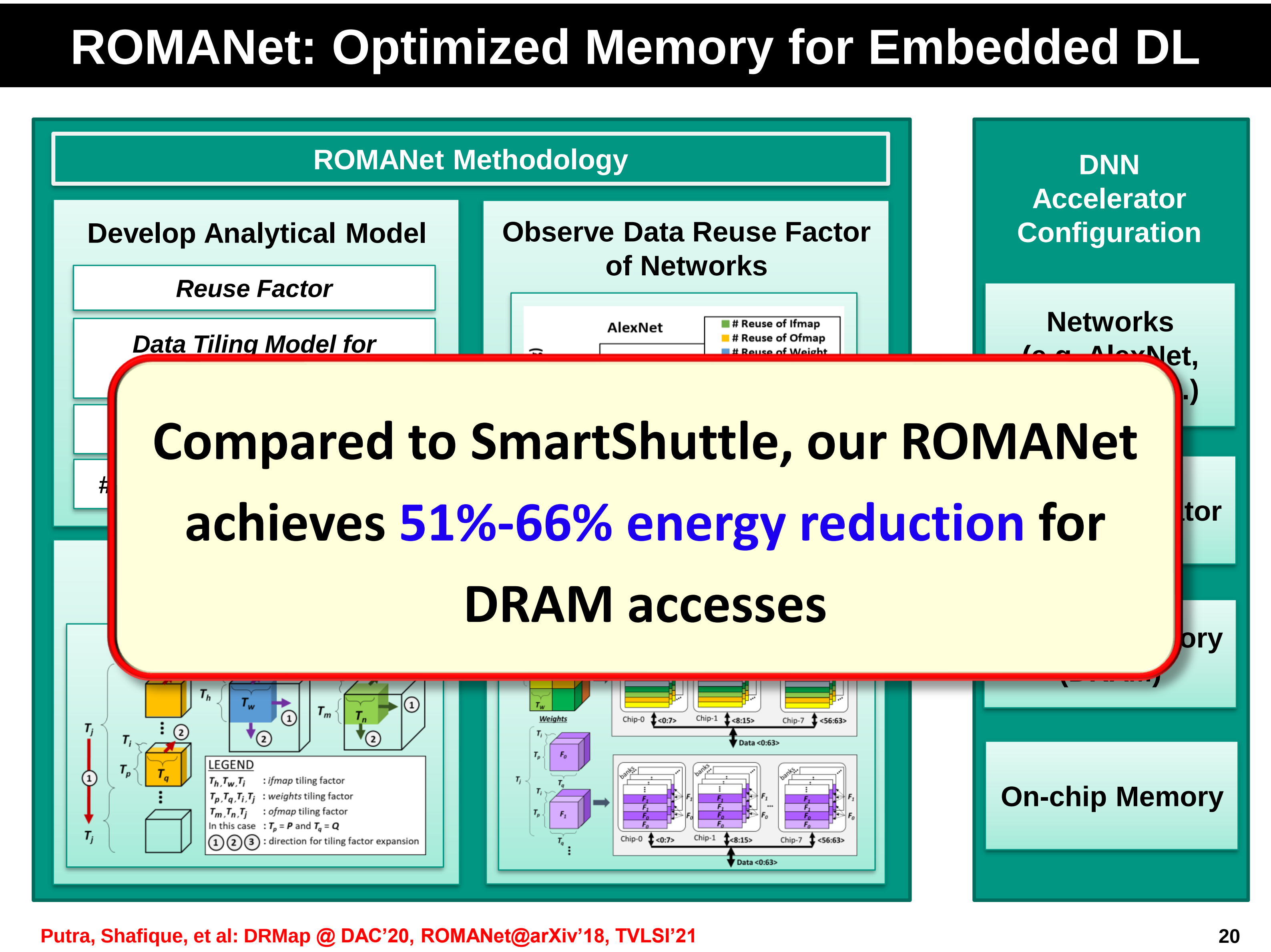
Analysis & Optimization

Input Feature Maps (IF)
Filters (W)
Output Feature Maps (OF)
Case 1
w ps w ps w ps w ps
layers
Accumulation
Pooling and Activation
Control Unit
weight reg.
data reg.
psum reg.
weight
output psum
2's
ctrl
0
AlexNet
Reuse (log)
10,000
100
# Reuse of Ifmap
# Reuse of Ofmap
# Reuse of Weight
100%
90%
80%
70%
60%
50%
CONV1
CONV2
CONV3
CONV4
CONV5
FC1
FC2
FC3
DRAM
OnChip

- ***CNN Accelerator:*** **2x improved efficiency (GOPS/W) compared to Eyeriss (MIT), and 10x faster than traditional systolic arrays**
- ***CapsNet Accelerator:*** **6x faster compared to Nvidia 1070Ti GPU**

Hanif, Shafique et al. DAC'19, Hanif, et al: MPNA@arXiv'18, Marchisio, Shafique et al., DATE 2019

19



ROMANet: Optimized Memory for Embedded DL

ROMANet Methodology

Develop Analytical Model

Reuse Factor

Data Tiling Model for

Observe Data Reuse Factor of Networks

DNN Accelerator Configuration

Networks (e.g., AlexNet,

.)

tor

ory

(DRAM)

On-chip Memory

Compared to SmartShuttle, our ROMANet achieves 51%-66% energy reduction for DRAM accesses

AlexNet
# Reuse of Ifmap
# Reuse of Ofmap
# Reuse of Weight
LEGEND
T_h, T_w, T_i : ifmap tiling factor
T_p, T_q, T_i, T_j : weights tiling factor
T_m, T_n, T_j : ofmap tiling factor
In this case : $T_p = P$ and $T_q = Q$
①②③ : direction for tiling factor expansion
Weights
Chip-0 <0:7>
Chip-1 <8:15>
Chip-7 <56:63>
Data <0:63>

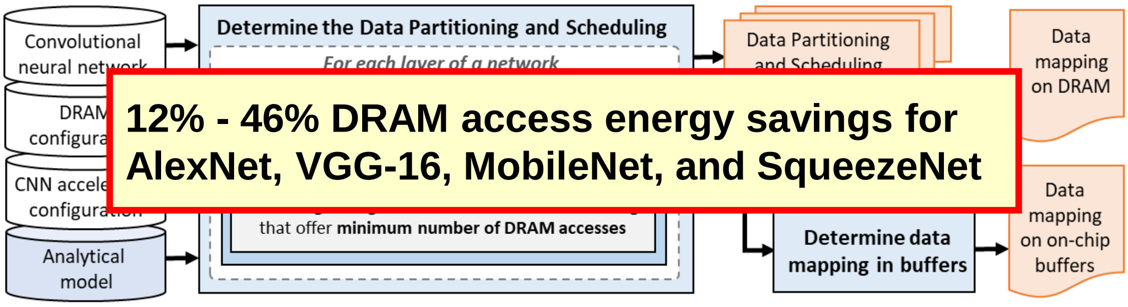
Putra, Shafique, et al: DRMap @ DAC'20, ROMANet@arXiv'18, TVLSI'21

20

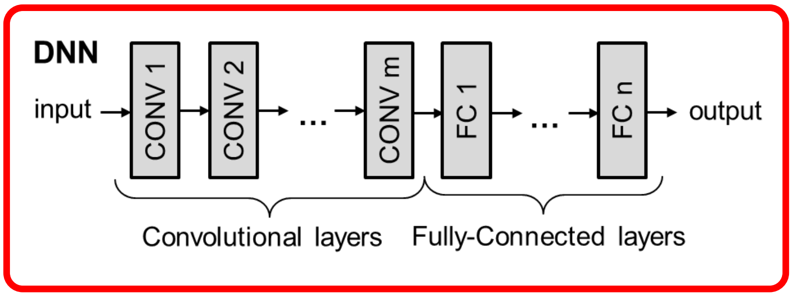
Deep Learning Research

Energy-Efficient Memory Accesses for DNN Accelerators (IEEE TVLSI'21)

①

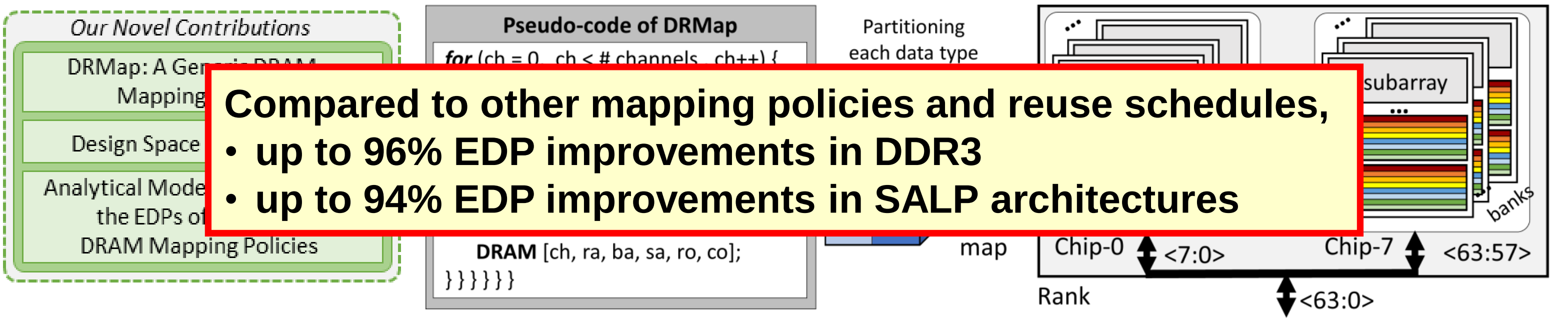

Convolutional neural network
DRAM configura
CNN accele configuration
Analytical model
Determine the Data Partitioning and Scheduling
For each layer of a network
that offer minimum number of DRAM accesses
Data Partitioning and Scheduling
Data mapping on DRAM
Determine data mapping in buffers
Data mapping on on-chip buffers

12% - 46% DRAM access energy savings for AlexNet, VGG-16, MobileNet, and SqueezeNet



②

Generic DRAM Mapping for Energy-Efficient DNNs (DAC'20)


Our Novel Contributions
DRMap: A Generic DRAM Mapping
Design Space
Analytical Model the EDPs of DRAM Mapping Policies
Pseudo-code of DRMap
for (ch = 0, ch < # channels, ch++) {
DRAM [ch, ra, ba, sa, ro, co];
}}}}}}
Partitioning each data type
map
subarray
banks
Chip-0
<7:0>
Chip-7
<63:57>
Rank
<63:0>

Compared to other mapping policies and reuse schedules,
- **up to 96% EDP improvements in DDR3**
- **up to 94% EDP improvements in SALP architectures**

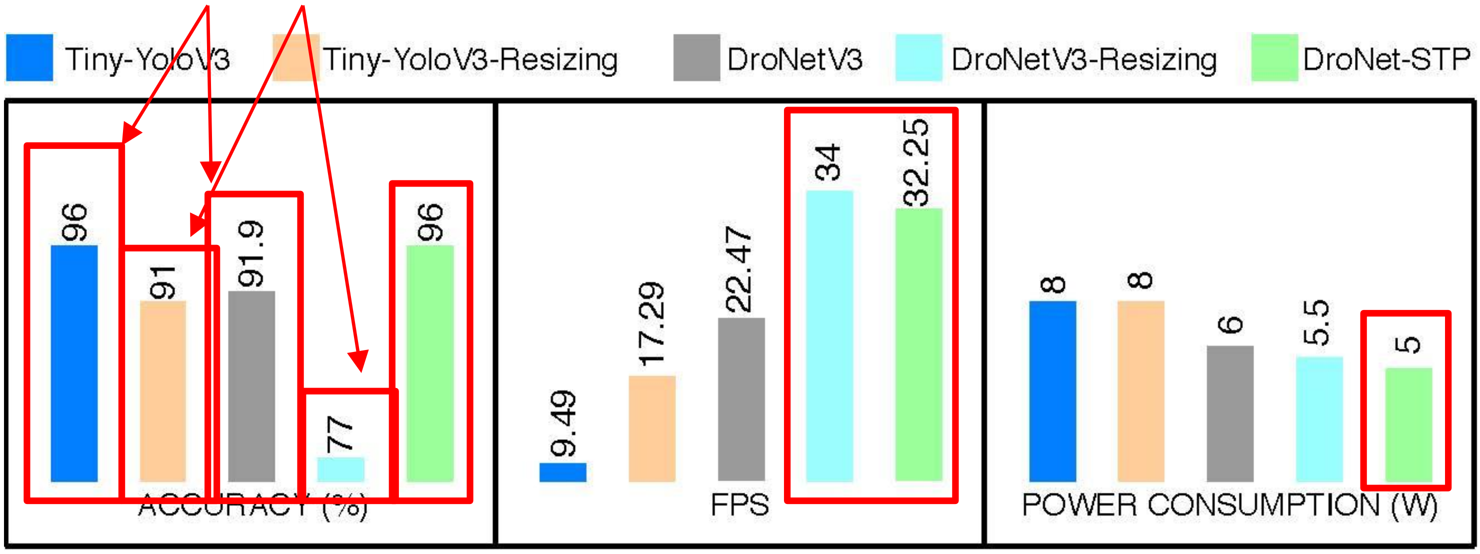
21

Selective Tile Processing on Jetson TX2

- ❑ Resizing the input images decreases accuracy
- ❑ Networks with STP offer
  - ❑ Baseline Accuracy
  - ❑ High Frame Rate
  - ❑ Low Power Consumption

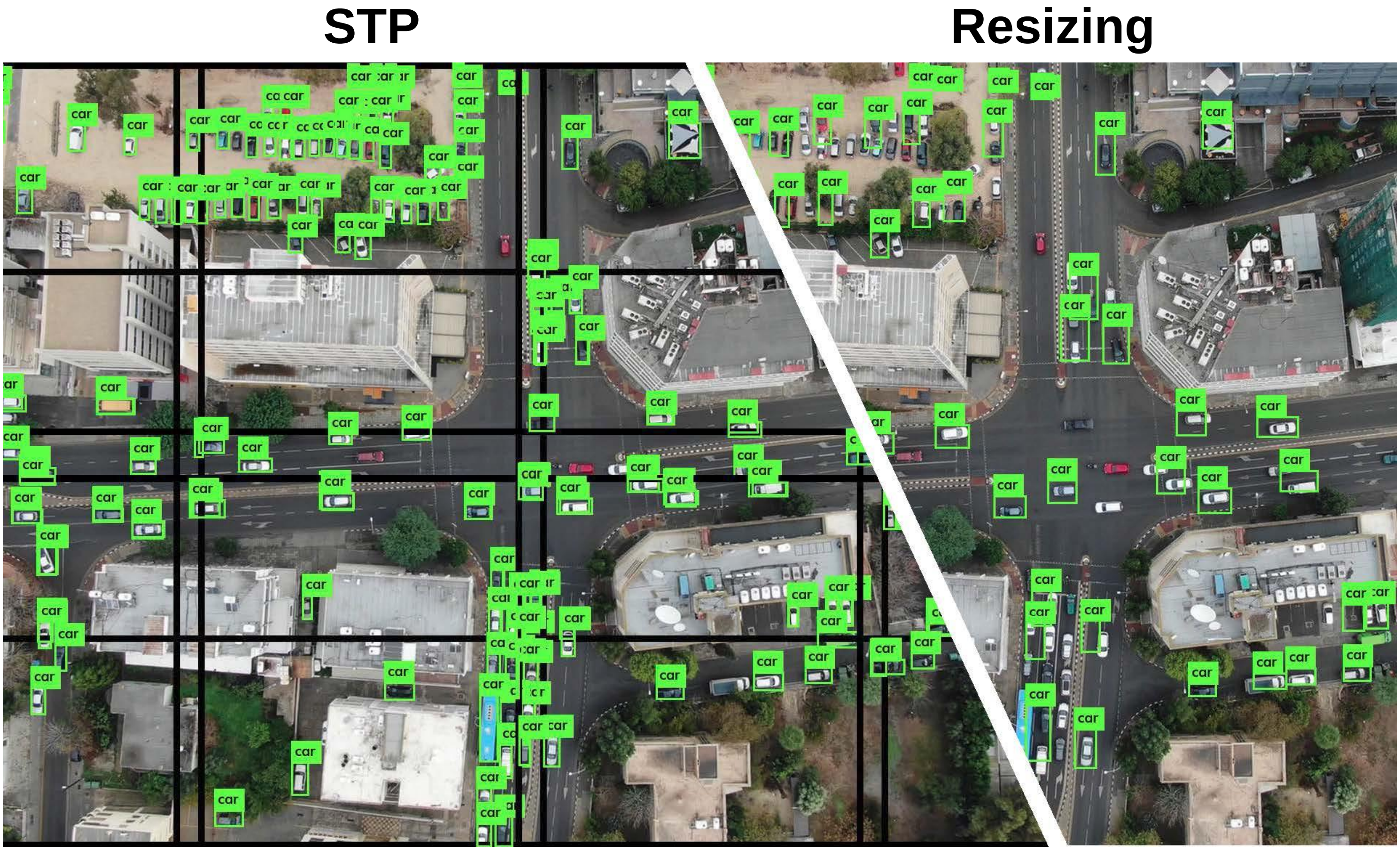
Baseline Accuracy

Accuracy with Resized Images



[Marchisio, Hanif, Shafique, et al. @ISVLSI'19]

STP vs. Resizing

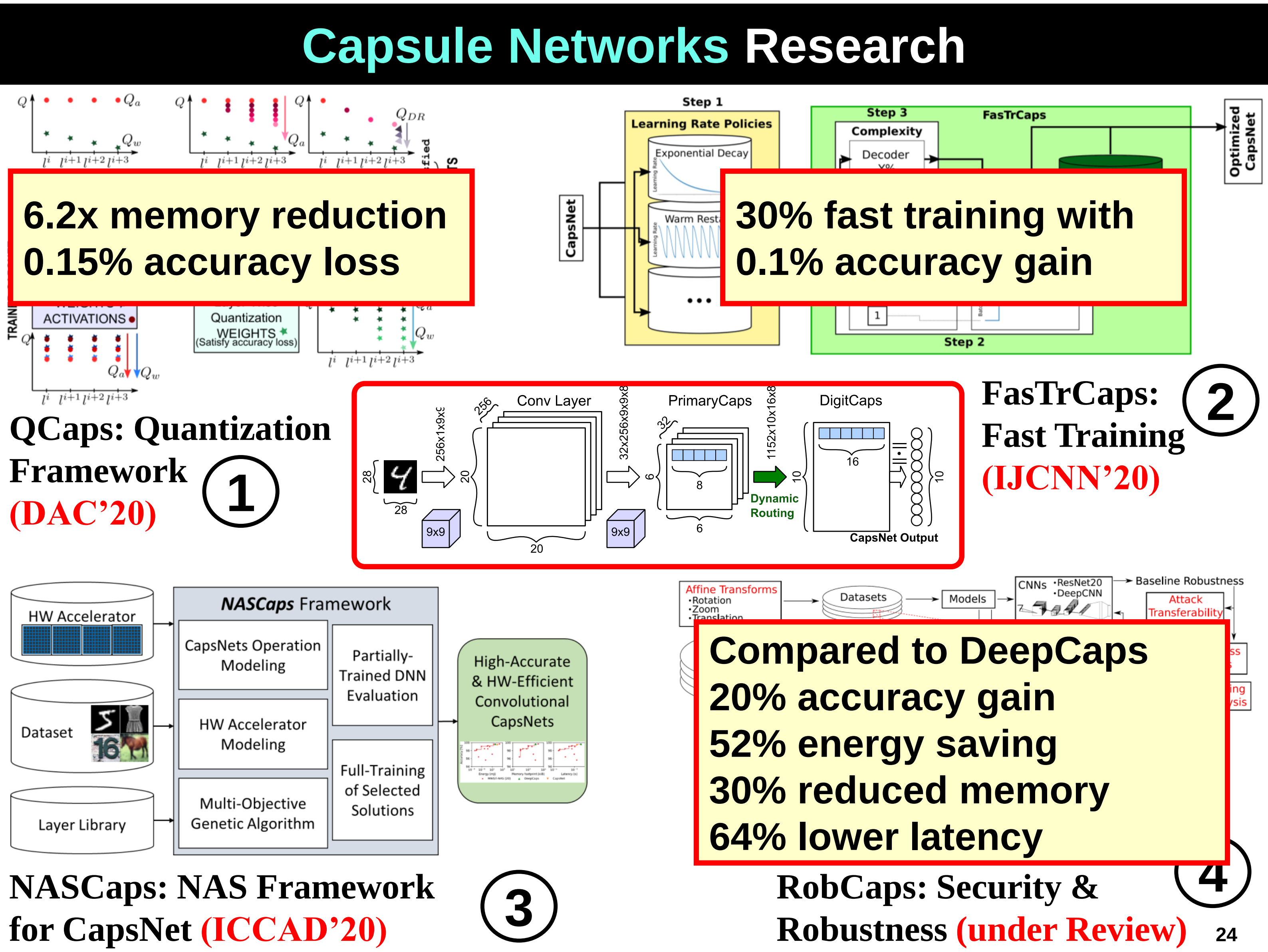


STP

Resizing

[Marchisio, Hanif, Shafique, et al. @ISVLSI'19]

23



Capsule Networks Research

6.2x memory reduction
0.15% accuracy loss

QCaps: Quantization Framework **1** (DAC'20)

30% fast training with
0.1% accuracy gain

FasTrCaps: Fast Training **2** (IJCNN'20)

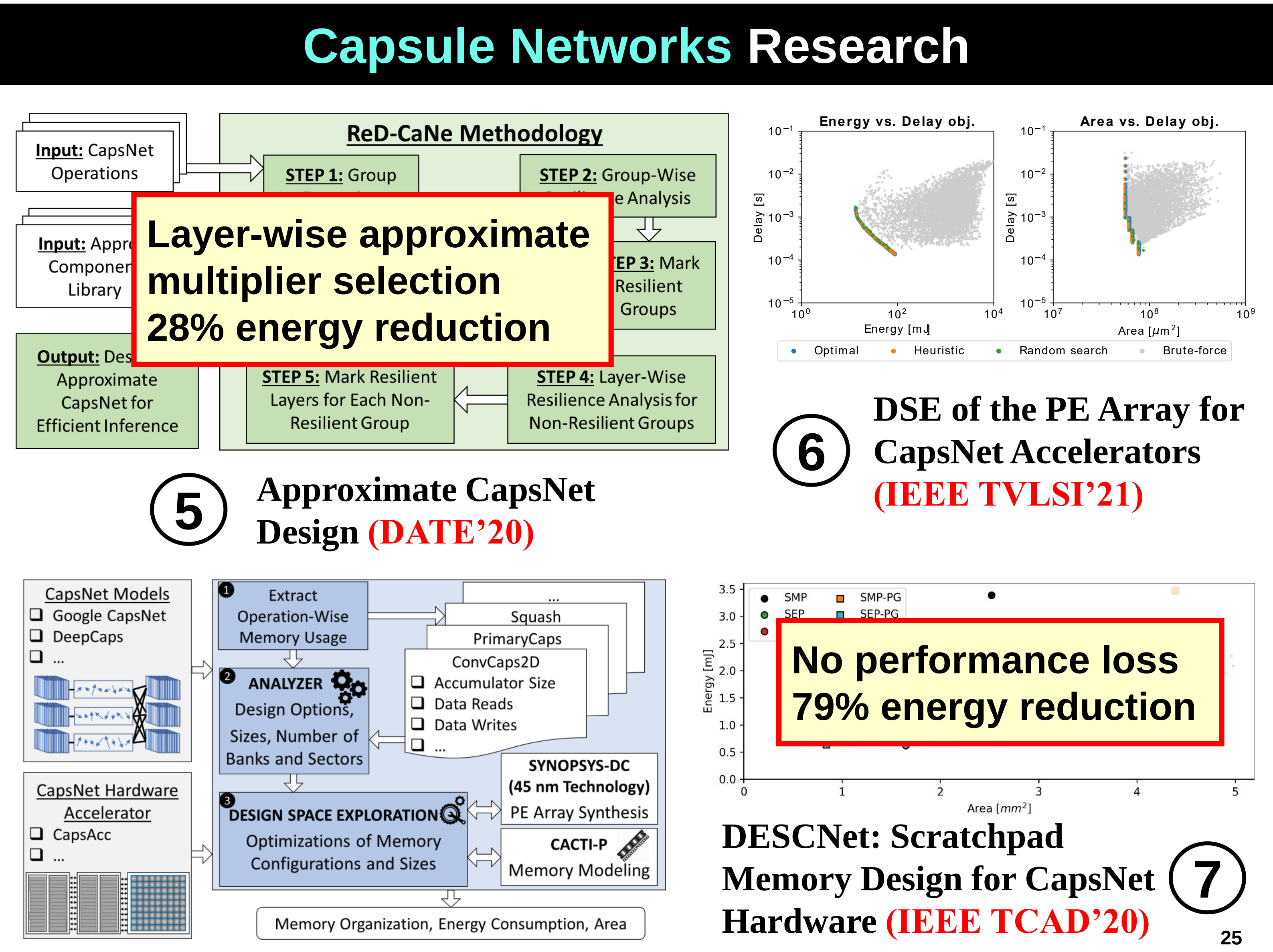
HW Accelerator
Dataset
Layer Library
NASCaps Framework
CapsNets Operation Modeling
HW Accelerator Modeling
Multi-Objective Genetic Algorithm
Partially-Trained DNN Evaluation
Full-Training of Selected Solutions
High-Accurate & HW-Efficient Convolutional CapsNets

NASCaps: NAS Framework for CapsNet (ICCAD'20) **3**

Compared to DeepCaps
20% accuracy gain
52% energy saving
30% reduced memory
64% lower latency

RobCaps: Security & Robustness (under Review) **4**

24



Capsule Networks Research

ReD-CaNe Methodology

Input: CapsNet Operations

STEP 1: Group

STEP 2: Group-Wise ...e Analysis

Input: Appr... Componen... Library

...EP 3: Mark Resilient Groups

Output: Des... Approximate CapsNet for Efficient Inference

STEP 5: Mark Resilient Layers for Each Non-Resilient Group

STEP 4: Layer-Wise Resilience Analysis for Non-Resilient Groups

Layer-wise approximate multiplier selection
28% energy reduction

5 Approximate CapsNet Design (DATE'20)

6 DSE of the PE Array for CapsNet Accelerators (IEEE TVLSI'21)

CapsNet Models
- □ Google CapsNet
- □ DeepCaps
- □ ...

CapsNet Hardware Accelerator
- □ CapsAcc
- □ ...

1 Extract Operation-Wise Memory Usage

...
Squash
PrimaryCaps
ConvCaps2D
- □ Accumulator Size
- □ Data Reads
- □ Data Writes
- □ ...

2 ANALYZER Design Options, Sizes, Number of Banks and Sectors

3 DESIGN SPACE EXPLORATION Optimizations of Memory Configurations and Sizes

SYNOPSYS-DC (45 nm Technology) PE Array Synthesis

CACTI-P Memory Modeling

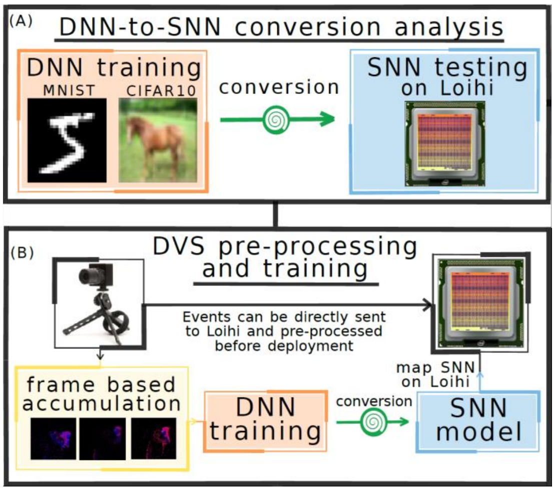
Memory Organization, Energy Consumption, Area

No performance loss
79% energy reduction

DESCNet: Scratchpad Memory Design for CapsNet Hardware (IEEE TCAD'20) 7

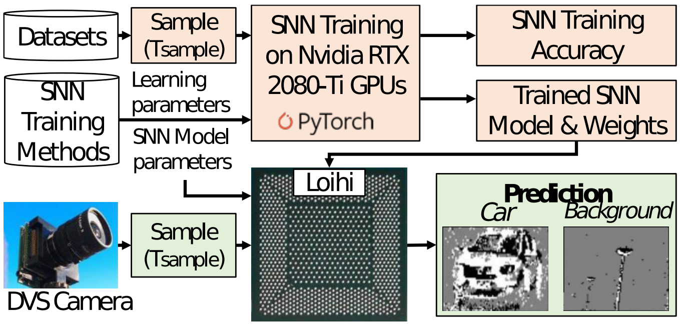
25

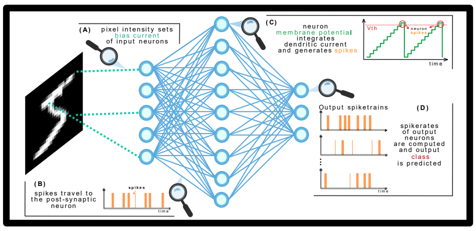
Neuromorphic Computing using Intel's Loihi


(A)
DNN-to-SNN conversion analysis
DNN training
MNIST
CIFAR10
conversion
SNN testing on Loihi
(B)
DVS pre-processing and training
Events can be directly sent to Loihi and pre-processed before deployment
frame based accumulation
DNN training
conversion
map SNN on Loihi
SNN model

SNN Mapping over Intel's Loihi Processor (IJCNN'20)

1




(A) pixel intensity sets bias current of input neurons
(B) spikes travel to the post-synaptic neuron
spikes
time
(C) neuron membrane potential integrates dendritic current and generates spikes
Vth
neuron spikes
time
Output spiketrains
(D) spikerates of output neurons are computed and output class is predicted
time

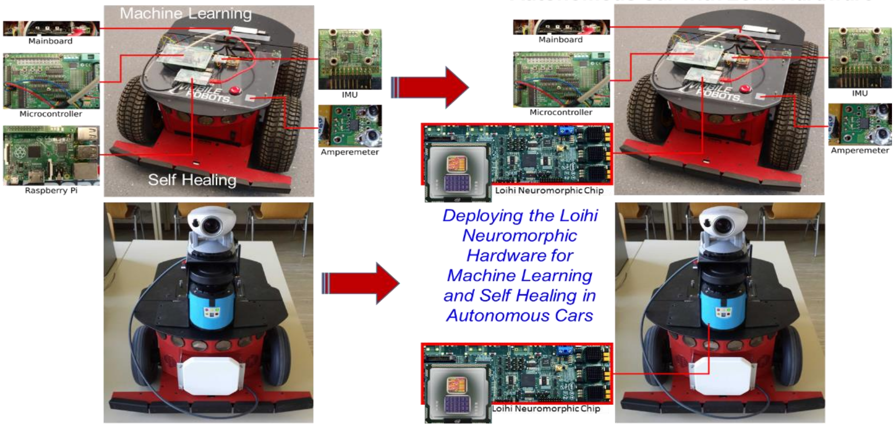
2

DVS-Based Car vs. Background Classification on Intel's Loihi (IJCNN'21)

Autonomous Driving

Current Prototypes of Autonomous Car

Envisioned Prototypes of Autonomous Car with *Loihi Hardware*

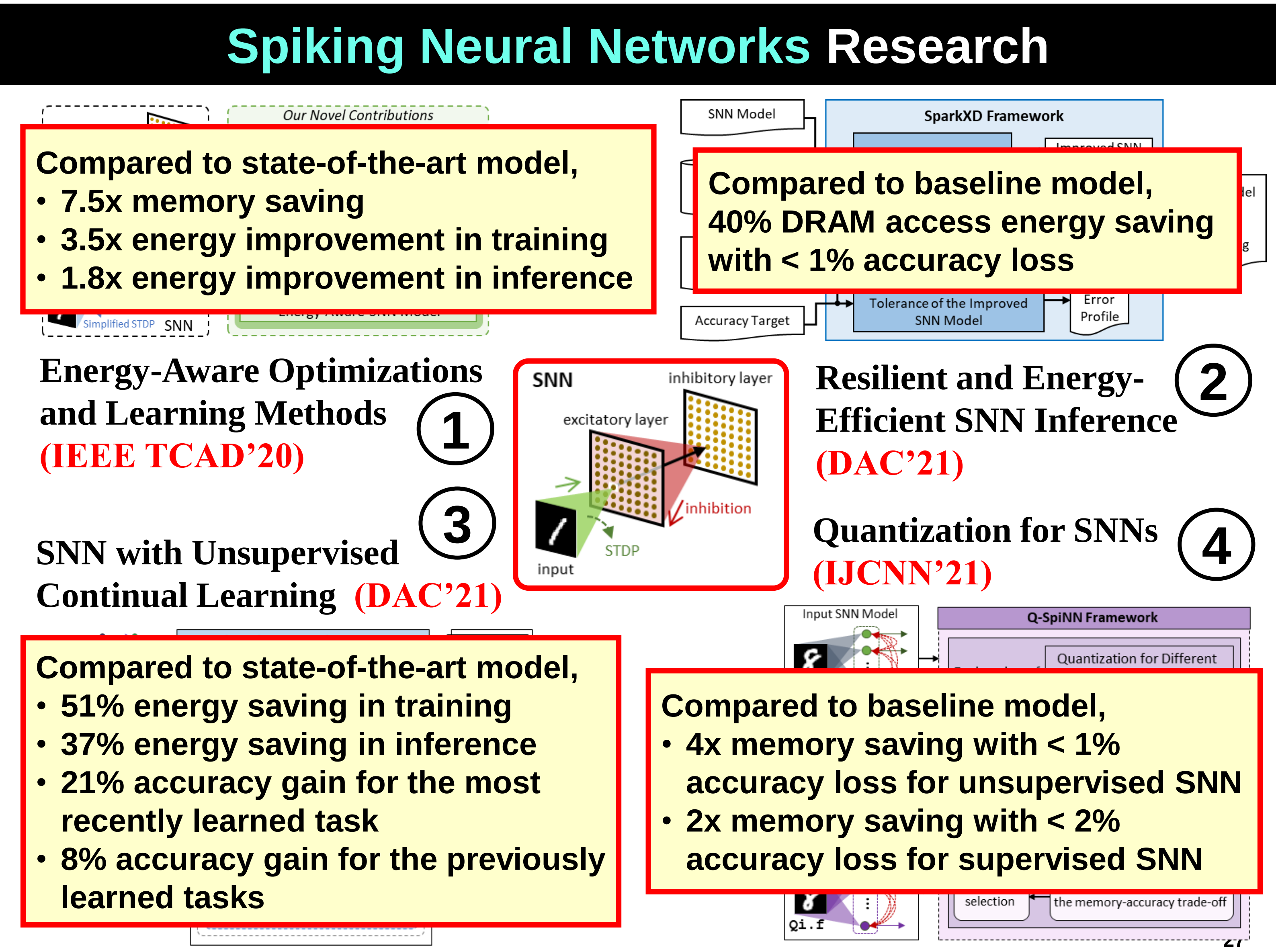


Deploying the Loihi Neuromorphic Hardware for Machine Learning and Self Healing in Autonomous Cars

Smart Farming

26

©MECO.net



Spiking Neural Networks Research

Compared to state-of-the-art model,

- 7.5x memory saving
- 3.5x energy improvement in training
- 1.8x energy improvement in inference

Compared to baseline model, 40% DRAM access energy saving with < 1% accuracy loss

Energy-Aware Optimizations and Learning Methods (IEEE TCAD'20) 1

Resilient and Energy-Efficient SNN Inference (DAC'21) 2

SNN with Unsupervised Continual Learning (DAC'21) 3

Quantization for SNNs (IJCNN'21) 4

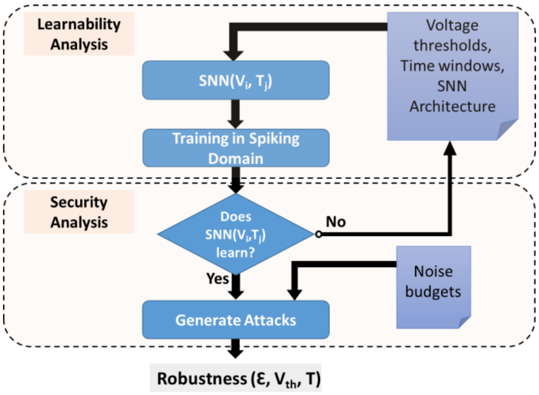
Compared to state-of-the-art model,

- 51% energy saving in training
- 37% energy saving in inference
- 21% accuracy gain for the most recently learned task
- 8% accuracy gain for the previously learned tasks

Compared to baseline model,

- 4x memory saving with < 1% accuracy loss for unsupervised SNN
- 2x memory saving with < 2% accuracy loss for supervised SNN

Security for SNNs & Neuromorphic Computing



Learnability Analysis

Voltage thresholds, Time windows, SNN Architecture

$SNN(V_i, T_j)$

Training in Spiking Domain

Security Analysis

Does $SNN(V_i,T_j)$ learn?

No

Yes

Noise budgets

Generate Attacks

Robustness (ε, V_{th}, T)

Robust SNN Design against Adversarial Attacks (DATE'21)

1

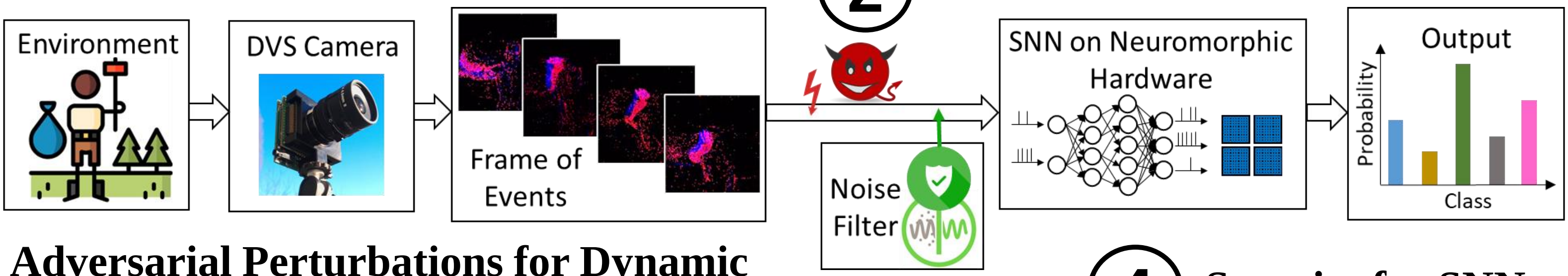
Same clean accuracy than CNN

75% higher accuracy for large perturbations

Ɛ (Noise budget)

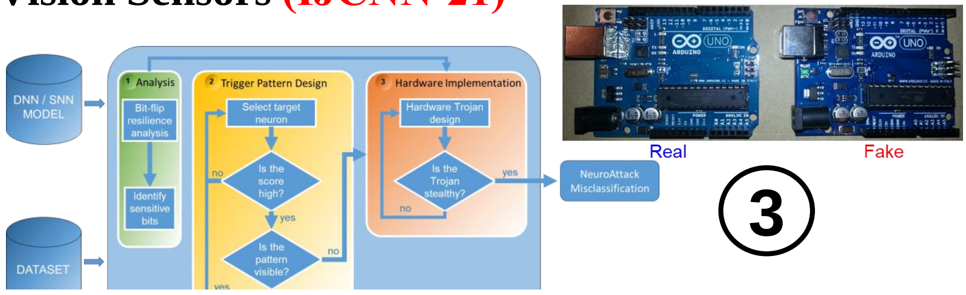
● [T=72;v_th=0.5] ● [T=32;v_th=1.0] ● CNN ● [T=56;v_th=2.25] ● [T=48;v_th=1.0]

2



Adversarial Perturbations for Dynamic Vision Sensors (IJCNN'21)

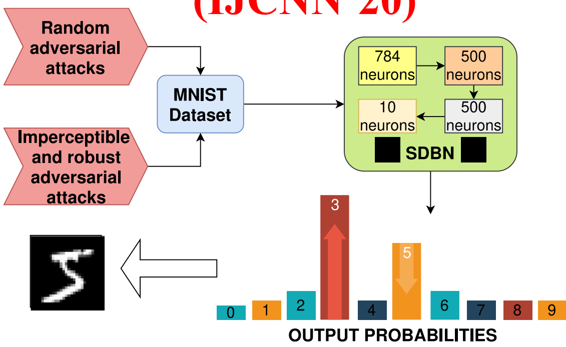
Counterfeiting



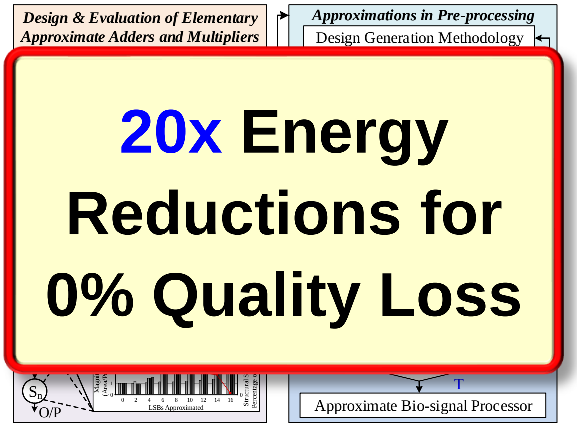
Fault-Injection Attacks on SNNs (IJCNN'20)

4

Security for SNNs (IJCNN'20)



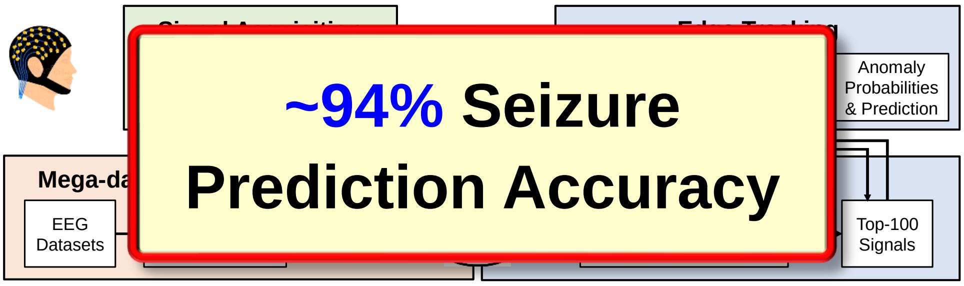
Energy-Efficient IoT-Healthcare and AI


Design & Evaluation of Elementary Approximate Adders and Multipliers
Approximations in Pre-processing
Design Generation Methodology
S_n
O/P
T
LSBs Approximated
Approximate Bio-signal Processor

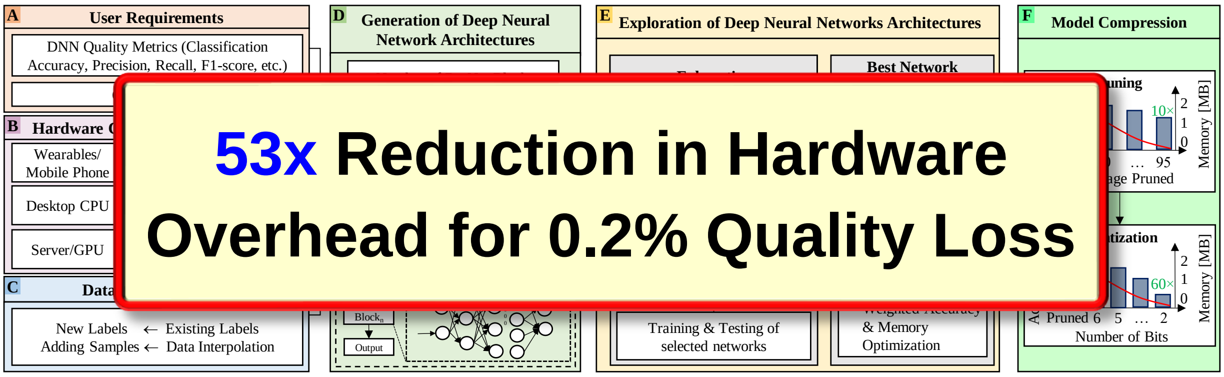
20x Energy Reductions for 0% Quality Loss

Methodology for Approx. Bio-signal Processing: **DAC'19** ①

Cloud-Edge Framework for EEG Monitoring and Real-time Anomaly Prediction: **DAC'20** ②



~94% Seizure Prediction Accuracy

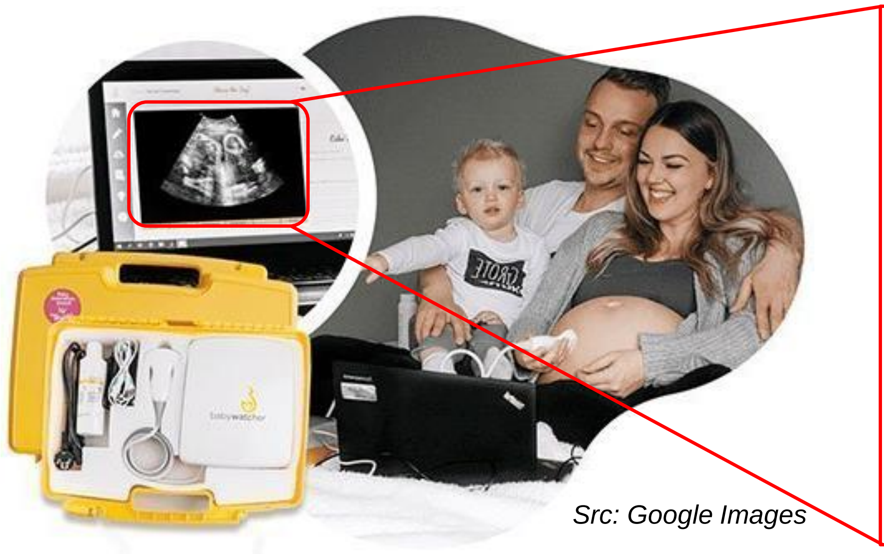

A
User Requirements
DNN Quality Metrics (Classification Accuracy, Precision, Recall, F1-score, etc.)
B
Hardware C
Wearables/ Mobile Phone
Desktop CPU
Server/GPU
C
Data
New Labels ← Existing Labels
Adding Samples ← Data Interpolation
D
Generation of Deep Neural Network Architectures
Block$_n$
Output
E
Exploration of Deep Neural Networks Architectures
Best Network
Training & Testing of selected networks
& Memory Optimization
F
Model Compression
uning
10×
2
1
0
… 95
age Pruned
Memory [MB]
tization
60×
Pruned 6 5 … 2
Number of Bits

53x Reduction in Hardware Overhead for 0.2% Quality Loss

NAS for HW-Constrained Healthcare DNNs: **(IEEE IoT'21)** ③

29

EdgeAI for Healthcare: Moore4Medical EU Project


Src: Google Images

Next Generation Ultrasound

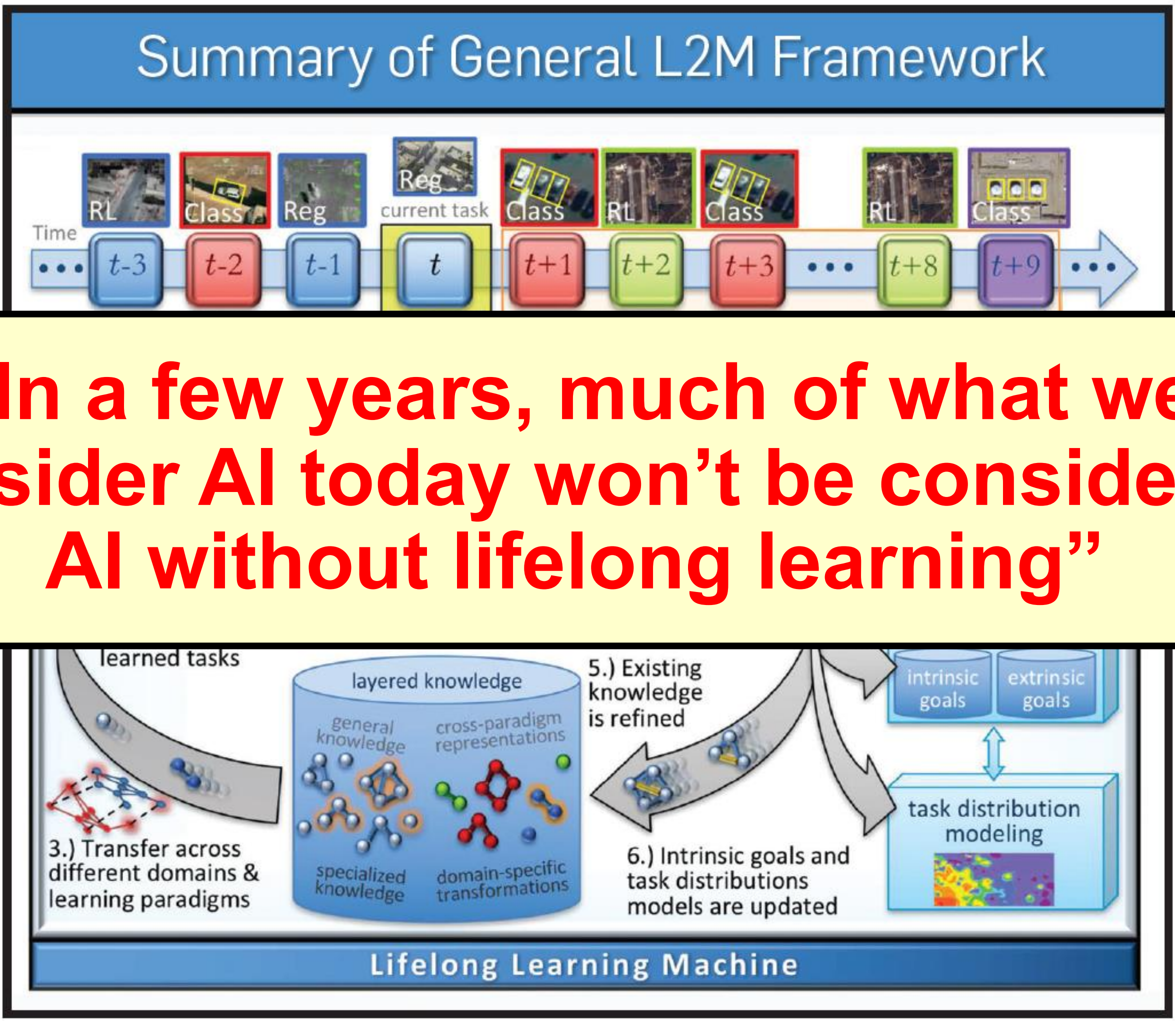
□ Data Acquisition
□ 3D Reconstruction
□ Edge Processing

□ AI algorithms for detecting fetus' anatomical features
□ Hardware accelerator for high throughput feature extraction
□ Closed-loop system for real-time user feedback

□ Investigating DL architectures and statistical ML techniques for classification, segmentation, and anatomical feature extraction
□ Evaluating requirements of proposed algorithms to develop energy-efficient hardware accelerators for edge processing
□ Develop **FPGA prototype** to demonstrate the efficacy of the accelerator and deployability of the HW-SW system

Moore4Medical

Lifelong Learning in Artificial Neural Networks


Summary of General L2M Framework
Time
RL
Class
Reg
Reg
current task
Class
RL
Class
RL
Class
t-3
t-2
t-1
t
t+1
t+2
t+3
t+8
t+9
learned tasks
3.) Transfer across different domains & learning paradigms
layered knowledge
general knowledge
cross-paradigm representations
specialized knowledge
domain-specific transformations
5.) Existing knowledge is refined
intrinsic goals
extrinsic goals
task distribution modeling
6.) Intrinsic goals and task distributions models are updated
Lifelong Learning Machine

"In a few years, much of what we consider AI today won't be considered AI without lifelong learning"

Data and image source: "Lifelong Learning in Artificial Neural Networks" in Communications of the ACM

Robustness for Machine Learning: News Feed

Beware: Galaxy S10's Facial Recognition Easily Fooled with a Photo

Jesus Diaz · Freelance Writer
Updated Mar 11, 2019

Self-driving Uber kills Arizona woman in first fatal crash involving pedestrian

Tempe police said car was in autonomous mode at the time of the crash and that the vehicle hit a woman who later died at a hospital

Hackers trick a Tesla into veering into the wrong lane

https://www.youtube.com/watch?v=a7L51u23YoM

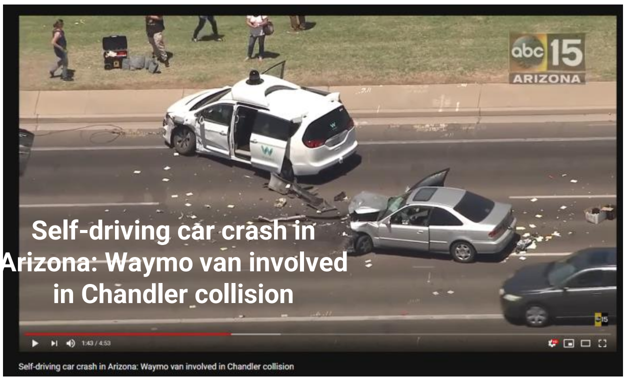
BBC

Tesla Model 3: Autopilot engaged during fatal crash

17 May 2019

Tesla driver dies in first fatal crash while using autopilot mode

The autopilot sensors on the Model S failed to distinguish a white tractor-trailer crossing the highway against a bright sky



Self-driving car crash in Arizona: Waymo van involved in Chandler collision

Self-driving car crash in Arizona: Waymo van involved in Chandler collision

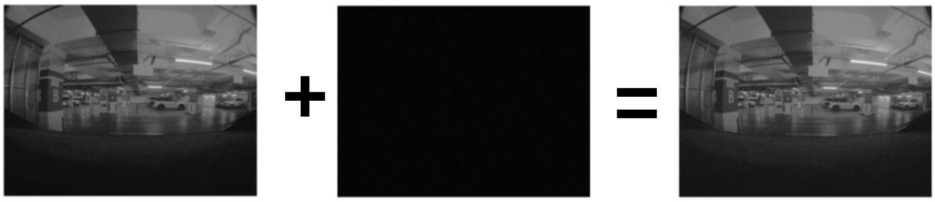
GOOGLE SELF DRIVING CAR CRASHES INTO A BUS

https://www.technologyreview.com/f/613254/hackers-trick-teslas-autopilot-into-veering-towards-oncoming-traffic/

Adversarial Attacks on Tesla Autopilot by Tencent Keen Security Lab

Digital Adversarial Examples

❑ Insert the noise into the DNN input



Rainy Score: 0.0113

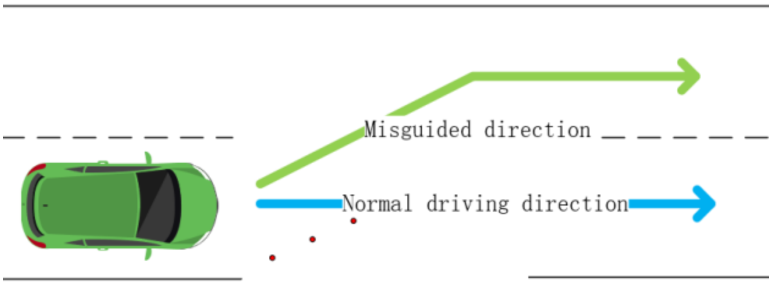
Adversarial Noise

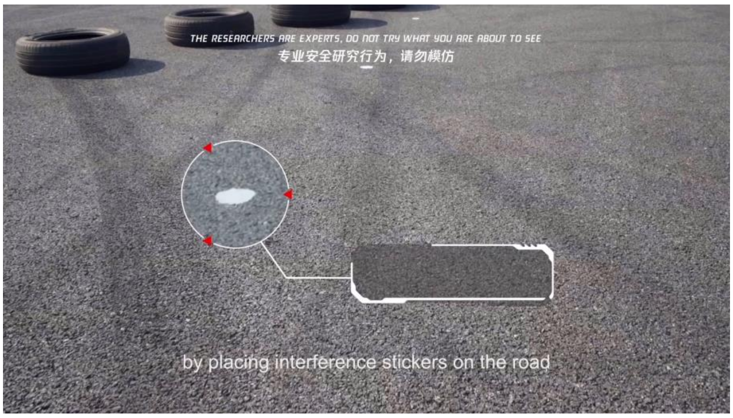
Rainy score: 0.8204

Black-Box Attack

Physical World Adversarial Examples

❑ Place the small stickers on the ground

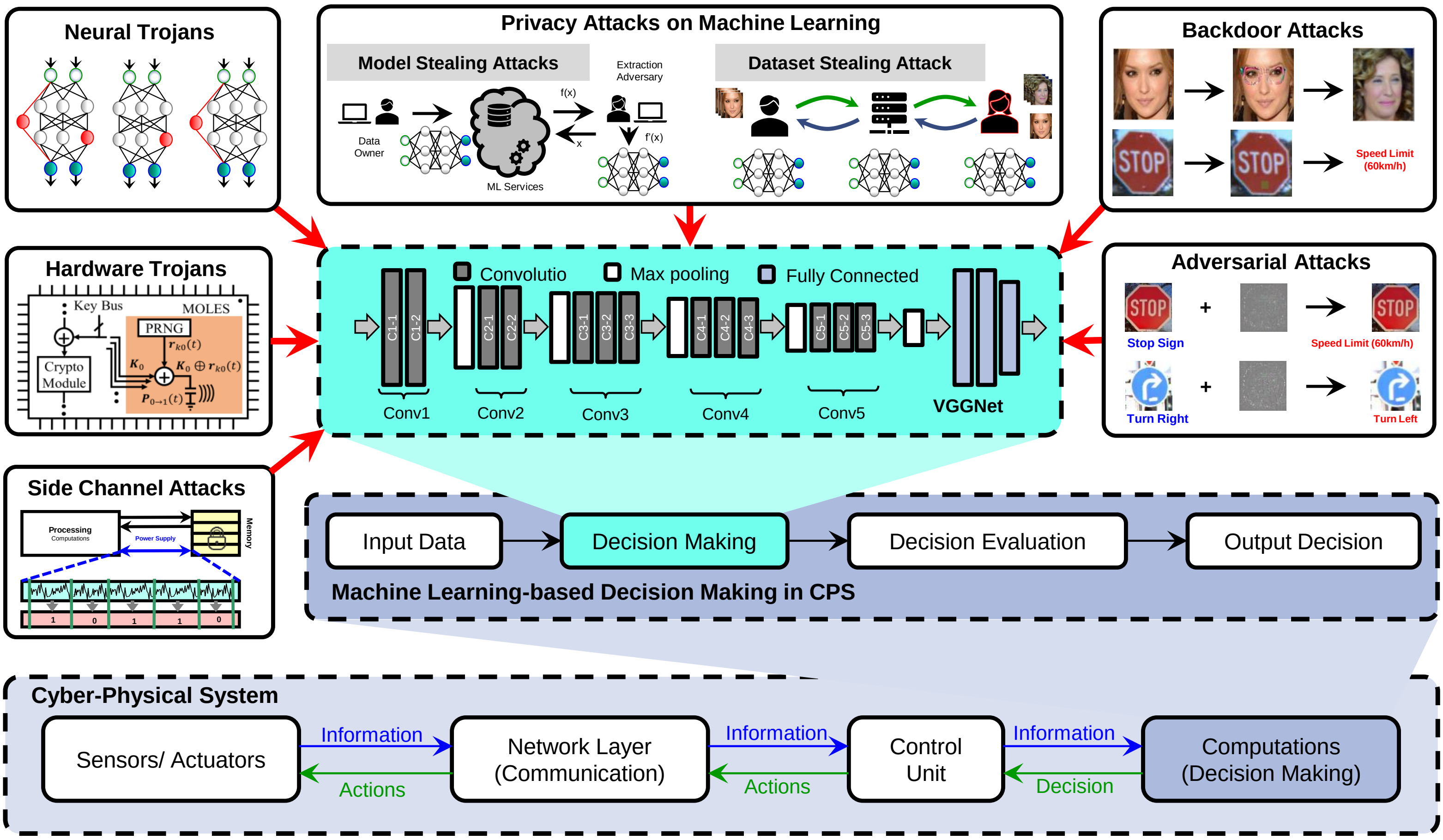



THE RESEARCHERS ARE EXPERTS, DO NOT TRY WHAT YOU ARE ABOUT TO SEE
专业安全研究行为，请勿模仿
by placing interference stickers on the road

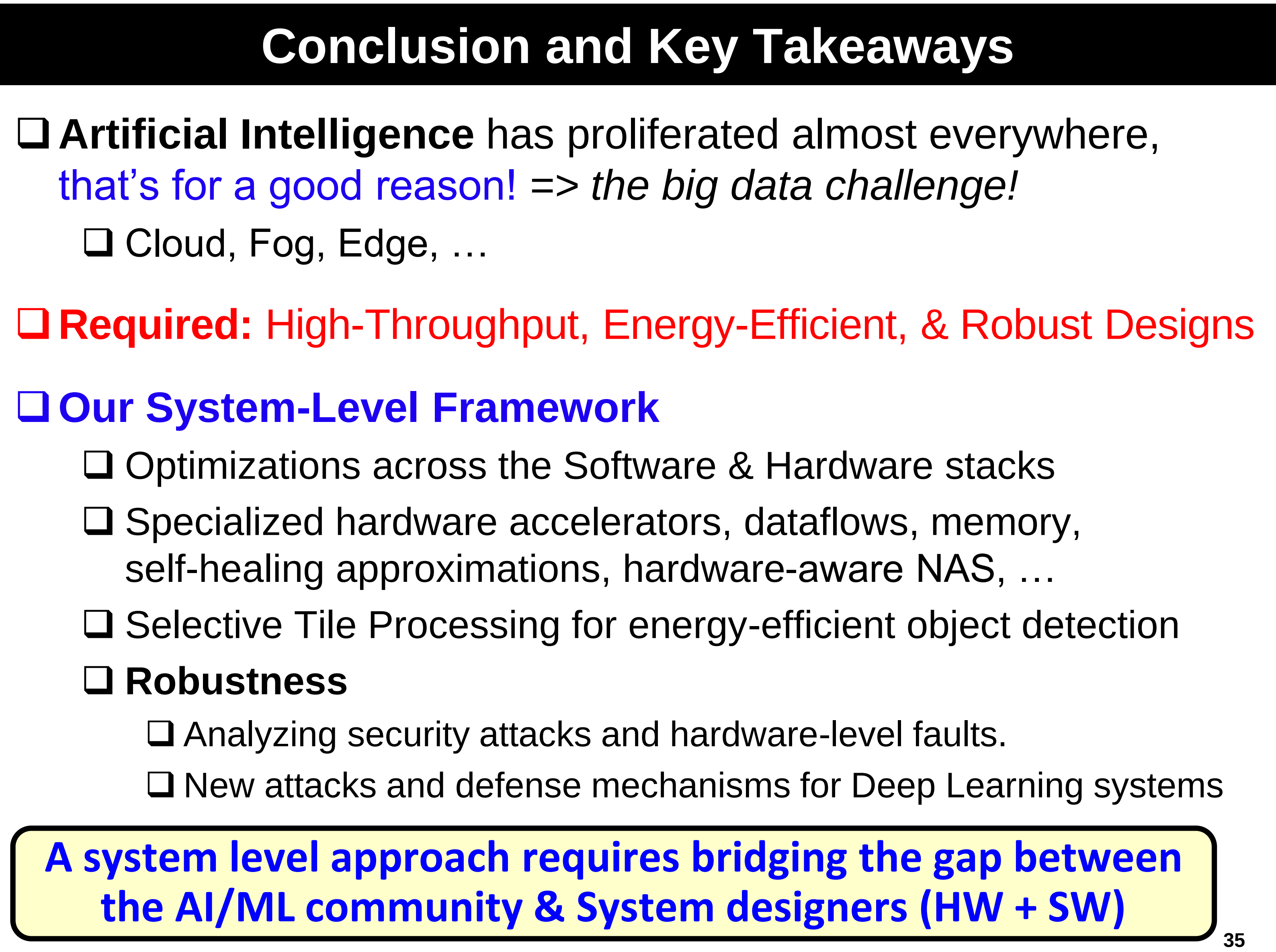
Tencent Keen Security Lab, “Experimental Security Research of Tesla Autopilot” Technical Report 2019-03

33

Security Vulnerabilities in Machine Learning



- M. A. Hanif, F. Khalid, R. V. W. Putra, S. Rehman, M. Shafique, "Robust Machine Learning Systems: Reliability and Security for Deep Neural Networks", in IOLTS-2018, Platja d'Aro, Spain, pp. 257 - 260.
- F. Kriebel, S. Rehman, M. A. Hanif, F. Khalid, M. Shafique, "Robustness for Smart Cyber-Physical Systems and Internet-of-Things: From Adaptive Robustness Methods to Reliability and Security for Machine Learning", ISVLSI-2018, Hong Kong, China, pp. 581-586.



Conclusion and Key Takeaways

□ **Artificial Intelligence** has proliferated almost everywhere, that's for a good reason! => *the big data challenge!*

  □ Cloud, Fog, Edge, …

□ **Required:** High-Throughput, Energy-Efficient, & Robust Designs

□ **Our System-Level Framework**

  □ Optimizations across the Software & Hardware stacks

  □ Specialized hardware accelerators, dataflows, memory, self-healing approximations, hardware-aware NAS, …

  □ Selective Tile Processing for energy-efficient object detection

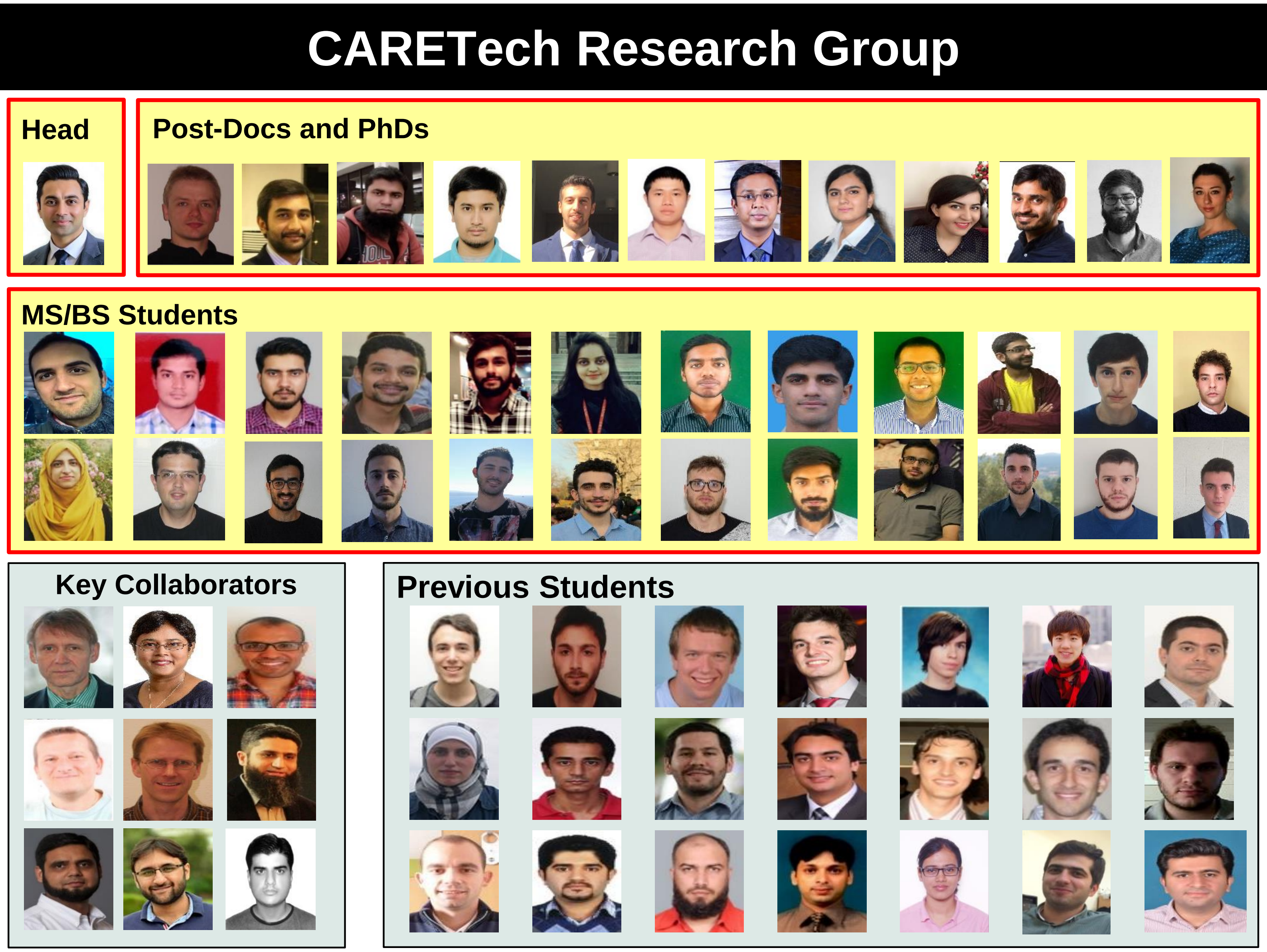
  □ **Robustness**

    □ Analyzing security attacks and hardware-level faults.

    □ New attacks and defense mechanisms for Deep Learning systems

A system level approach requires bridging the gap between the AI/ML community & System designers (HW + SW)

35



CARETech Research Group

Head

Post-Docs and PhDs

MS/BS Students

Key Collaborators

Previous Students

References: ML Papers @ CARE-Tech.

- D, Sabir, M. A. Hanif, A. Hassan, S. Rehman, M. Shafique, “TiQSA: Workload Minimization in Convolutional Neural Networks Using Tile Quantization and Symmetry Approximation”, IEEE **Access**, 2021.
- R. V. W. Putra, M. A. Hanif, M. Shafique, “ROMANet: Fine-Grained Reuse-Driven Off-Chip Memory Access Management and Data Organization for Deep Neural Network Accelerators”, IEEE **TVLSI**, 2021.
- A. Marchisio, V. Mrazek, M. A. Hanif, M. Shafique, “FEECA: Design Space Exploration for Low-Latency and Energy-Efficient Capsule Network Accelerators”, IEEE **TVLSI**, 2021.
- B. S. Prabakaran, A. Akhtar, S. Rehman, O. Hasan and M. Shafique, “BioNetExplorer: Architecture-Space Exploration of Bio-Signal Processing Deep Neural Networks for Wearables”, IEEE **JIOT**, 2021.
- A. Marchisio, G. Pira, M. Martina, G. Masera, M. Shafique, “DVS-Attacks: Adversarial Attacks on Dynamic Vision Sensors for Spiking Neural Networks”, **IJCNN**, 2021.
- A. Viale, A. Marchisio, M. Martina, G. Masera, M. Shafique, “CarSNN: An Efficient Spiking Neural Network for Event-Based Autonomous Cars on the Loihi Neuromorphic Research Processor. **IJCNN**, 2021.
- R. V. W. Putra, M. Shafique, “Q-SpiNN: A Framework for Quantizing Spiking Neural Networks”, **IJCNN**, 2021.
- R. V. W. Putra, M. A. Hanif, M. Shafique, “SparkXD: A Framework for Resilient and Energy-Efficient Spiking Neural Network Inference using Approximate DRAM”, **DAC**, 2021.
- R. V. W. Putra, M. Shafique, “SpikeDyn: A Framework for Energy-Efficient Spiking Neural Networks with Continual and Unsupervised Learning Capabilities in Dynamic Environments”, **DAC**, 2021.
- M. A. Hanif, M. Shafique, “DNN-Life: An Energy-Efficient Aging Mitigation Framework for Improving the Lifetime of On-Chip Weight Memories in Deep Neural Network Hardware Architectures”, **DATE**, 2021.
- R. El-Allami, A. Marchisio, M. Shafique, I. Alouani, “Securing Deep Spiking Neural Networks against Adversarial Attacks through Inherent Structural Parameters”, **DATE**, 2021.
- M. Capra, B. Bussolino, A. Marchisio, G. Masera, M. Martina, M. Shafique, “Hardware and Software Optimizations for Accelerating Deep Neural Networks: Survey of Current Trends, Challenges, and the Road Ahead”, IEEE **Access**, 2020.

References: ML Papers @ CARE-Tech.

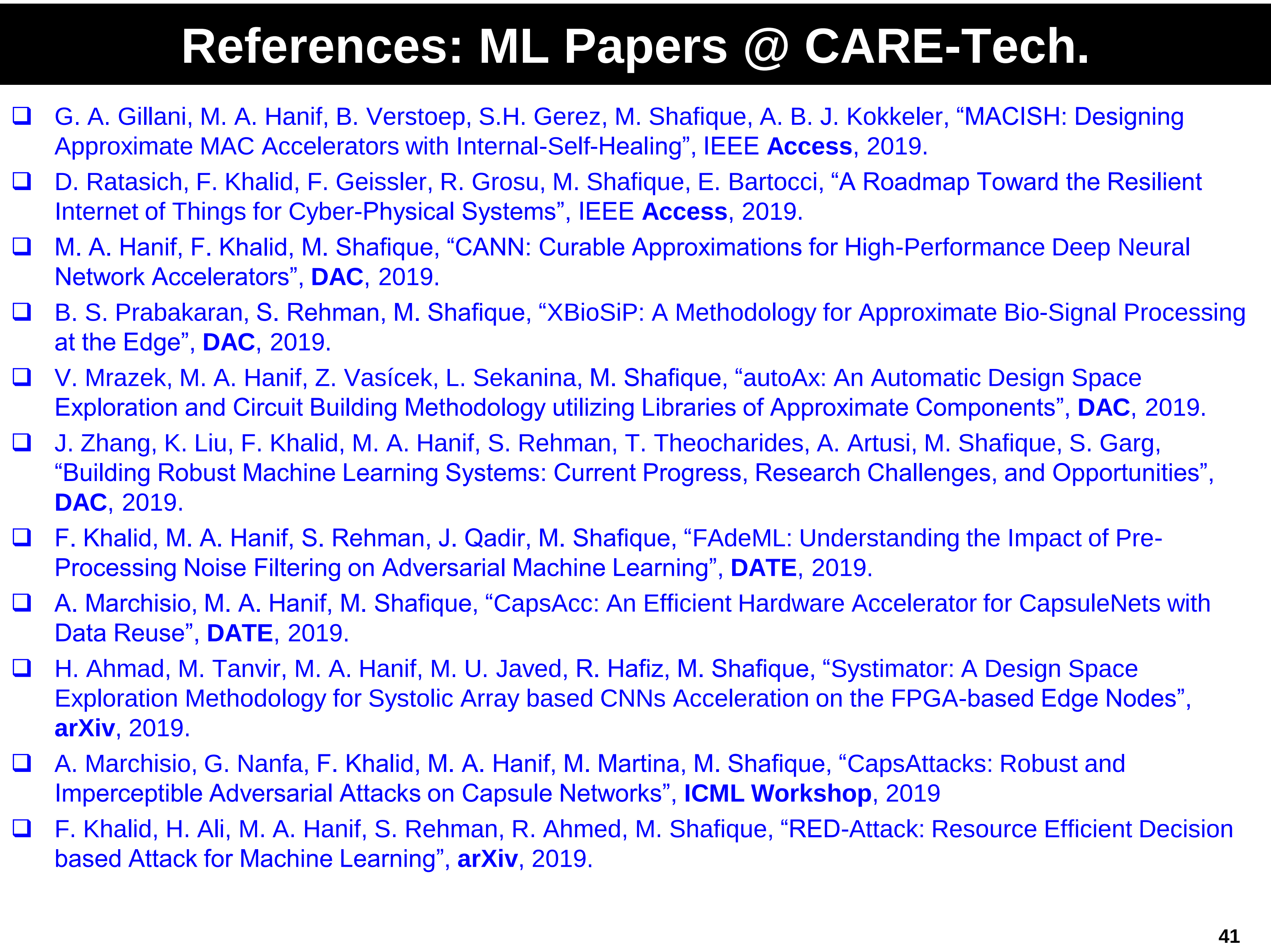
- M. A. Hanif, A. Manglik, M. Shafique, “Resistive Crossbar-Aware Neural Network Design and Optimization”, IEEE **Access**, 2020.
- A. Marchisio, V. Mrazek, M. A. Hanif, M. Shafique, “DESCNet: Developing Efficient Scratchpad Memories for Capsule Network Hardware”, IEEE **TCAD**, 2020.
- A. Marchisio, A. Massa, B. Bussolino, V. Mrazek, M. Martina, M. Shafique, “NASCaps: A Framework for Neural Architecture Search to Optimize the Accuracy and Hardware Efficiency of Convolutional Capsule Networks”, **ICCAD**, 2020.
- F. Khalid, M. A. Hanif, M. Shafique, “Exploiting Vulnerabilities in Deep Neural Networks: Adversarial and Fault-Injection Attacks”, **CYBER**, 2020.
- A. Colucci, A. Marchisio, B. Bussolino, V. Mrazek, M. Martina, G. Masera, M. Shafique, “A Fast Design Space Exploration Framework for the Deep Learning Accelerators”, **CODES+ISSS** (WiP), 2020.
- A. Marchisio, B. Bussolino, A. Colucci, M. A. Hanif, M. Martina, G. Masera, M. Shafique, “FasTrCaps: An Integrated Framework for Fast yet Accurate Training of Capsule Networks”, **IJCNN**, 2020.
- R. Massa, A. Marchisio, M. Martina, M. Shafique, “An Efficient Spiking Neural Network for Recognizing Gestures with a DVS Camera on the Loihi Neuromorphic Processor”, **IJCNN**, 2020.
- A. Marchisio, G. Nanfa, F. Khalid, M. A. Hanif, M. Martina, M. Shafique, “Is Spiking Secure? A Comparative Study on the Security Vulnerabilities of Spiking and Deep Neural Networks”, **IJCNN**, 2020.
- V. Venceslai, A. Marchisio, I. Alouani, M. Martina, M. Shafique, “NeuroAttack: Undermining Spiking Neural Networks Security through Externally Triggered Bit-Flips”, **IJCNN**, 2020.
- F. Khalid, H. Ali, M. A. Hanif, S. Rehman, R. Ahmed, M. Shafique, “FaDec: A Fast Decision-based Attack for Adversarial Machine Learning”, **IJCNN**, 2020.
- R. V. Wicaksana Putra, M. A. Hanif, M. Shafique, “DRMap: A Generic DRAM Data Mapping Policy for Energy-Efficient Processing of Convolutional Neural Networks”, **DAC**, 2020.
- A. Marchisio, B. Bussolino, A. Colucci, M. Martina, G. Masera, M. Shafique, “Q-CapsNets: A Specialized Framework for Quantizing Capsule Networks”, **DAC**, 2020.

References: ML Papers @ CARE-Tech.

- ❑ B. S. Prabakaran, A. García Jiménez, G. M. Martínez, M. Shafique, “EMAP: A Cloud-Edge Hybrid Framework for EEG Monitoring and Cross-Correlation Based Real-time Anomaly Prediction”, **DAC**, 2020.
- ❑ M. A. Hanif, M. Shafique, "Dependable Deep Learning: Towards Cost-Efficient Resilience of Deep Neural Network Accelerators against Soft Errors and Permanent Faults", **IOLTS**, 2020.
- ❑ L.-H. Hoang, M. A. Hanif, M. Shafique, "FT-ClipAct: Resilience Analysis of Deep Neural Networks and Improving their Fault Tolerance using Clipped Activation", **DATE**, 2020.
- ❑ A. Marchisio, V. Mrazek, M. A. Hanif, M. Shafique, "ReD-CaNe: A Systematic Methodology for Resilience Analysis and Design of Capsule Networks under Approximations", **DATE**, 2020.
- ❑ M. Naseer, M. F. Minhas, F. Khalid, M. A. Hanif, O. Hasan, M. Shafique, “FANNet: Formal Analysis of Noise Tolerance, Training Bias and Input Sensitivity in Neural Networks”, **DATE**, 2020.
- ❑ J. Castro-Godínez, D. Hernández-Araya, M. Shafique, J. Henkel, “Approximate Acceleration for CNN-based Applications on IoT Edge Devices”, **LASCAS**, 2020.
- ❑ R. V. Wicaksana Putra, M. Shafique, “FSpiNN: An Optimization Framework for Memory- and Energy-Efficient Spiking Neural Networks”, IEEE **TCAD**, ESWeek-Special Issue, 2020.
- ❑ H. Ahmad, T. Arif, M. A. Hanif, R. Hafiz, M. Shafique, “SuperSlash: A Unified Design Space Exploration and Model Compression Methodology for Design of Deep Learning Accelerators with Reduced Off-Chip Memory Access”, IEEE **TCAD**, ESWeek-Special Issue, 2020.
- ❑ F. Khalid, S. R. Hasan, S. Zia, O. Hasan, F. Awwad, M. Shafique, “MacLeR: Machine Learning-based Run-Time Hardware Trojan Detection in Microprocessors in Resource-Constrained IoT Edge Devices”, IEEE **TCAD**, ESWeek-Special Issue, 2020.
- ❑ P. Achararit, M. A. Hanif, R. V. Wicaksana Putra, M. Shafique, Y. Hara-Azumi, “APNAS: Accuracy-and-Performance-Aware Neural Architecture Search Considering Neural Hardware Accelerators”, IEEE **Access**, 2020.

References: ML Papers @ CARE-Tech.

- M. Riaz, R. Hafiz, S. A. Khaliq, M. Faisal, M. Ali, M. Shafique, “CAxCNN: Towards the use of Canonic Sign Digit based Approximation for Hardware-Friendly Convolutional Neural Networks”, IEEE **Access**, 2020.
- S. Ud Din, N. Akhtar, M. S. Younis, F. Shafait, A. Mansoor, M. Shafique, “Pseudo Steganographic Universal Adversarial Perturbations”, **PRL**, 2020.
- M. Shafique, M. Naseer, T. Theocharides, C. Kyrkou, O. Mutlu, L. Orosa, J. Choi, “Robust Machine Learning Systems: Challenges, Current Trends, Perspectives, and the Road Ahead”, IEEE **D&T**, 2020.
- Z. Yahya, M. Hassan, M. S. Younis, M. Shafique, “Probabilistic Analysis of Targeted Attacks Using Transform-Domain Adversarial Examples”, IEEE **Access**, 2020
- M. Capra, B. Bussolino, A. Marchisio, M. Shafique, G. Masera, M. Martina, “An Updated Survey of Efficient Architectures for Accelerating Deep Neural Networks”, **Future Internet**, 2020.
- M. A. Hanif, M. Shafique, “SalvageDNN: Salvaging Deep Neural Network Accelerators with Permanent Faults through Fault-Aware Mapping”, **RSTA**, 2019.
- V. Mrazek, Z. Vasicek, L. Sekanina, M. A. Hanif, M. Shafique, “ALWANN: Automatic Layer-Wise Approximation of Deep Neural Network Accelerators without Retraining”, **ICCAD**, 2019
- M. A. Hanif, M. Z. Akbar, R. Ahmed, S. Rehman, A. Jantsch, M. Shafique, “MemGANs: Memory Management for Energy-Efficient Acceleration of Complex Computations in Hardware Architectures for Generative Adversarial Networks”, **ISLPED**, 2019.
- A. Marchisio, M. A. Hanif, F. Khalid, G. Plastiras, C. Kyrkou, T. Theocharides, M. Shafique, “Deep Learning for Edge Computing: Current Trends, Cross-Layer Optimizations, and Open Research Challenges”, **ISVLSI**, 2019.
- F. Khalid, H. Ali, H. Tariq, M. A. Hanif, S. Rehman, R. Ahmed, M. Shafique, “QuSecNets: Quantization-based Defense Mechanism forSecuring Deep Neural Network against Adversarial Attacks”, **IOLTS**, 2019.
- F. Khalid, M. A. Hanif, S. Rehman, R. Ahmed, M. Shafique, “TrISec: Training Data-Unaware ImperceptibleSecurity Attacks on Deep Neural Networks”, **IOLTS**, 2019



References: ML Papers @ CARE-Tech.

❑ G. A. Gillani, M. A. Hanif, B. Verstoep, S.H. Gerez, M. Shafique, A. B. J. Kokkeler, “MACISH: Designing Approximate MAC Accelerators with Internal-Self-Healing”, IEEE **Access**, 2019.

❑ D. Ratasich, F. Khalid, F. Geissler, R. Grosu, M. Shafique, E. Bartocci, “A Roadmap Toward the Resilient Internet of Things for Cyber-Physical Systems”, IEEE **Access**, 2019.

❑ M. A. Hanif, F. Khalid, M. Shafique, “CANN: Curable Approximations for High-Performance Deep Neural Network Accelerators”, **DAC**, 2019.

❑ B. S. Prabakaran, S. Rehman, M. Shafique, “XBioSiP: A Methodology for Approximate Bio-Signal Processing at the Edge”, **DAC**, 2019.

❑ V. Mrazek, M. A. Hanif, Z. Vasícek, L. Sekanina, M. Shafique, “autoAx: An Automatic Design Space Exploration and Circuit Building Methodology utilizing Libraries of Approximate Components”, **DAC**, 2019.

❑ J. Zhang, K. Liu, F. Khalid, M. A. Hanif, S. Rehman, T. Theocharides, A. Artusi, M. Shafique, S. Garg, “Building Robust Machine Learning Systems: Current Progress, Research Challenges, and Opportunities”, **DAC**, 2019.

❑ F. Khalid, M. A. Hanif, S. Rehman, J. Qadir, M. Shafique, “FAdeML: Understanding the Impact of Pre-Processing Noise Filtering on Adversarial Machine Learning”, **DATE**, 2019.

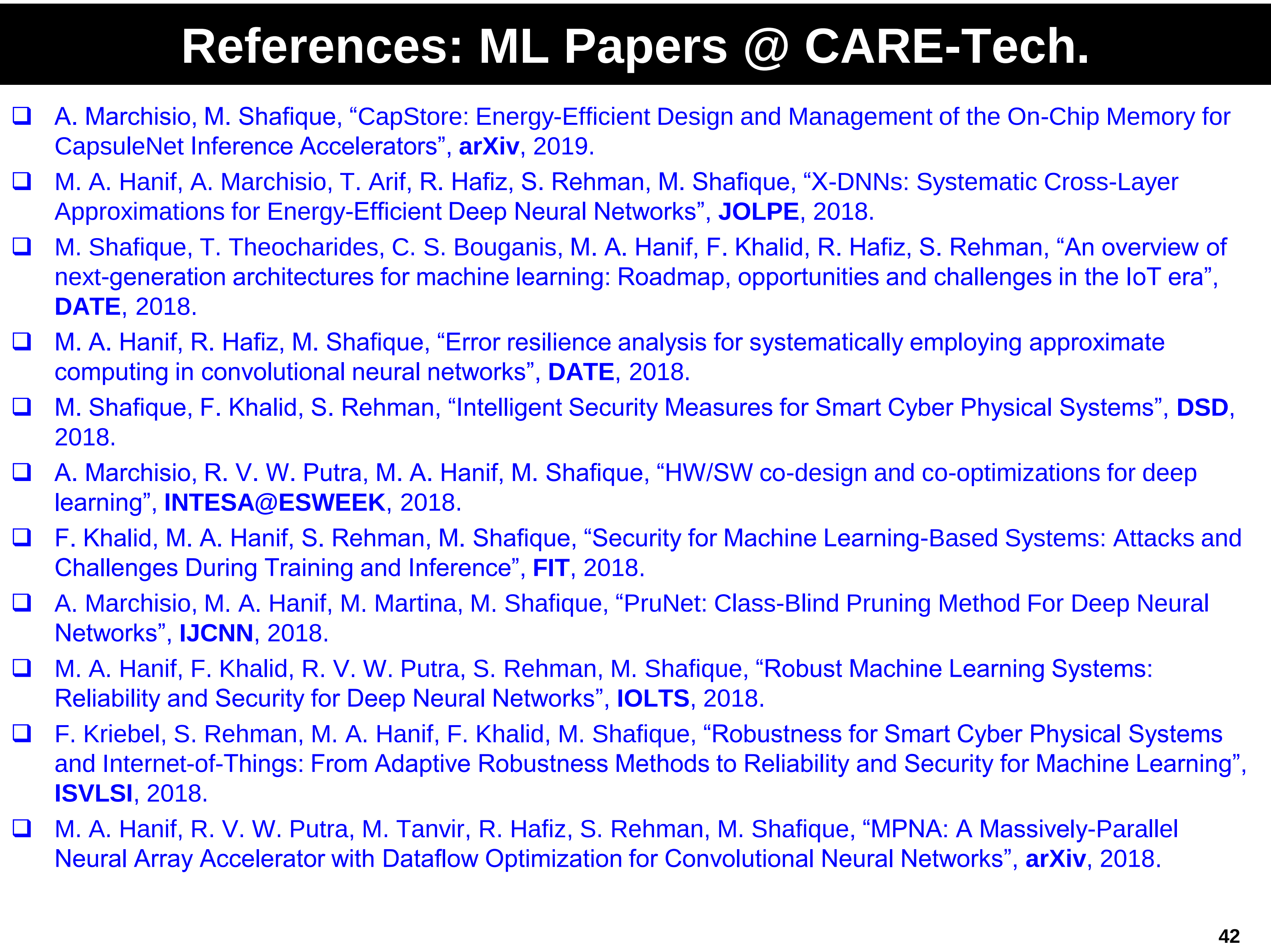
❑ A. Marchisio, M. A. Hanif, M. Shafique, “CapsAcc: An Efficient Hardware Accelerator for CapsuleNets with Data Reuse”, **DATE**, 2019.

❑ H. Ahmad, M. Tanvir, M. A. Hanif, M. U. Javed, R. Hafiz, M. Shafique, “Systimator: A Design Space Exploration Methodology for Systolic Array based CNNs Acceleration on the FPGA-based Edge Nodes”, **arXiv**, 2019.

❑ A. Marchisio, G. Nanfa, F. Khalid, M. A. Hanif, M. Martina, M. Shafique, “CapsAttacks: Robust and Imperceptible Adversarial Attacks on Capsule Networks”, **ICML Workshop**, 2019

❑ F. Khalid, H. Ali, M. A. Hanif, S. Rehman, R. Ahmed, M. Shafique, “RED-Attack: Resource Efficient Decision based Attack for Machine Learning”, **arXiv**, 2019.

41



References: ML Papers @ CARE-Tech.

- □ A. Marchisio, M. Shafique, “CapStore: Energy-Efficient Design and Management of the On-Chip Memory for CapsuleNet Inference Accelerators”, **arXiv**, 2019.
- □ M. A. Hanif, A. Marchisio, T. Arif, R. Hafiz, S. Rehman, M. Shafique, “X-DNNs: Systematic Cross-Layer Approximations for Energy-Efficient Deep Neural Networks”, **JOLPE**, 2018.
- □ M. Shafique, T. Theocharides, C. S. Bouganis, M. A. Hanif, F. Khalid, R. Hafiz, S. Rehman, “An overview of next-generation architectures for machine learning: Roadmap, opportunities and challenges in the IoT era”, **DATE**, 2018.
- □ M. A. Hanif, R. Hafiz, M. Shafique, “Error resilience analysis for systematically employing approximate computing in convolutional neural networks”, **DATE**, 2018.
- □ M. Shafique, F. Khalid, S. Rehman, “Intelligent Security Measures for Smart Cyber Physical Systems”, **DSD**, 2018.
- □ A. Marchisio, R. V. W. Putra, M. A. Hanif, M. Shafique, “HW/SW co-design and co-optimizations for deep learning”, **INTESA@ESWEEK**, 2018.
- □ F. Khalid, M. A. Hanif, S. Rehman, M. Shafique, “Security for Machine Learning-Based Systems: Attacks and Challenges During Training and Inference”, **FIT**, 2018.
- □ A. Marchisio, M. A. Hanif, M. Martina, M. Shafique, “PruNet: Class-Blind Pruning Method For Deep Neural Networks”, **IJCNN**, 2018.
- □ M. A. Hanif, F. Khalid, R. V. W. Putra, S. Rehman, M. Shafique, “Robust Machine Learning Systems: Reliability and Security for Deep Neural Networks”, **IOLTS**, 2018.
- □ F. Kriebel, S. Rehman, M. A. Hanif, F. Khalid, M. Shafique, “Robustness for Smart Cyber Physical Systems and Internet-of-Things: From Adaptive Robustness Methods to Reliability and Security for Machine Learning”, **ISVLSI**, 2018.
- □ M. A. Hanif, R. V. W. Putra, M. Tanvir, R. Hafiz, S. Rehman, M. Shafique, “MPNA: A Massively-Parallel Neural Array Accelerator with Dataflow Optimization for Convolutional Neural Networks”, **arXiv**, 2018.

42

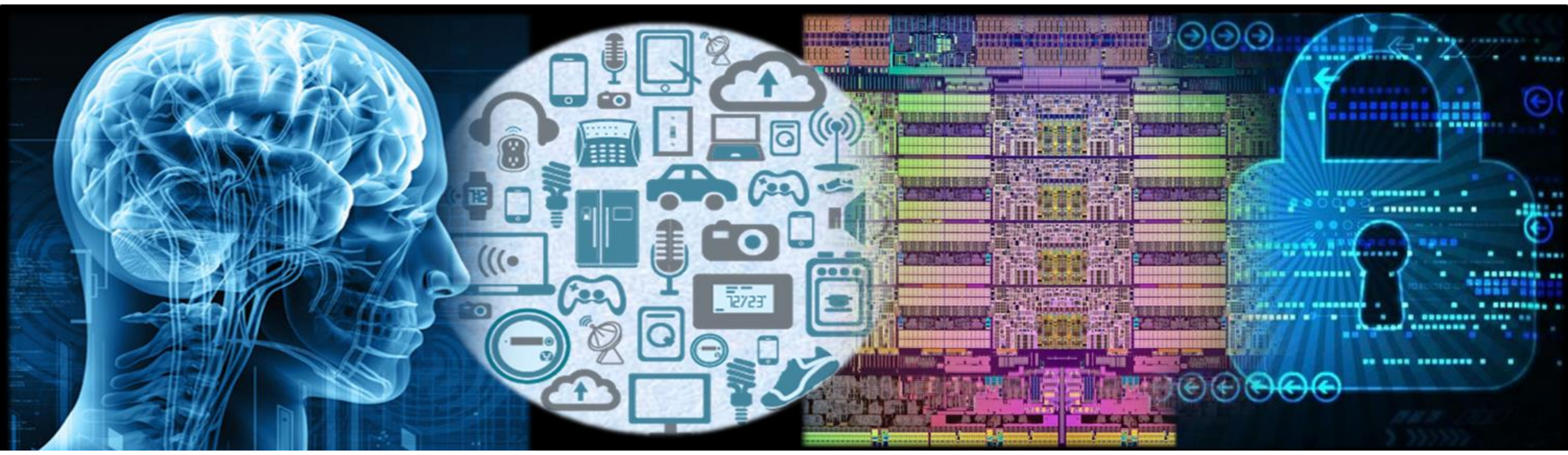
جامعـة نيويورك أبـوظـبي NYU ABU DHABI NYU TANDON SCHOOL OF ENGINEERING CENTER FOR CYBER SECURITY sites.nyuad.nyu.edu/ccs-ad/ CARE Tech Computer Architecture and Robust, Energy-Efficient Technologies Group TU WIEN

Thank You!

Questions?

A. Marchisio

alberto.marchisio@tuwien.ac.at



CPS&IoT'2021
2nd Summer School on Cyber Physical +
Systems and Internet of Things

Dataflow-Based Toolchain for Adaptive Hardware Accelerators Deployment and Monitoring

Daniel Madronal[1], Francesco Ratto[2], Giacomo Valente[3]

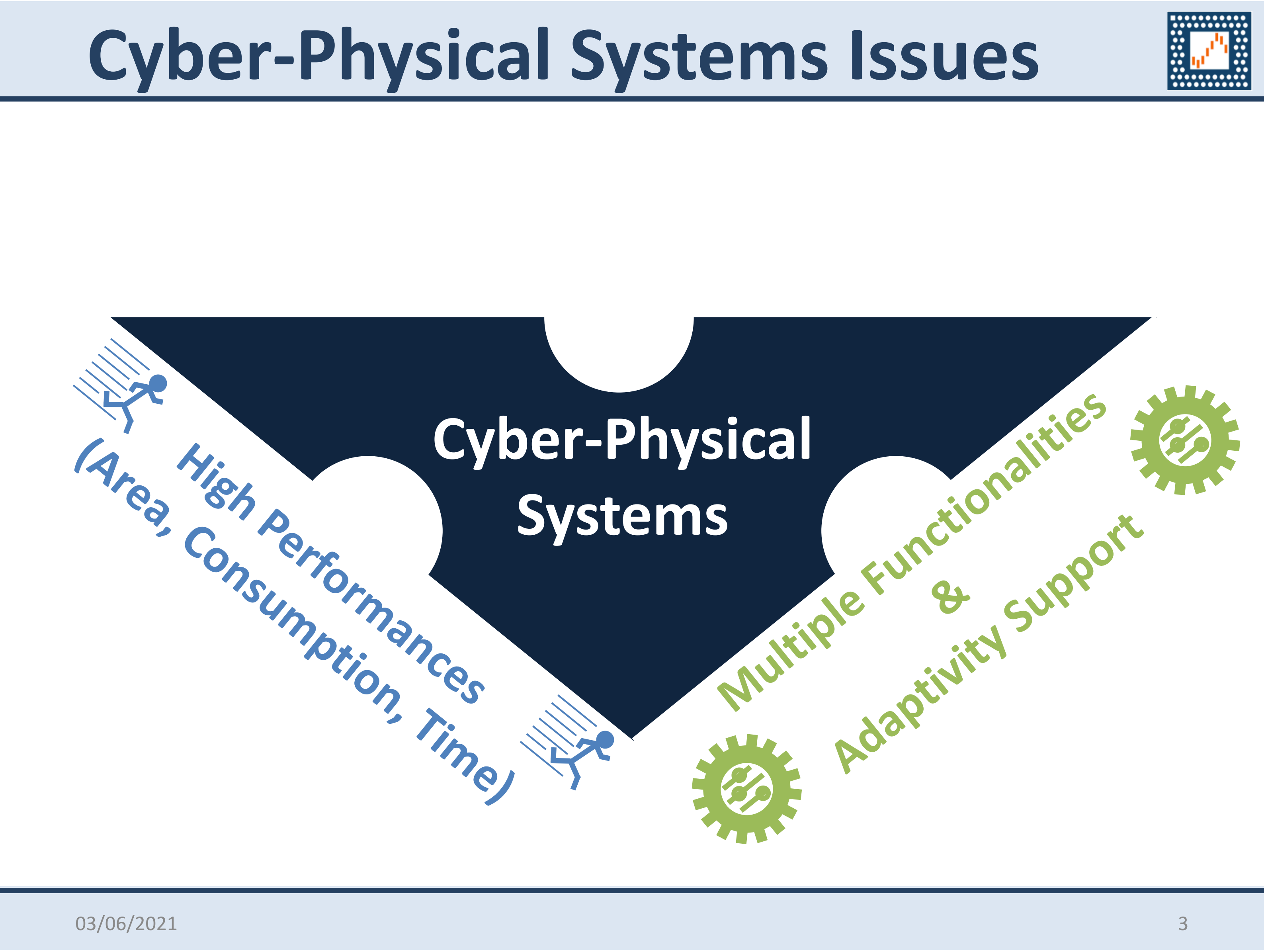
[1]University of Sassari, Intelligent system DEsign and Application (IDEA) Group

[2]University of Cagliari, Diee – Microelectronics and Bioengineering (EOLAB) Group

[3]University of L'Aquila, Disim – Embedded Systems Group

CPS&IoT’2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

Introduction and Motivation



Cyber-Physical Systems Issues

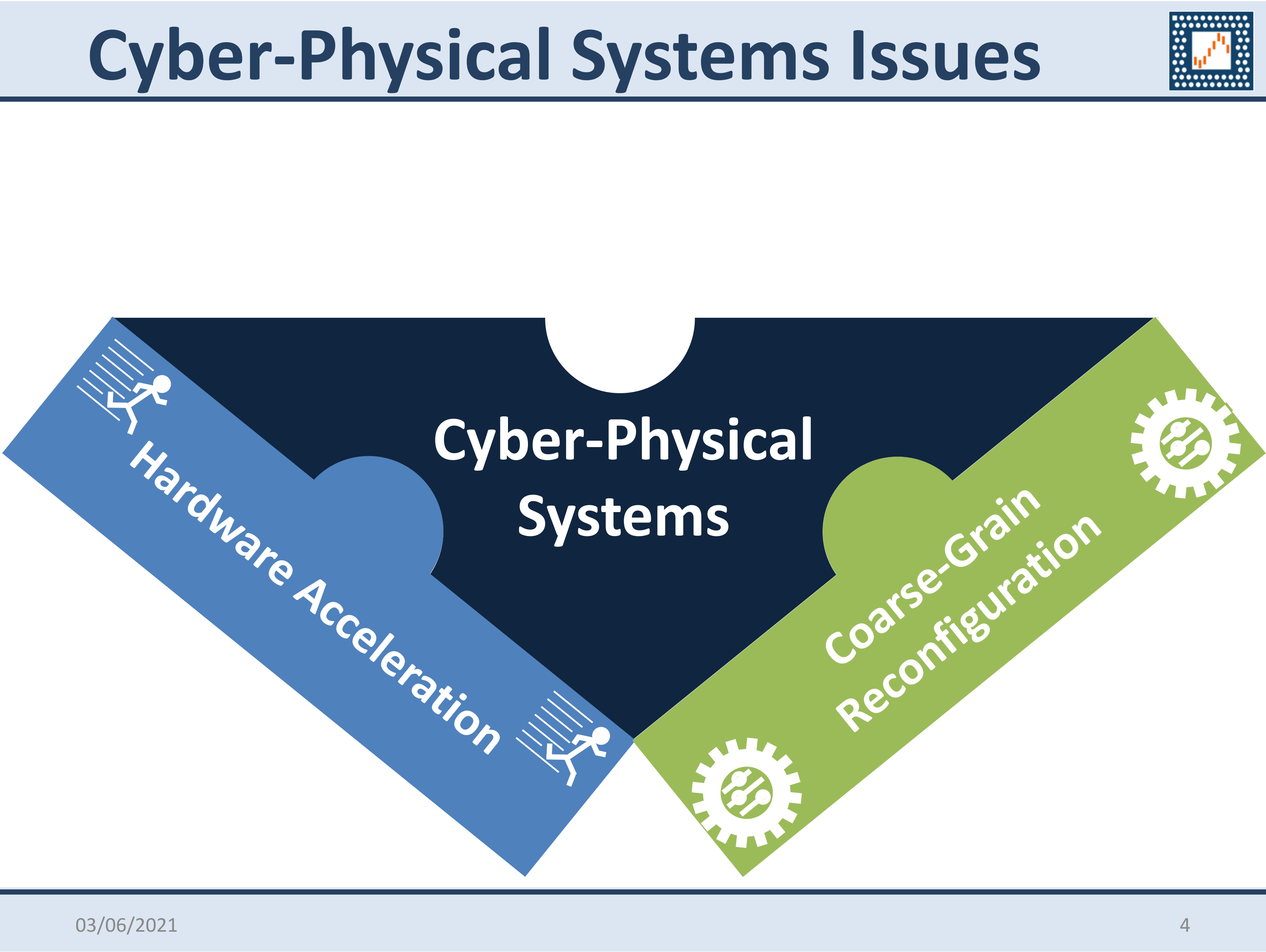
Cyber-Physical Systems

High Performances (Area, Consumption, Time)

Multiple Functionalities & Adaptivity Support

03/06/2021

3



Cyber-Physical Systems Issues

Cyber-Physical Systems

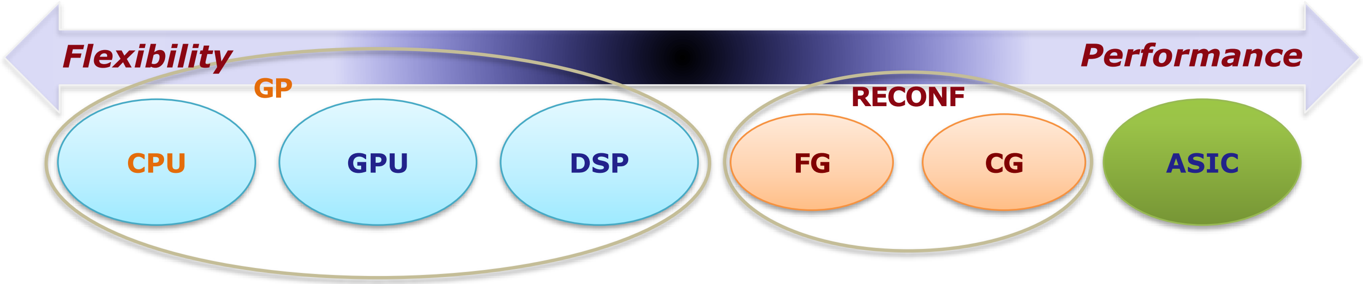
Hardware Acceleration

Coarse-Grain Reconfiguration

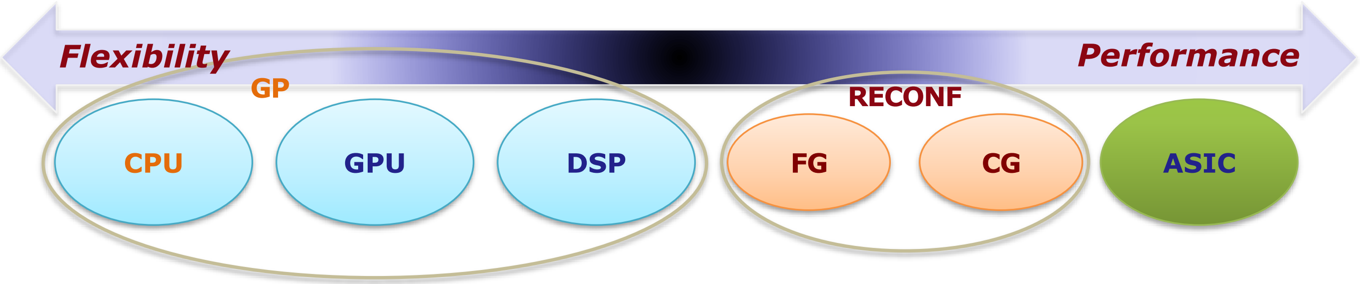
03/06/2021

4

Reconfigurable Hardware

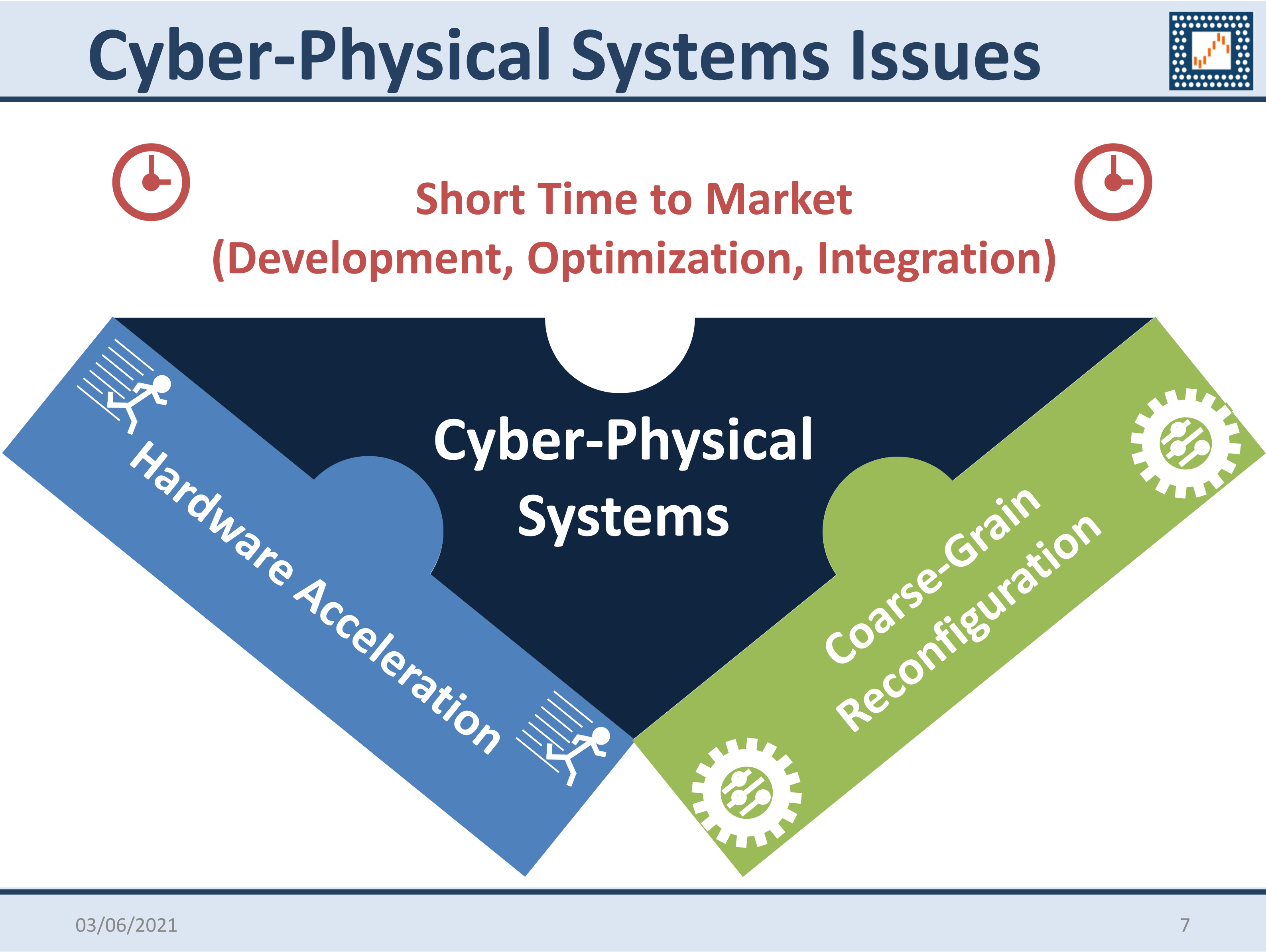


Reconfigurable Hardware



	Fine Grained	Coarse Grained
	bit-level	word-level
Flexibility	🙂	😐
Speed	😐	🙂
Memory	☹	😐

- **Coarse Grained (CG):**
  - both in ASIC and FPGA
  - 1 clock cycle switching, with dedicated switching blocks.
- **Fine Grained (FG):**
  - FPGA only
  - switching requires a new bit-stream



Cyber-Physical Systems Issues

Short Time to Market
(Development, Optimization, Integration)

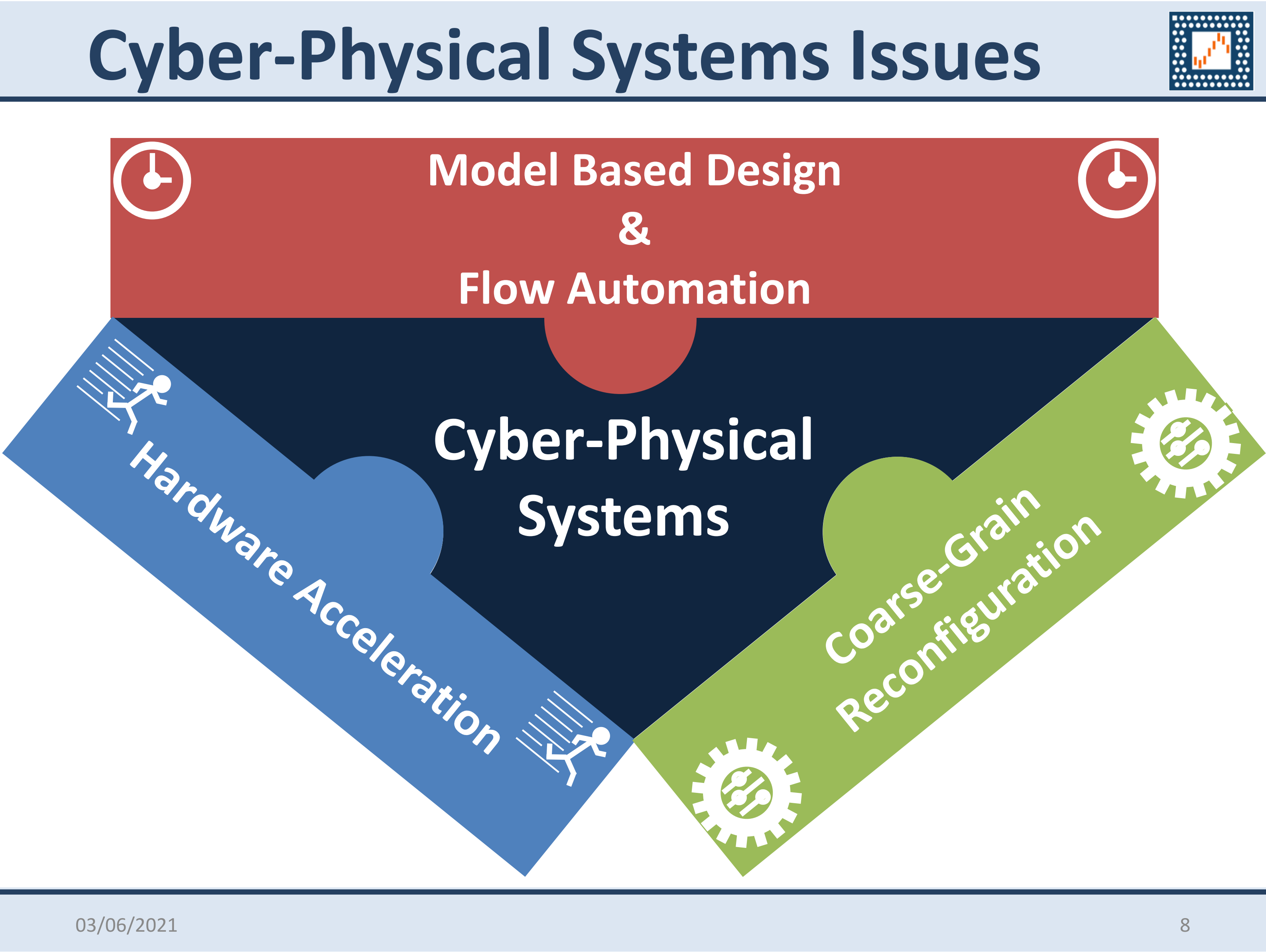
Cyber-Physical Systems

Hardware Acceleration

Coarse-Grain Reconfiguration

03/06/2021

7



Cyber-Physical Systems Issues

Model Based Design
&
Flow Automation

Cyber-Physical Systems

Hardware Acceleration

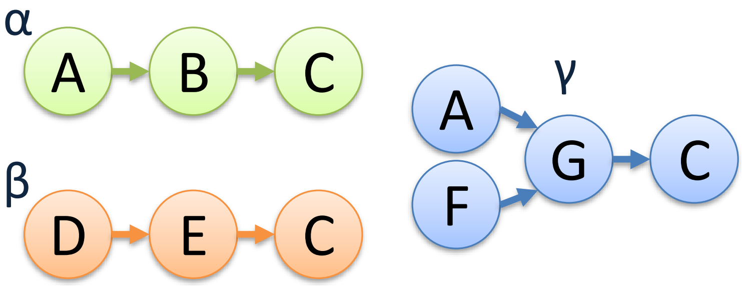
Coarse-Grain Reconfiguration

03/06/2021

8

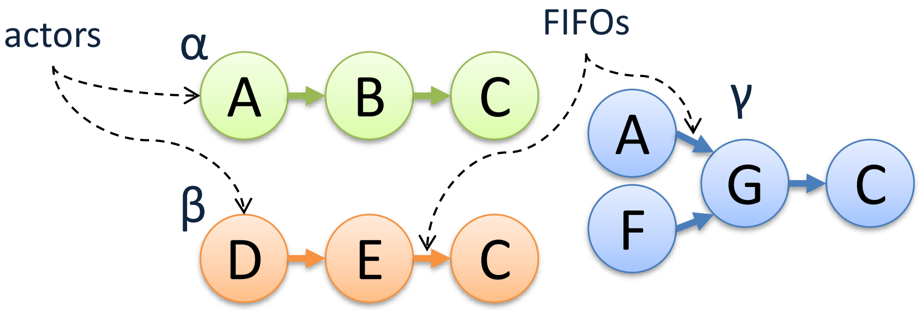
Model-Based Design Automation

Dataflow Models of Computation



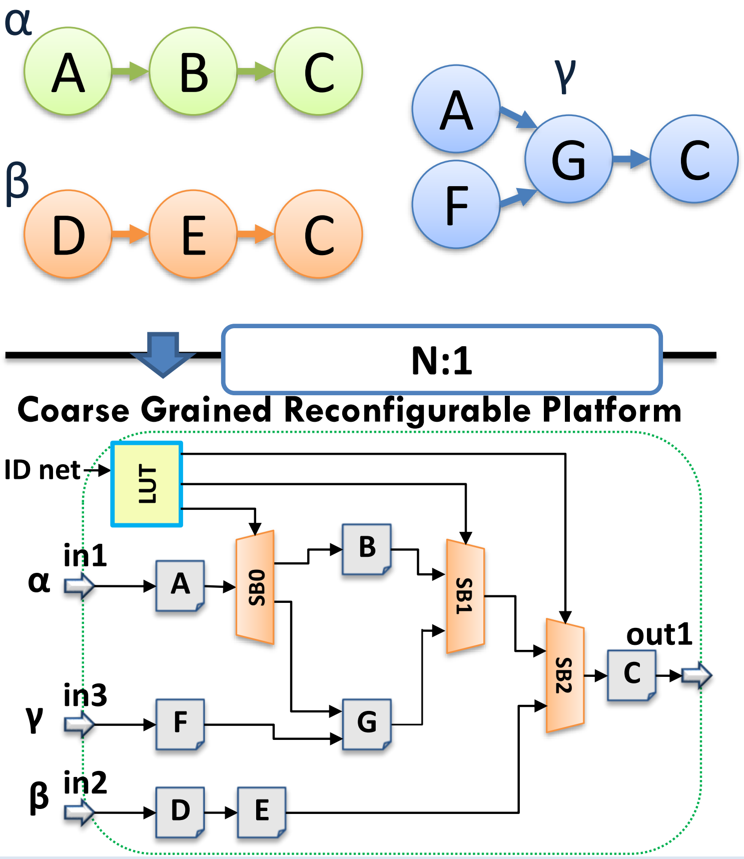
Model-Based Design Automation

Dataflow Models of Computation

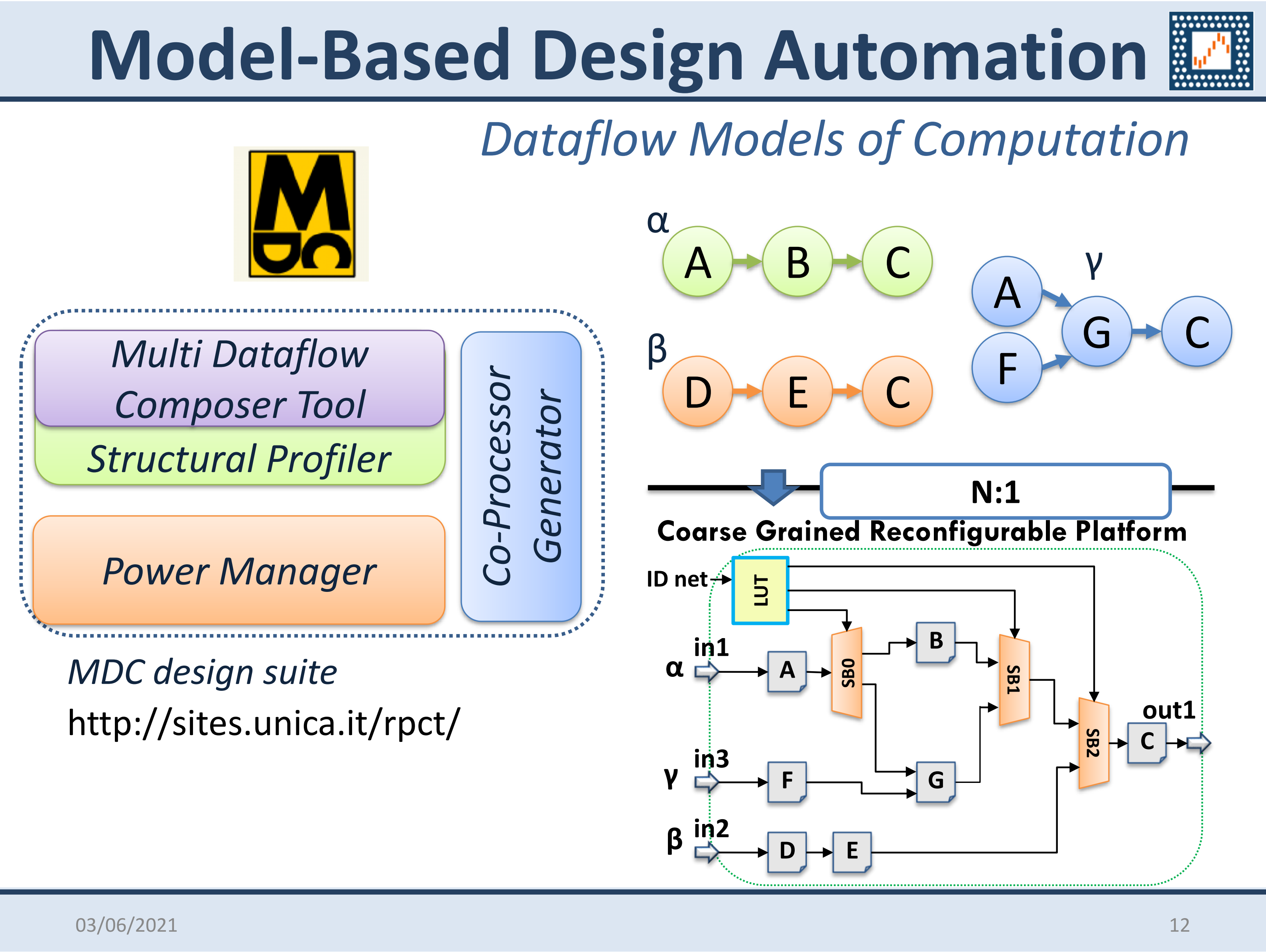


Model-Based Design Automation

Dataflow Models of Computation



03/06/2021 11



Model-Based Design Automation

Dataflow Models of Computation

Multi Dataflow Composer Tool

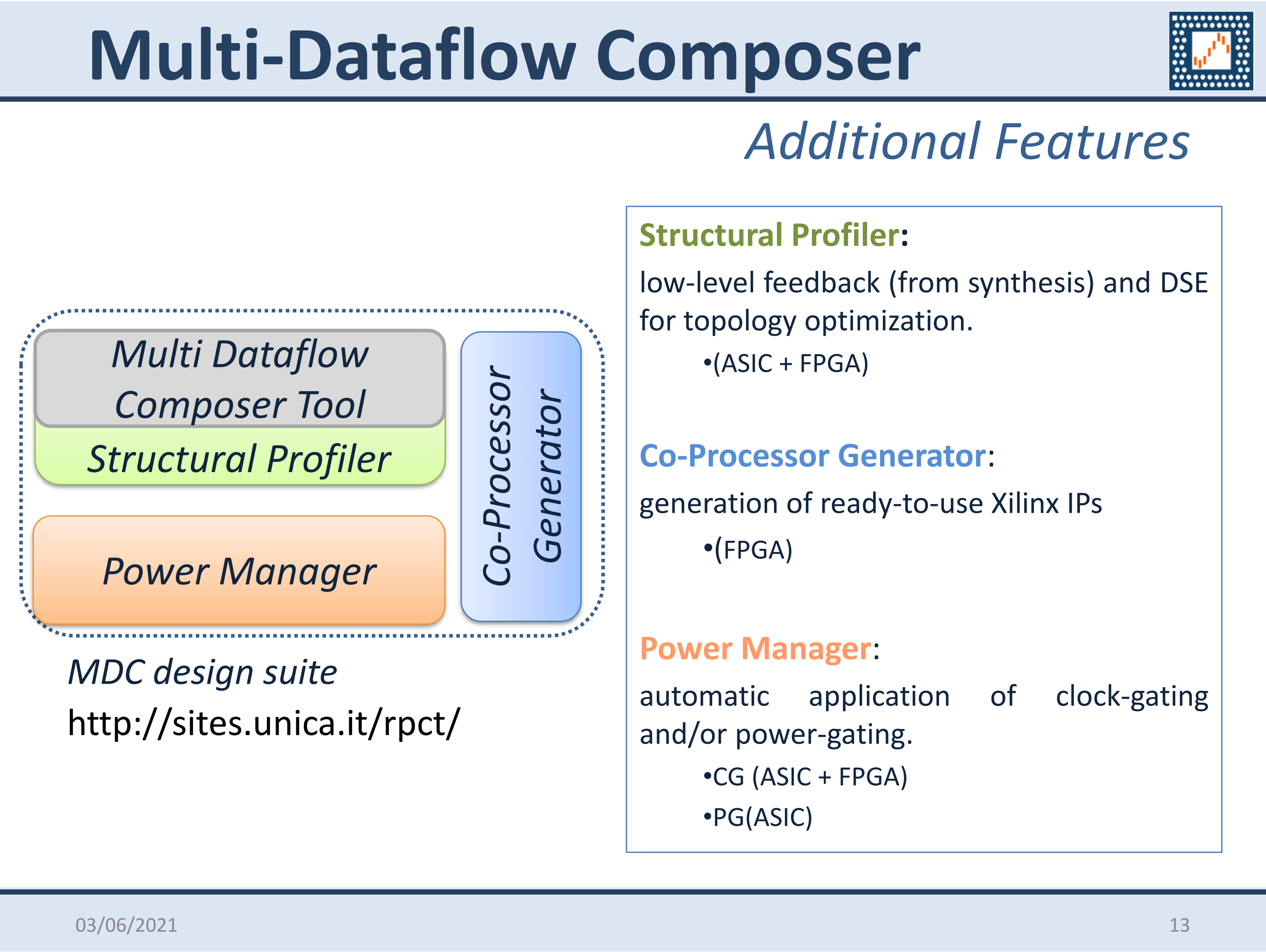
Structural Profiler

Power Manager

Co-Processor Generator

MDC design suite

http://sites.unica.it/rpct/



Multi-Dataflow Composer

Additional Features

Multi Dataflow Composer Tool

Structural Profiler

Power Manager

Co-Processor Generator

MDC design suite

http://sites.unica.it/rpct/

Structural Profiler:

low-level feedback (from synthesis) and DSE for topology optimization.

- (ASIC + FPGA)

Co-Processor Generator:

generation of ready-to-use Xilinx IPs

- (FPGA)

Power Manager:

automatic application of clock-gating and/or power-gating.

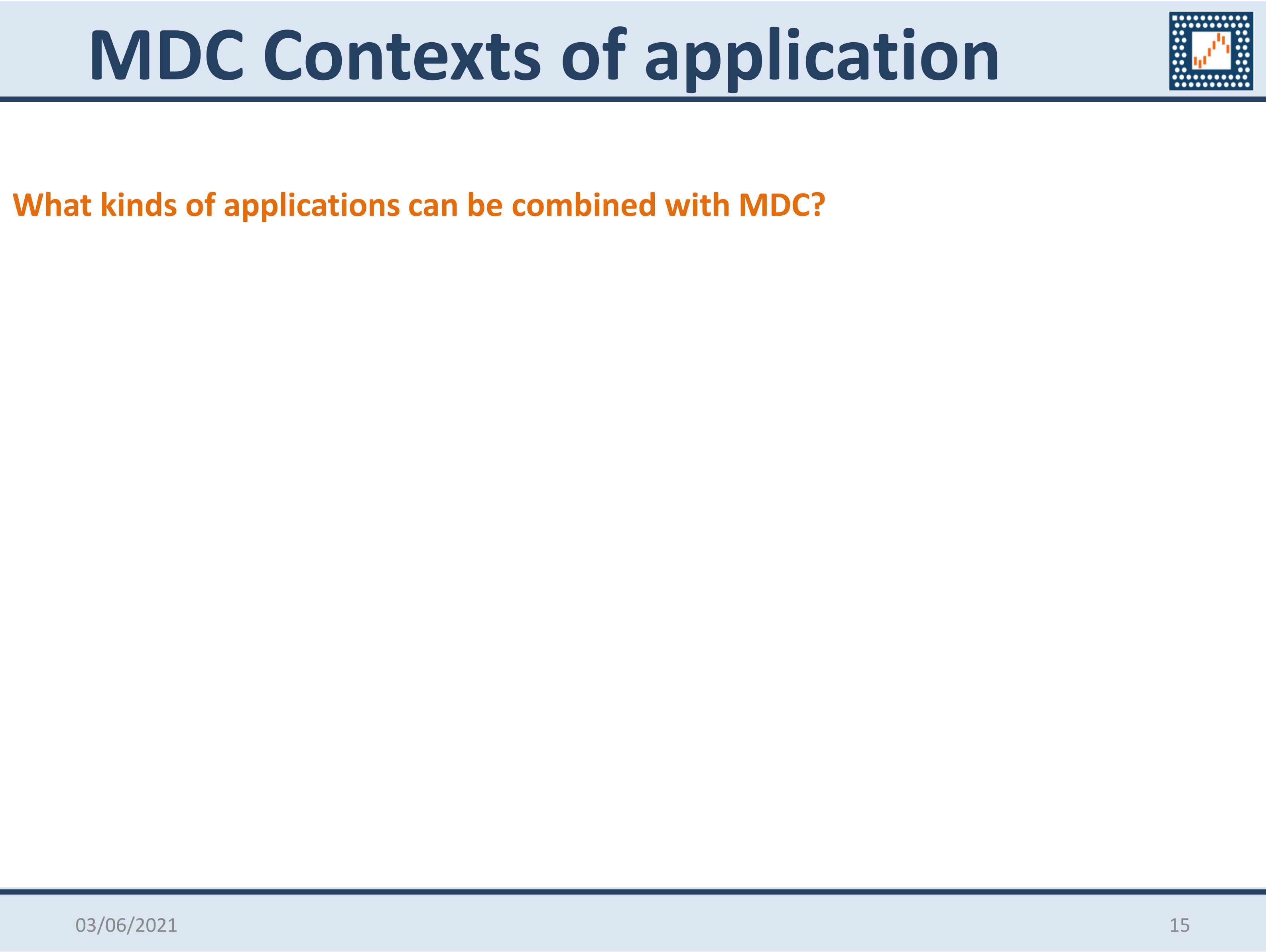
- CG (ASIC + FPGA)
- PG(ASIC)

03/06/2021 13

CPS&IoT'2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

MDC Contexts of Application

uniss
UNIVERSITÀ DEGLI STUDI DI SASSARI



MDC Contexts of application

What kinds of applications can be combined with MDC?

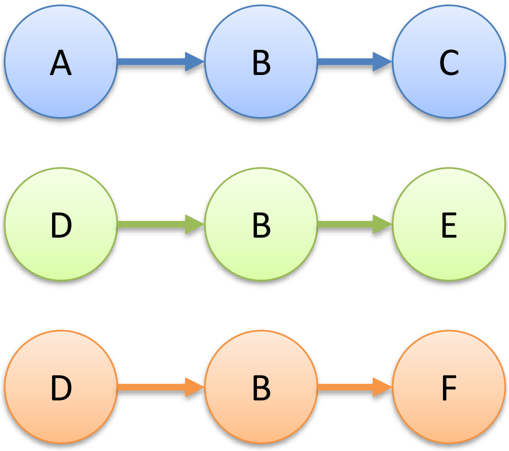
03/06/2021

15

MDC Contexts of application

What kinds of applications can be combined with MDC?

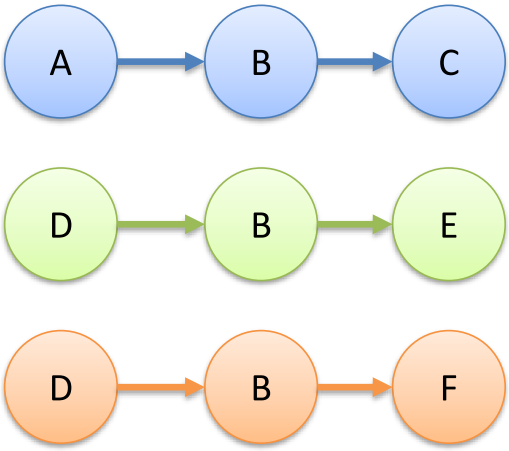
1. **Different applications with common computational operations**: it is achieved by considering applications from the same **application field** or **small actor granularities**.



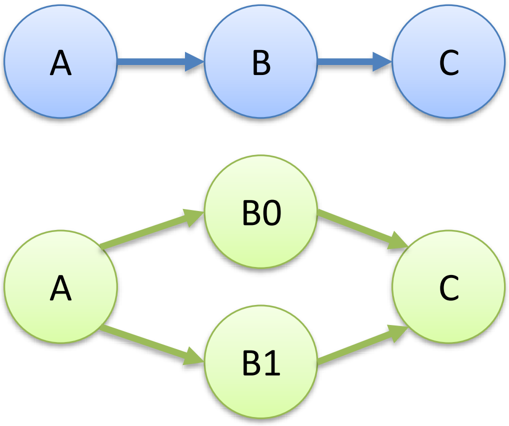
MDC Contexts of application

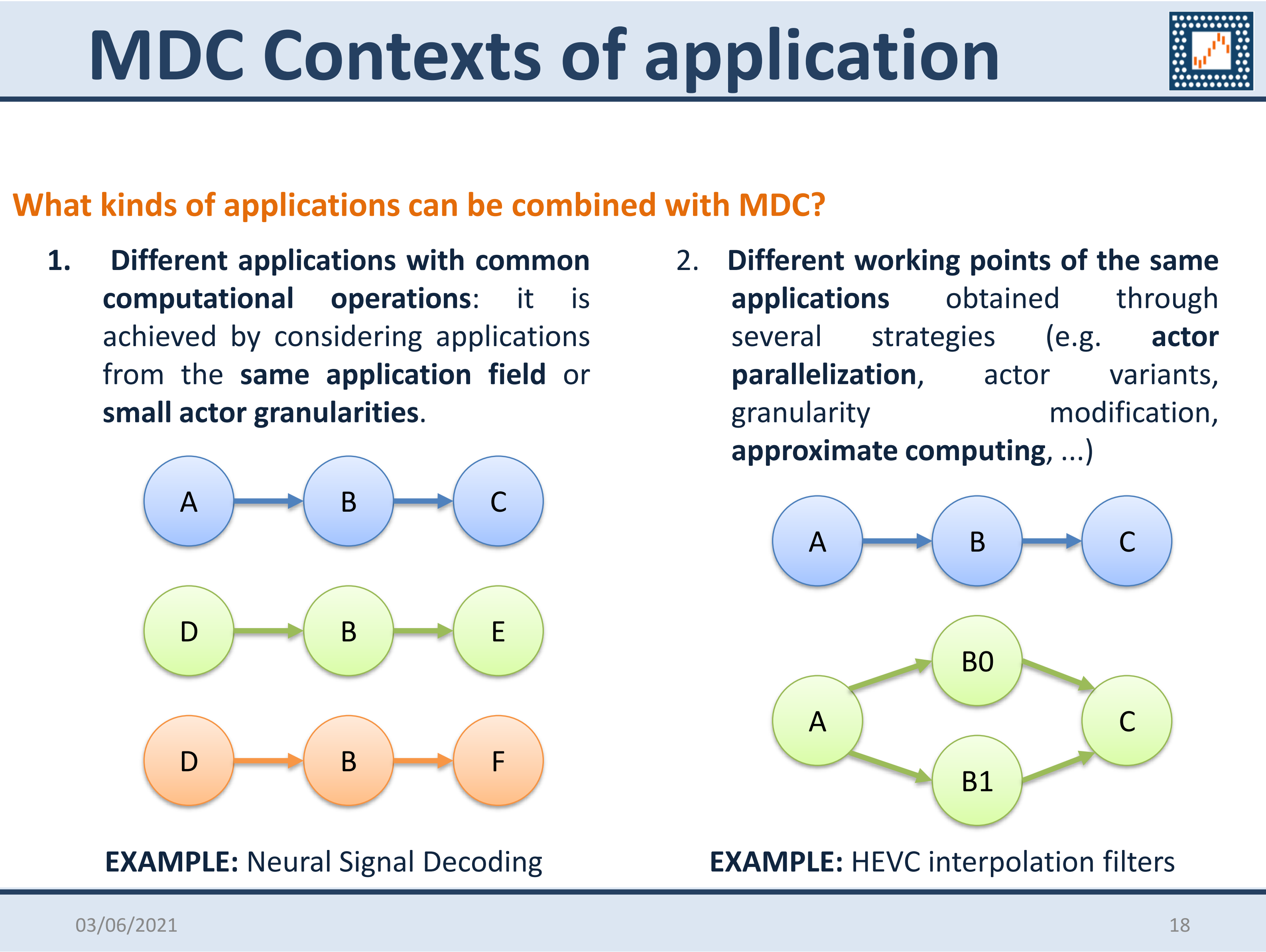
What kinds of applications can be combined with MDC?

1. **Different applications with common computational operations**: it is achieved by considering applications from the **same application field** or **small actor granularities**.



2. **Different working points of the same applications** obtained through several strategies (e.g. **actor parallelization**, actor variants, granularity modification, **approximate computing**, ...)





MDC Contexts of application

What kinds of applications can be combined with MDC?

1. **Different applications with common computational operations**: it is achieved by considering applications from the **same application field** or **small actor granularities**.

EXAMPLE: Neural Signal Decoding

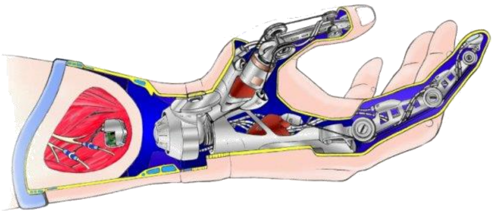
2. **Different working points of the same applications** obtained through several strategies (e.g. **actor parallelization**, actor variants, granularity modification, **approximate computing**, ...)

EXAMPLE: HEVC interpolation filters

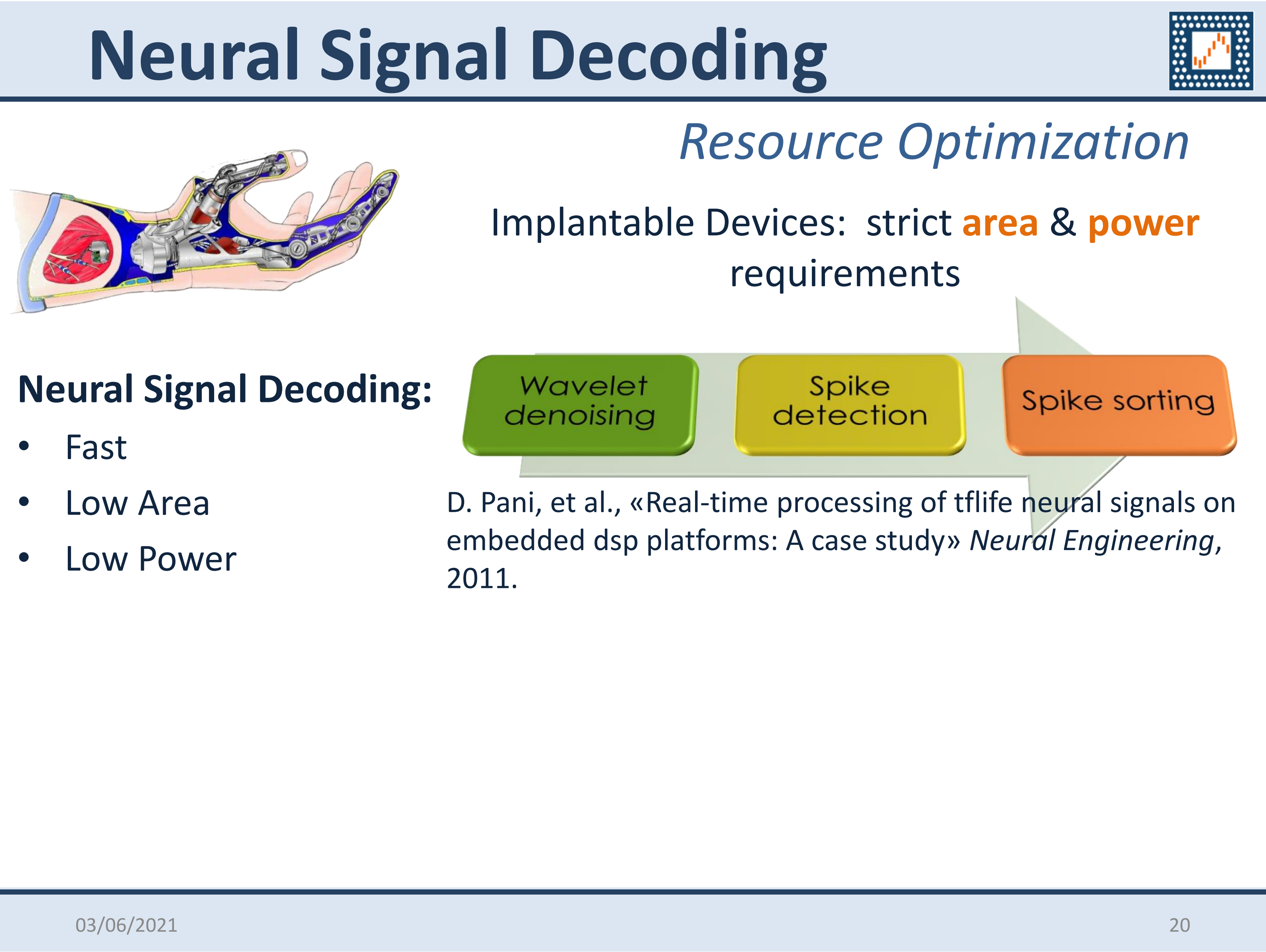
03/06/2021 18

Neural Signal Decoding

Resource Optimization



Implantable Devices: strict **area** & **power** requirements



Neural Signal Decoding

Resource Optimization

Implantable Devices: strict **area** & **power** requirements

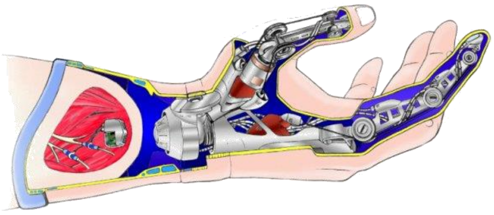
Wavelet denoising
Spike detection
Spike sorting

Neural Signal Decoding:

- Fast
- Low Area
- Low Power

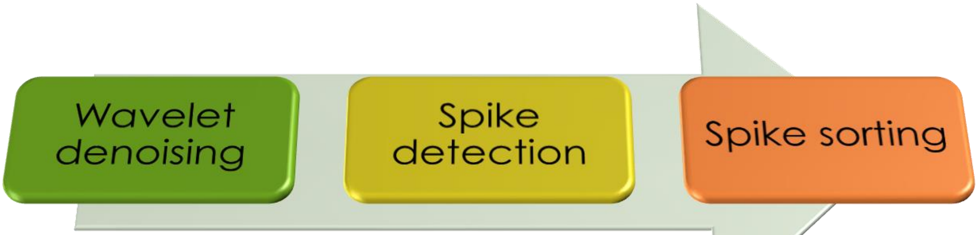
D. Pani, et al., «Real-time processing of tflife neural signals on embedded dsp platforms: A case study» *Neural Engineering*, 2011.

Neural Signal Decoding



Resource Optimization

Implantable Devices: strict **area** & **power** requirements



Wavelet denoising

Spike detection

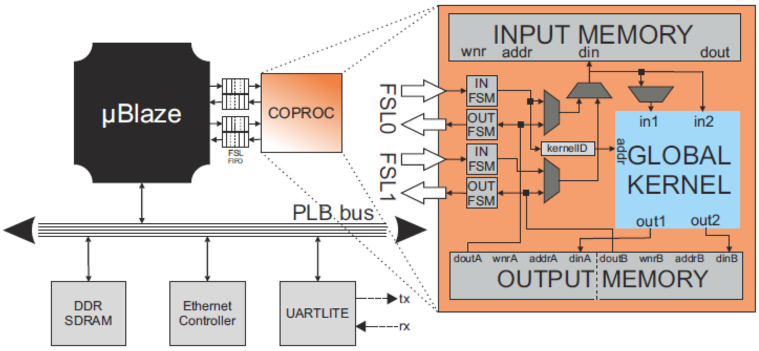
Spike sorting

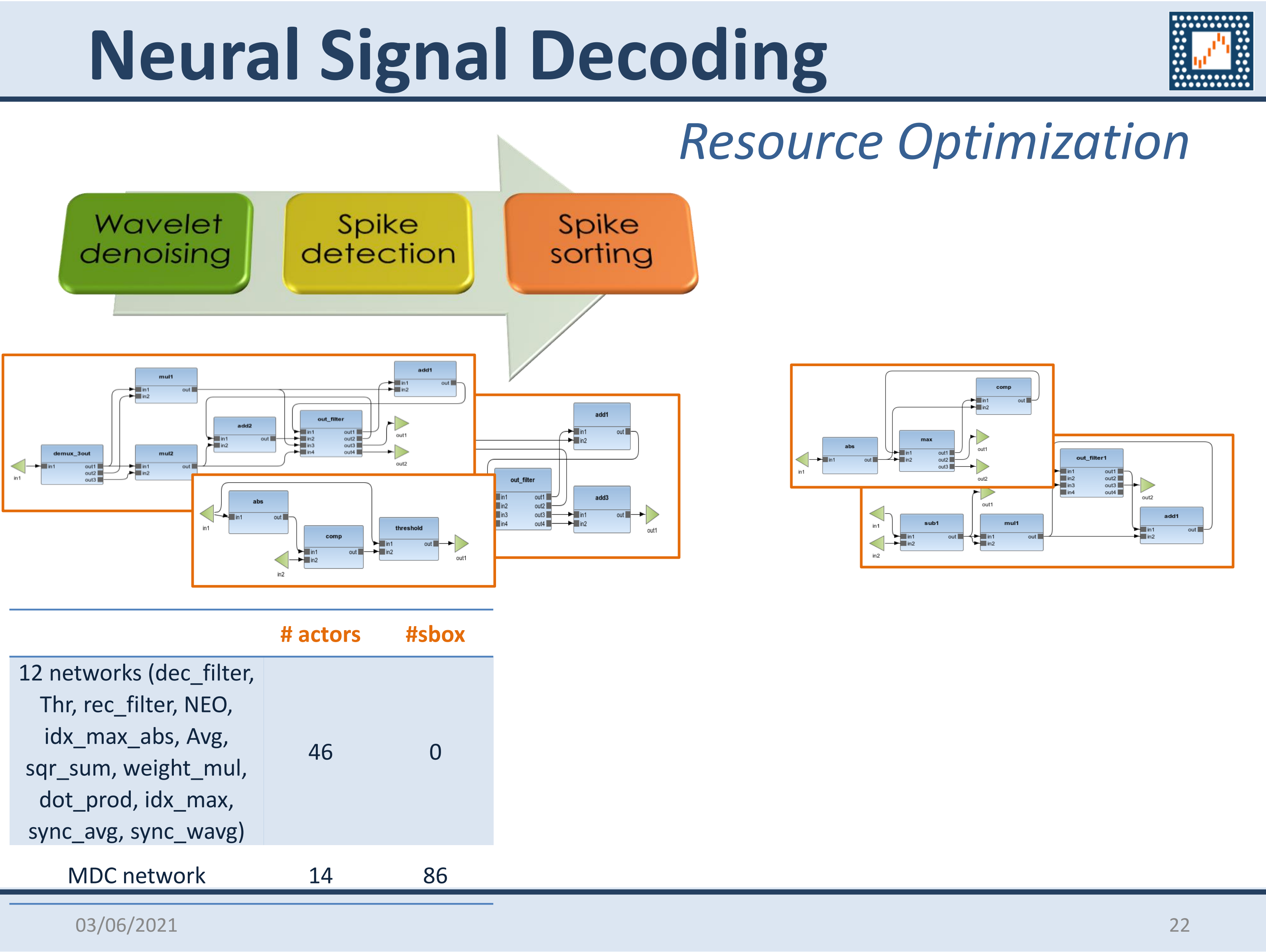
Neural Signal Decoding:

- Fast
- Low Area
- Low Power

D. Pani, et al., «Real-time processing of tflife neural signals on embedded dsp platforms: A case study» *Neural Engineering*, 2011.

MDC can be used to build the accelerators compliant to those constraints.





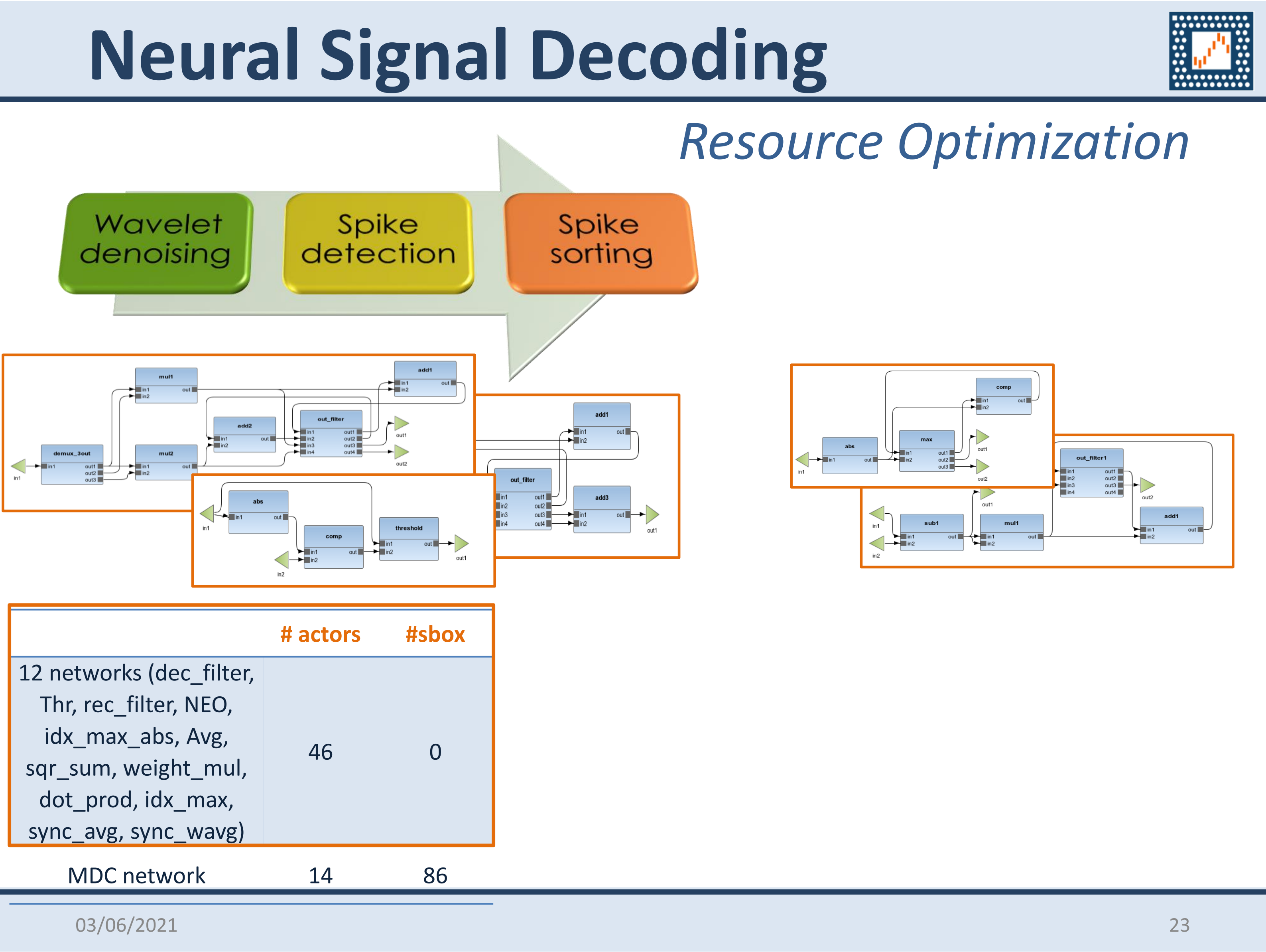
Neural Signal Decoding

Resource Optimization

	# actors	#sbox
12 networks (dec_filter, Thr, rec_filter, NEO, idx_max_abs, Avg, sqr_sum, weight_mul, dot_prod, idx_max, sync_avg, sync_wavg)	46	0
MDC network	14	86

03/06/2021

22



Neural Signal Decoding

Resource Optimization

Wavelet denoising

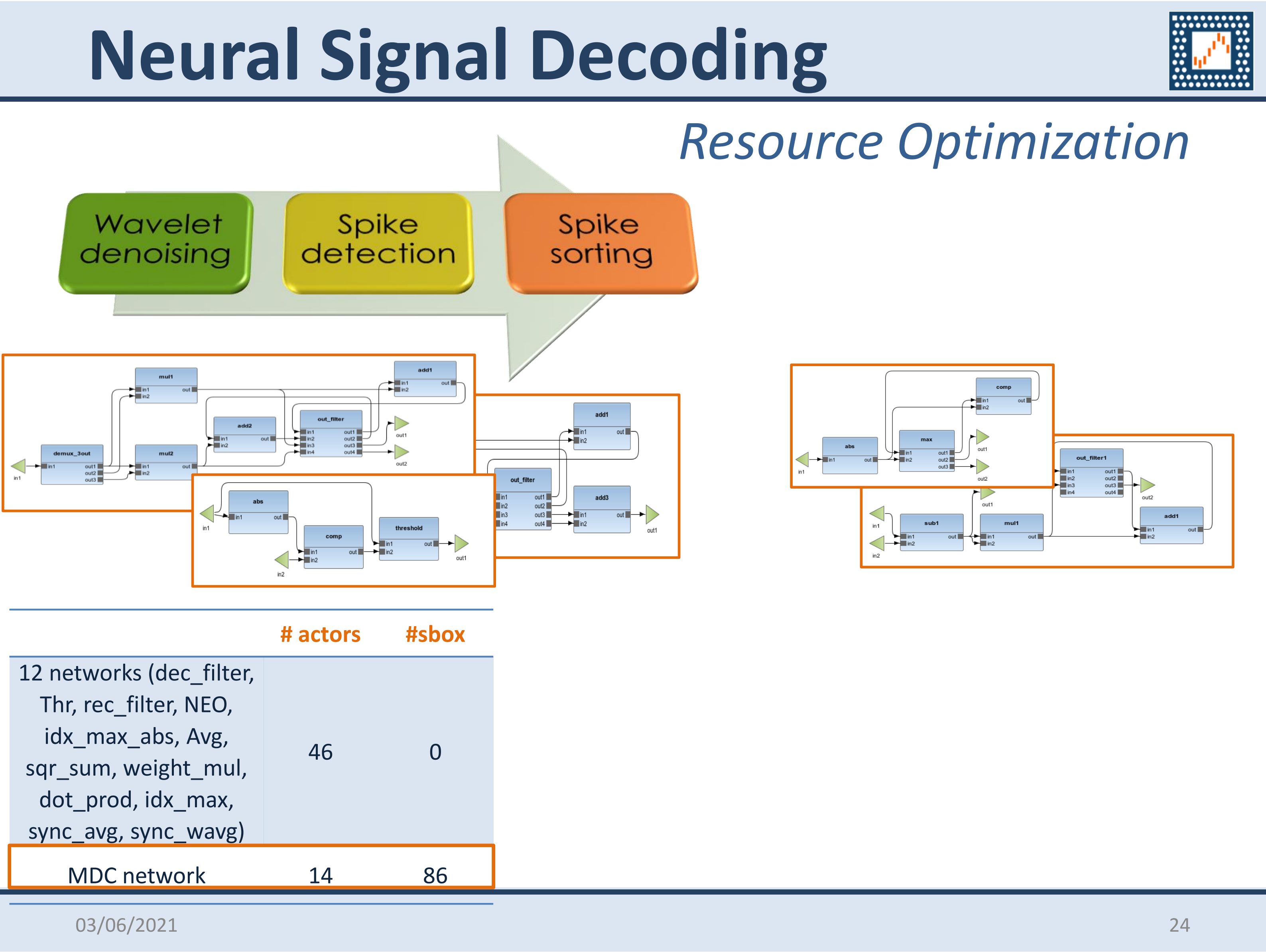
Spike detection

Spike sorting

	# actors	#sbox
12 networks (dec_filter, Thr, rec_filter, NEO, idx_max_abs, Avg, sqr_sum, weight_mul, dot_prod, idx_max, sync_avg, sync_wavg)	46	0
MDC network	14	86

03/06/2021

23



Neural Signal Decoding

Resource Optimization

Wavelet denoising

Spike detection

Spike sorting

	# actors	#sbox
12 networks (dec_filter, Thr, rec_filter, NEO, idx_max_abs, Avg, sqr_sum, weight_mul, dot_prod, idx_max, sync_avg, sync_wavg)	46	0
MDC network	14	86

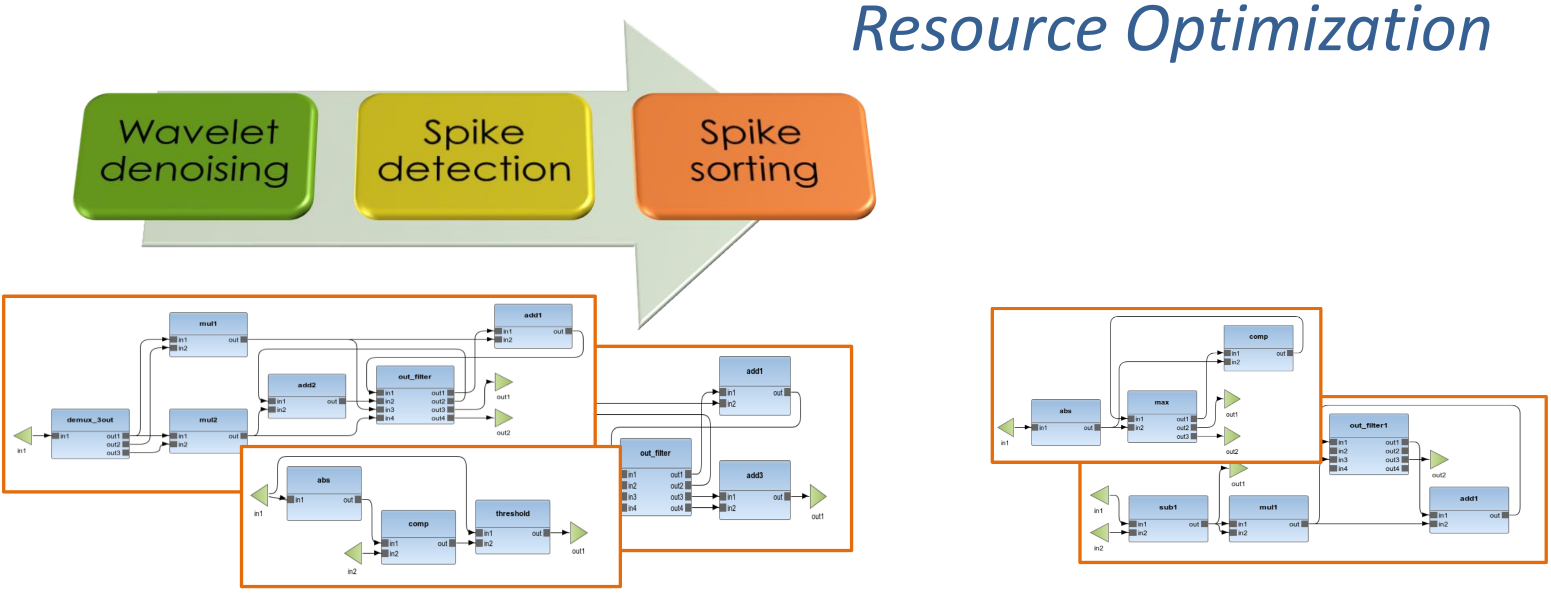
03/06/2021

24

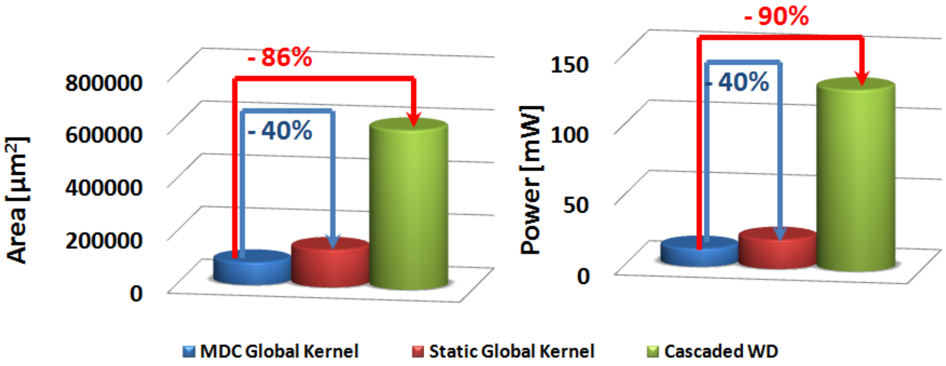
©MECO.net

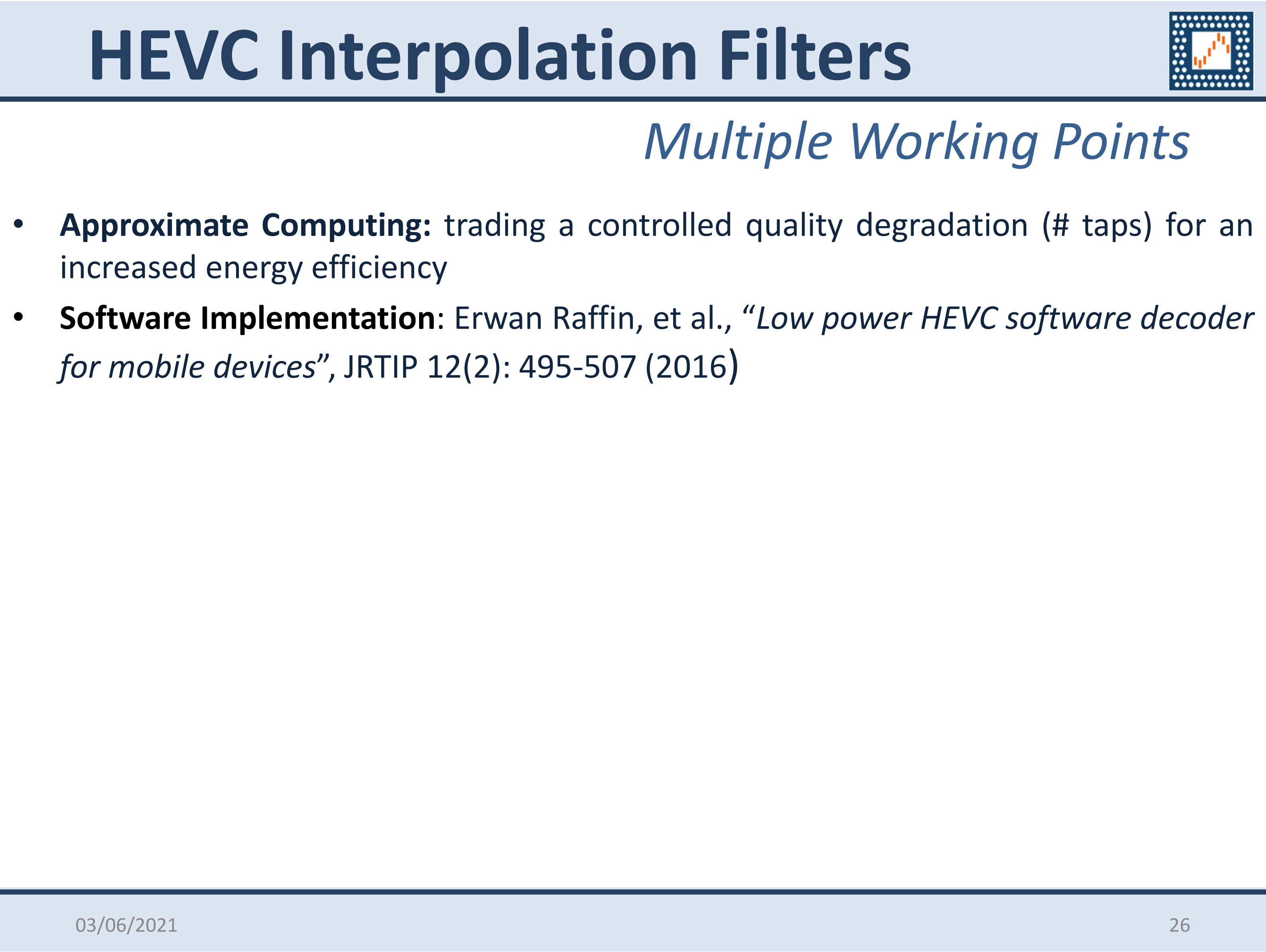
Neural Signal Decoding

Resource Optimization



	# actors	#sbox
12 networks (dec_filter, Thr, rec_filter, NEO, idx_max_abs, Avg, sqr_sum, weight_mul, dot_prod, idx_max, sync_avg, sync_wavg)	46	0
MDC network	14	86





HEVC Interpolation Filters

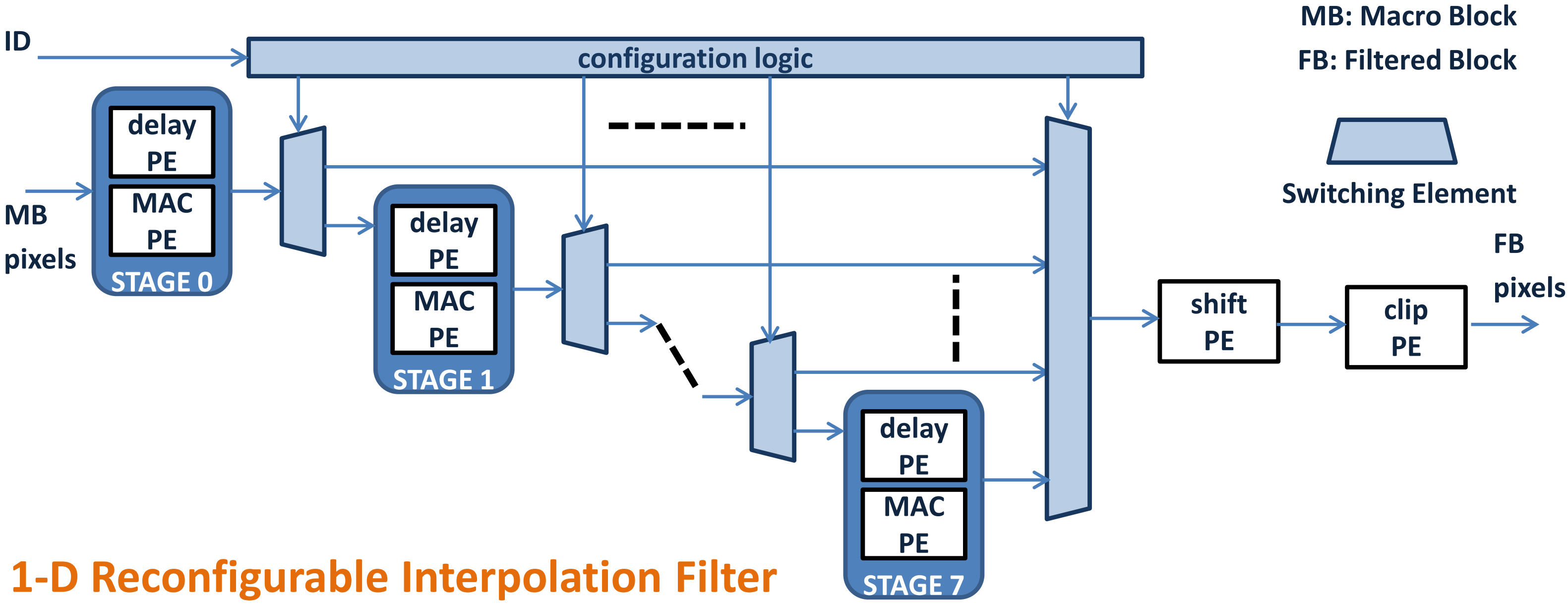
Multiple Working Points

- **Approximate Computing:** trading a controlled quality degradation (# taps) for an increased energy efficiency
- **Software Implementation**: Erwan Raffin, et al., "*Low power HEVC software decoder for mobile devices*", JRTIP 12(2): 495-507 (2016)

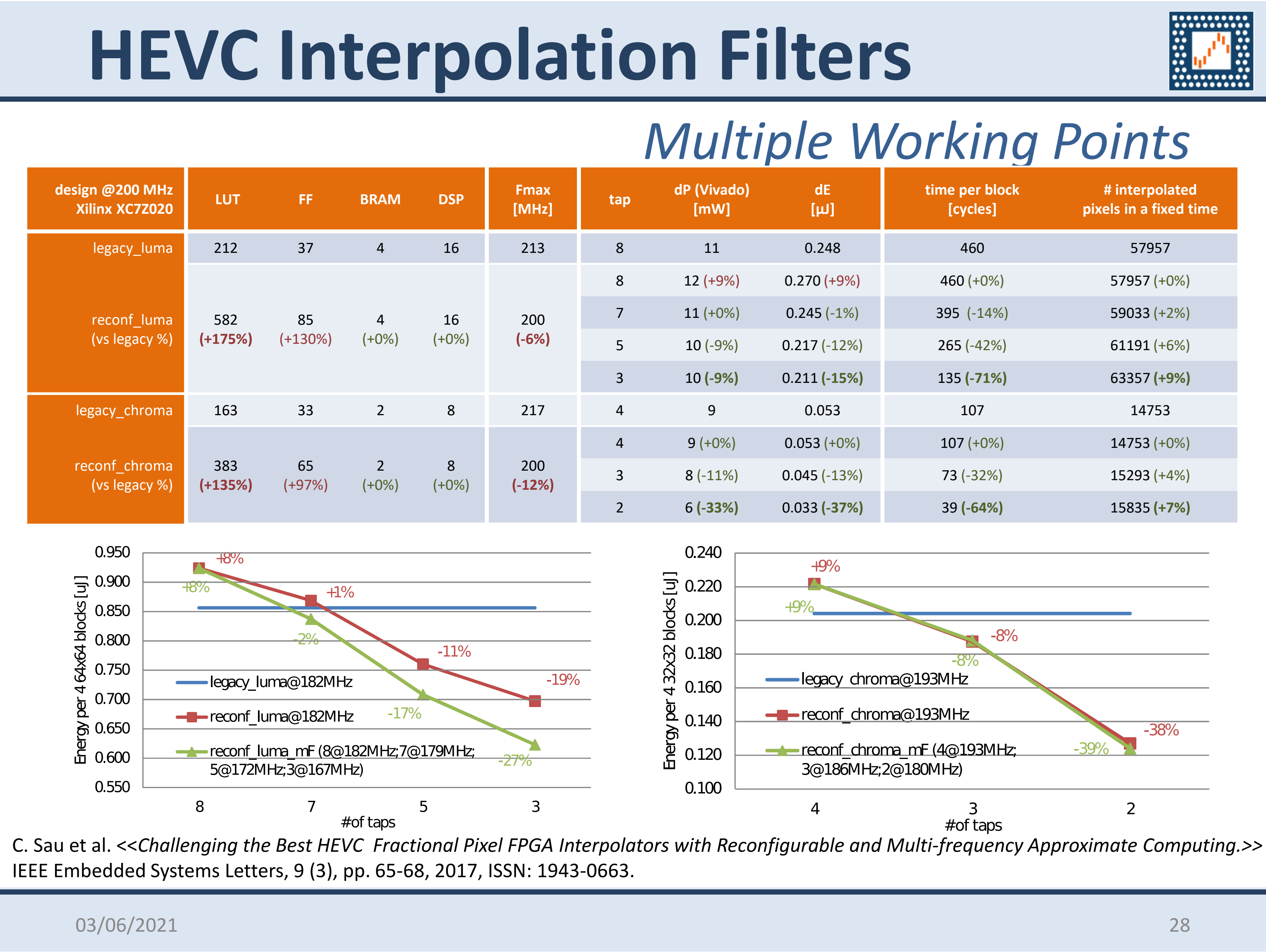
HEVC Interpolation Filters

Multiple Working Points

- **Approximate Computing:** trading a controlled quality degradation (# taps) for an increased energy efficiency
- **Software Implementation**: Erwan Raffin, et al., "*Low power HEVC software decoder for mobile devices*", JRTIP 12(2): 495-507 (2016)



1-D Reconfigurable Interpolation Filter



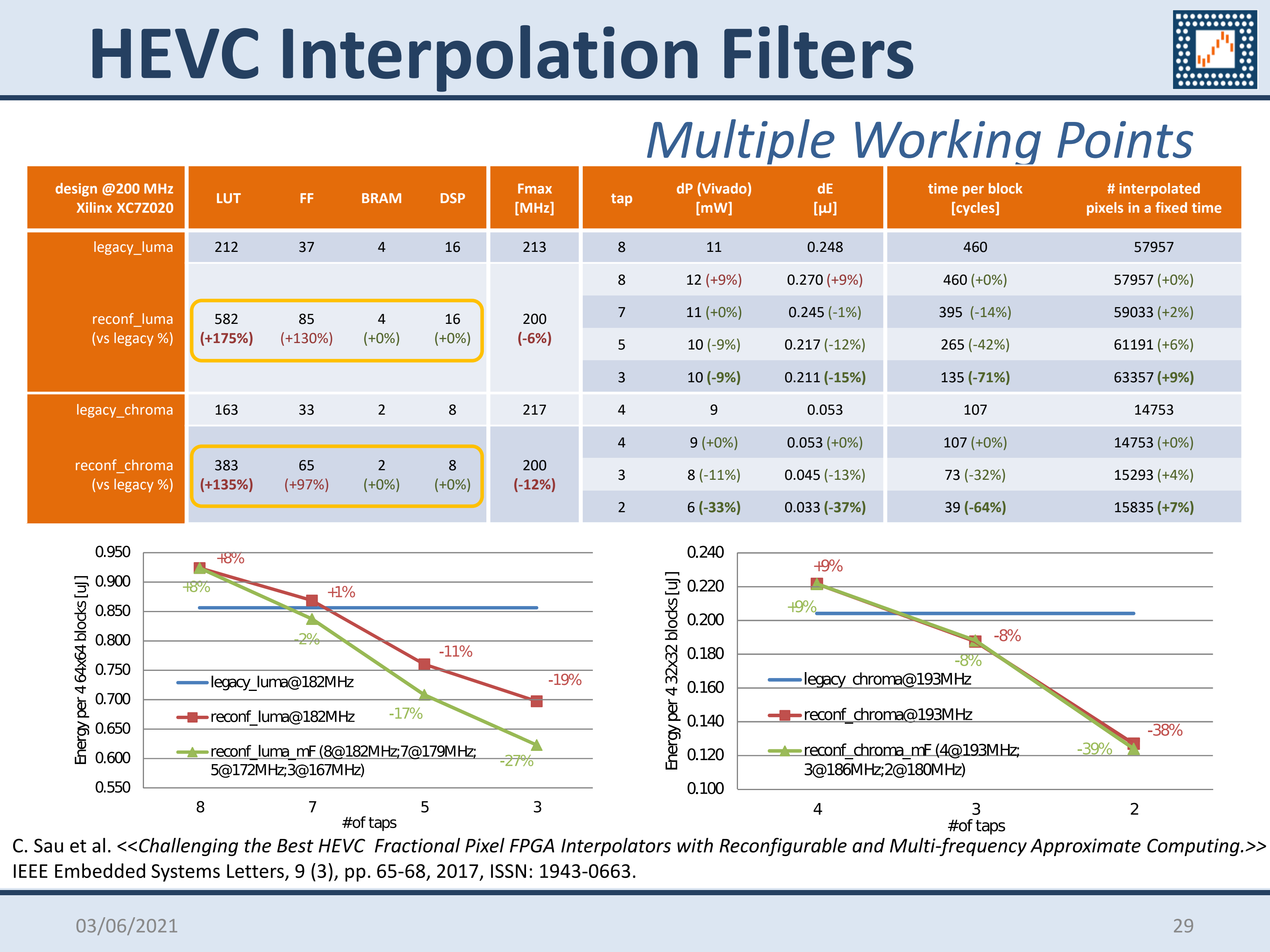
HEVC Interpolation Filters

Multiple Working Points

design @200 MHz Xilinx XC7Z020	LUT	FF	BRAM	DSP	Fmax [MHz]	tap	dP (Vivado) [mW]	dE [μJ]	time per block [cycles]	# interpolated pixels in a fixed time
legacy_luma	212	37	4	16	213	8	11	0.248	460	57957
reconf_luma (vs legacy %)	582 **(+175%)**	85 (+130%)	4 (+0%)	16 (+0%)	200 **(-6%)**	8	12 (+9%)	0.270 (+9%)	460 (+0%)	57957 (+0%)
						7	11 (+0%)	0.245 (-1%)	395 (-14%)	59033 (+2%)
						5	10 (-9%)	0.217 (-12%)	265 (-42%)	61191 (+6%)
						3	10 **(-9%)**	0.211 **(-15%)**	135 **(-71%)**	63357 **(+9%)**
legacy_chroma	163	33	2	8	217	4	9	0.053	107	14753
reconf_chroma (vs legacy %)	383 **(+135%)**	65 (+97%)	2 (+0%)	8 (+0%)	200 **(-12%)**	4	9 (+0%)	0.053 (+0%)	107 (+0%)	14753 (+0%)
						3	8 (-11%)	0.045 (-13%)	73 (-32%)	15293 (+4%)
						2	6 **(-33%)**	0.033 **(-37%)**	39 **(-64%)**	15835 **(+7%)**

C. Sau et al. <<*Challenging the Best HEVC Fractional Pixel FPGA Interpolators with Reconfigurable and Multi-frequency Approximate Computing.*>> IEEE Embedded Systems Letters, 9 (3), pp. 65-68, 2017, ISSN: 1943-0663.

03/06/2021 28



HEVC Interpolation Filters

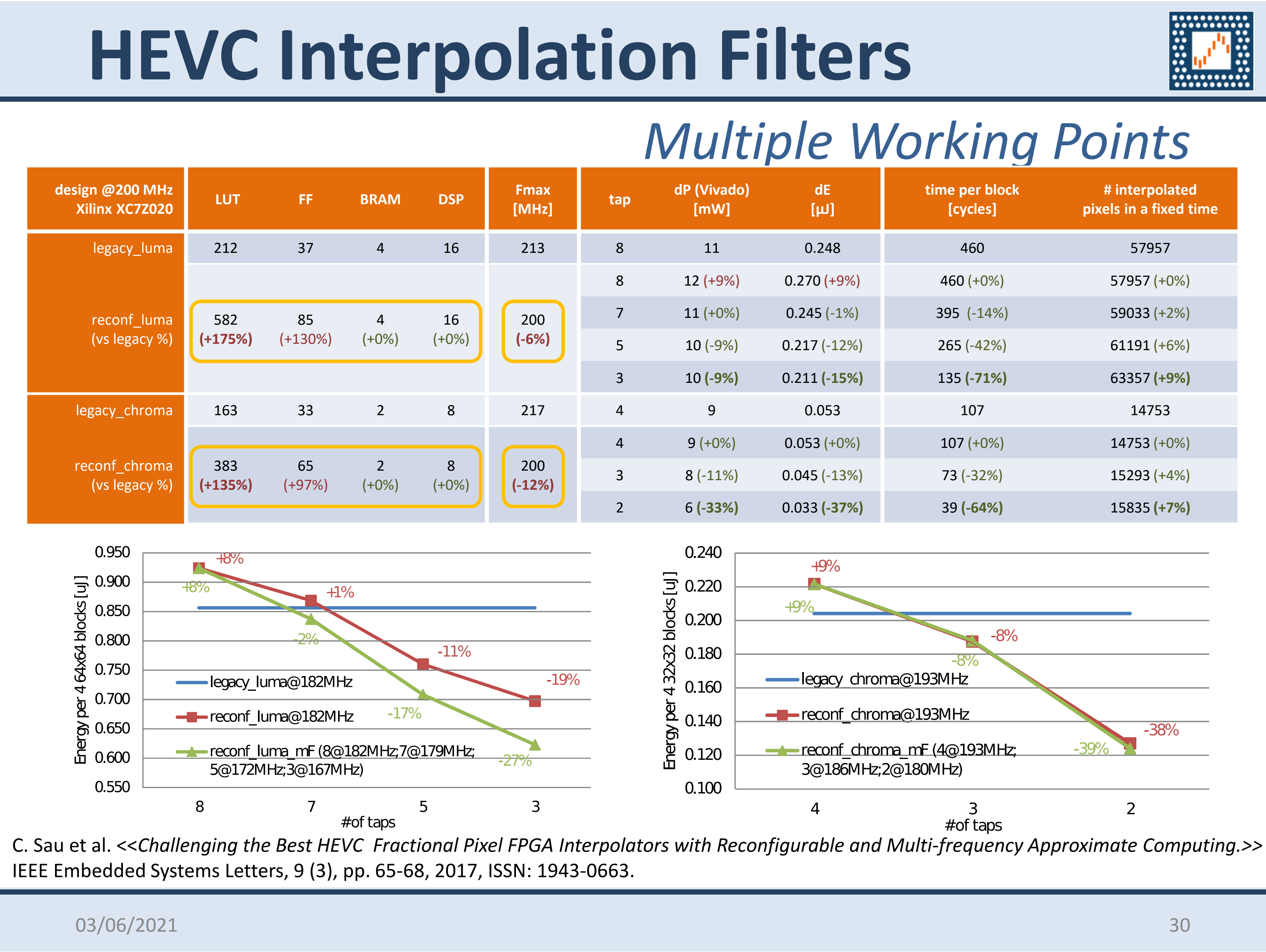
Multiple Working Points

design @200 MHz Xilinx XC7Z020	LUT	FF	BRAM	DSP	Fmax [MHz]	tap	dP (Vivado) [mW]	dE [μJ]	time per block [cycles]	# interpolated pixels in a fixed time
legacy_luma	212	37	4	16	213	8	11	0.248	460	57957
reconf_luma (vs legacy %)	582 **(+175%)**	85 (+130%)	4 (+0%)	16 (+0%)	200 **(-6%)**	8	12 (+9%)	0.270 (+9%)	460 (+0%)	57957 (+0%)
						7	11 (+0%)	0.245 (-1%)	395 (-14%)	59033 (+2%)
						5	10 (-9%)	0.217 (-12%)	265 (-42%)	61191 (+6%)
						3	10 **(-9%)**	0.211 **(-15%)**	135 **(-71%)**	63357 **(+9%)**
legacy_chroma	163	33	2	8	217	4	9	0.053	107	14753
reconf_chroma (vs legacy %)	383 **(+135%)**	65 (+97%)	2 (+0%)	8 (+0%)	200 **(-12%)**	4	9 (+0%)	0.053 (+0%)	107 (+0%)	14753 (+0%)
						3	8 (-11%)	0.045 (-13%)	73 (-32%)	15293 (+4%)
						2	6 **(-33%)**	0.033 **(-37%)**	39 **(-64%)**	15835 **(+7%)**

C. Sau et al. <<*Challenging the Best HEVC Fractional Pixel FPGA Interpolators with Reconfigurable and Multi-frequency Approximate Computing.*>> IEEE Embedded Systems Letters, 9 (3), pp. 65-68, 2017, ISSN: 1943-0663.

03/06/2021

29



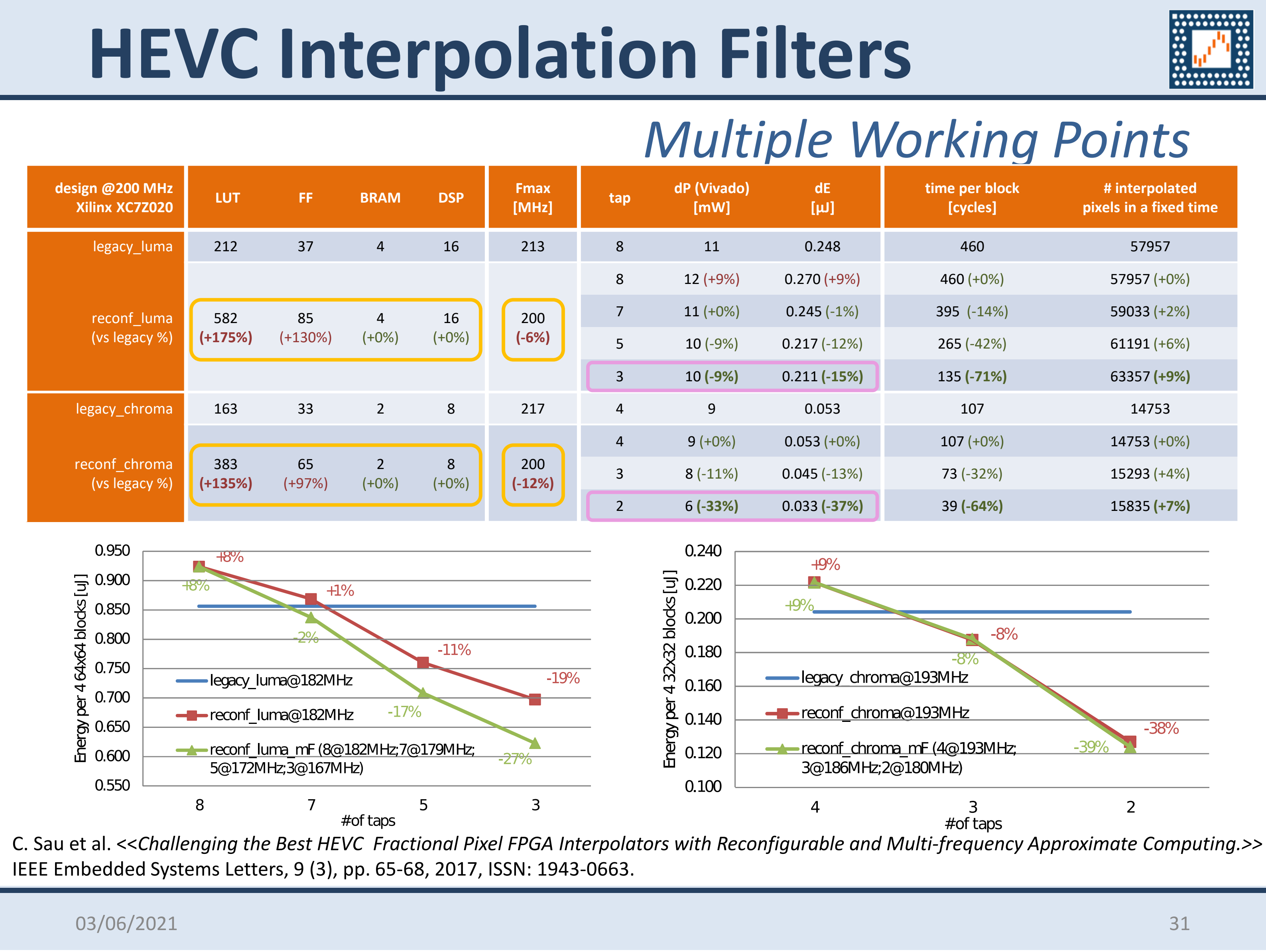
HEVC Interpolation Filters

Multiple Working Points

design @200 MHz Xilinx XC7Z020	LUT	FF	BRAM	DSP	Fmax [MHz]	tap	dP (Vivado) [mW]	dE [µJ]	time per block [cycles]	# interpolated pixels in a fixed time
legacy_luma	212	37	4	16	213	8	11	0.248	460	57957
reconf_luma (vs legacy %)	582 **(+175%)**	85 (+130%)	4 (+0%)	16 (+0%)	200 **(-6%)**	8	12 (+9%)	0.270 (+9%)	460 (+0%)	57957 (+0%)
						7	11 (+0%)	0.245 (-1%)	395 (-14%)	59033 (+2%)
						5	10 (-9%)	0.217 (-12%)	265 (-42%)	61191 (+6%)
						3	10 **(-9%)**	0.211 **(-15%)**	135 **(-71%)**	63357 **(+9%)**
legacy_chroma	163	33	2	8	217	4	9	0.053	107	14753
reconf_chroma (vs legacy %)	383 **(+135%)**	65 (+97%)	2 (+0%)	8 (+0%)	200 **(-12%)**	4	9 (+0%)	0.053 (+0%)	107 (+0%)	14753 (+0%)
						3	8 (-11%)	0.045 (-13%)	73 (-32%)	15293 (+4%)
						2	6 **(-33%)**	0.033 **(-37%)**	39 **(-64%)**	15835 **(+7%)**

C. Sau et al. <<*Challenging the Best HEVC Fractional Pixel FPGA Interpolators with Reconfigurable and Multi-frequency Approximate Computing.*>> IEEE Embedded Systems Letters, 9 (3), pp. 65-68, 2017, ISSN: 1943-0663.

03/06/2021 30

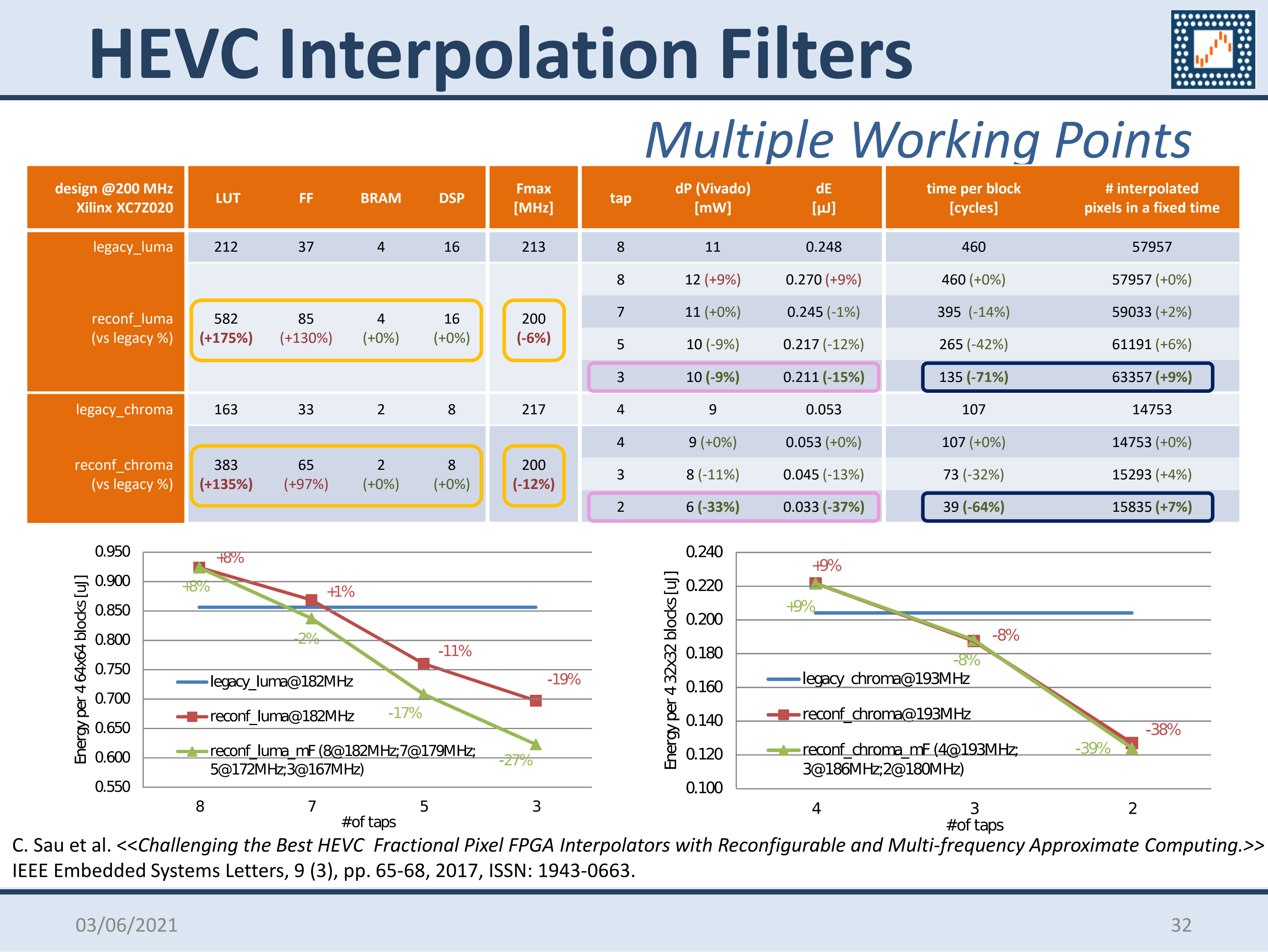


HEVC Interpolation Filters

Multiple Working Points

design @200 MHz Xilinx XC7Z020	LUT	FF	BRAM	DSP	Fmax [MHz]	tap	dP (Vivado) [mW]	dE [µJ]	time per block [cycles]	# interpolated pixels in a fixed time
legacy_luma	212	37	4	16	213	8	11	0.248	460	57957
reconf_luma (vs legacy %)	582 **(+175%)**	85 (+130%)	4 (+0%)	16 (+0%)	200 **(-6%)**	8	12 (+9%)	0.270 (+9%)	460 (+0%)	57957 (+0%)
						7	11 (+0%)	0.245 (-1%)	395 (-14%)	59033 (+2%)
						5	10 (-9%)	0.217 (-12%)	265 (-42%)	61191 (+6%)
						3	10 **(-9%)**	0.211 **(-15%)**	135 **(-71%)**	63357 **(+9%)**
legacy_chroma	163	33	2	8	217	4	9	0.053	107	14753
reconf_chroma (vs legacy %)	383 **(+135%)**	65 (+97%)	2 (+0%)	8 (+0%)	200 **(-12%)**	4	9 (+0%)	0.053 (+0%)	107 (+0%)	14753 (+0%)
						3	8 (-11%)	0.045 (-13%)	73 (-32%)	15293 (+4%)
						2	6 **(-33%)**	0.033 **(-37%)**	39 **(-64%)**	15835 **(+7%)**

C. Sau et al. <<*Challenging the Best HEVC Fractional Pixel FPGA Interpolators with Reconfigurable and Multi-frequency Approximate Computing.*>> IEEE Embedded Systems Letters, 9 (3), pp. 65-68, 2017, ISSN: 1943-0663.



HEVC Interpolation Filters

Multiple Working Points

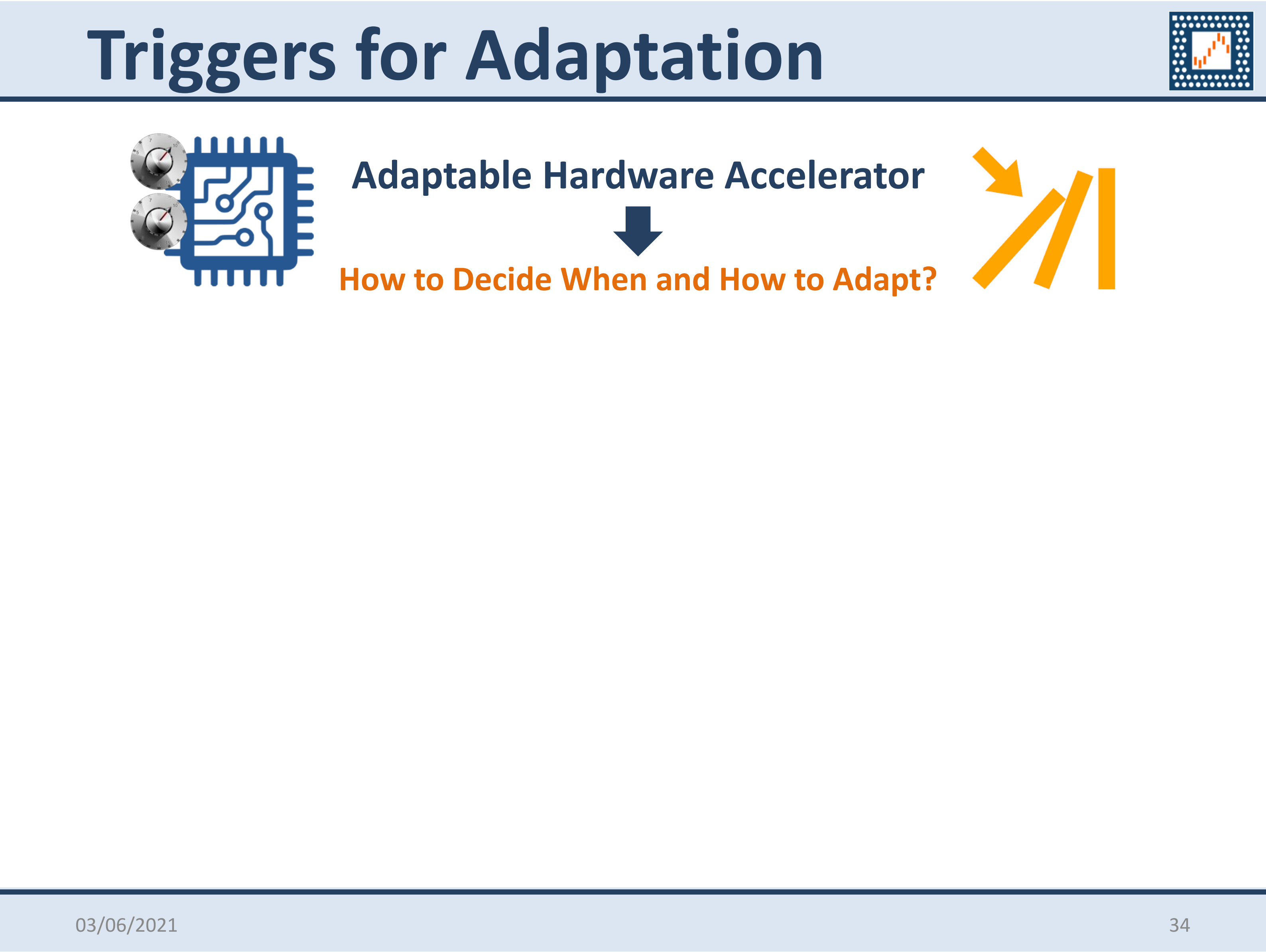
design @200 MHz Xilinx XC7Z020	LUT	FF	BRAM	DSP	Fmax [MHz]	tap	dP (Vivado) [mW]	dE [µJ]	time per block [cycles]	# interpolated pixels in a fixed time
legacy_luma	212	37	4	16	213	8	11	0.248	460	57957
reconf_luma (vs legacy %)	582 (+175%)	85 (+130%)	4 (+0%)	16 (+0%)	200 (-6%)	8	12 (+9%)	0.270 (+9%)	460 (+0%)	57957 (+0%)
						7	11 (+0%)	0.245 (-1%)	395 (-14%)	59033 (+2%)
						5	10 (-9%)	0.217 (-12%)	265 (-42%)	61191 (+6%)
						3	10 **(-9%)**	0.211 **(-15%)**	135 **(-71%)**	63357 **(+9%)**
legacy_chroma	163	33	2	8	217	4	9	0.053	107	14753
reconf_chroma (vs legacy %)	383 (+135%)	65 (+97%)	2 (+0%)	8 (+0%)	200 (-12%)	4	9 (+0%)	0.053 (+0%)	107 (+0%)	14753 (+0%)
						3	8 (-11%)	0.045 (-13%)	73 (-32%)	15293 (+4%)
						2	6 **(-33%)**	0.033 **(-37%)**	39 **(-64%)**	15835 **(+7%)**

C. Sau et al. <<*Challenging the Best HEVC Fractional Pixel FPGA Interpolators with Reconfigurable and Multi-frequency Approximate Computing.*>> IEEE Embedded Systems Letters, 9 (3), pp. 65-68, 2017, ISSN: 1943-0663.

03/06/2021 32

CPS&IoT'2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

Triggers for Adaptation



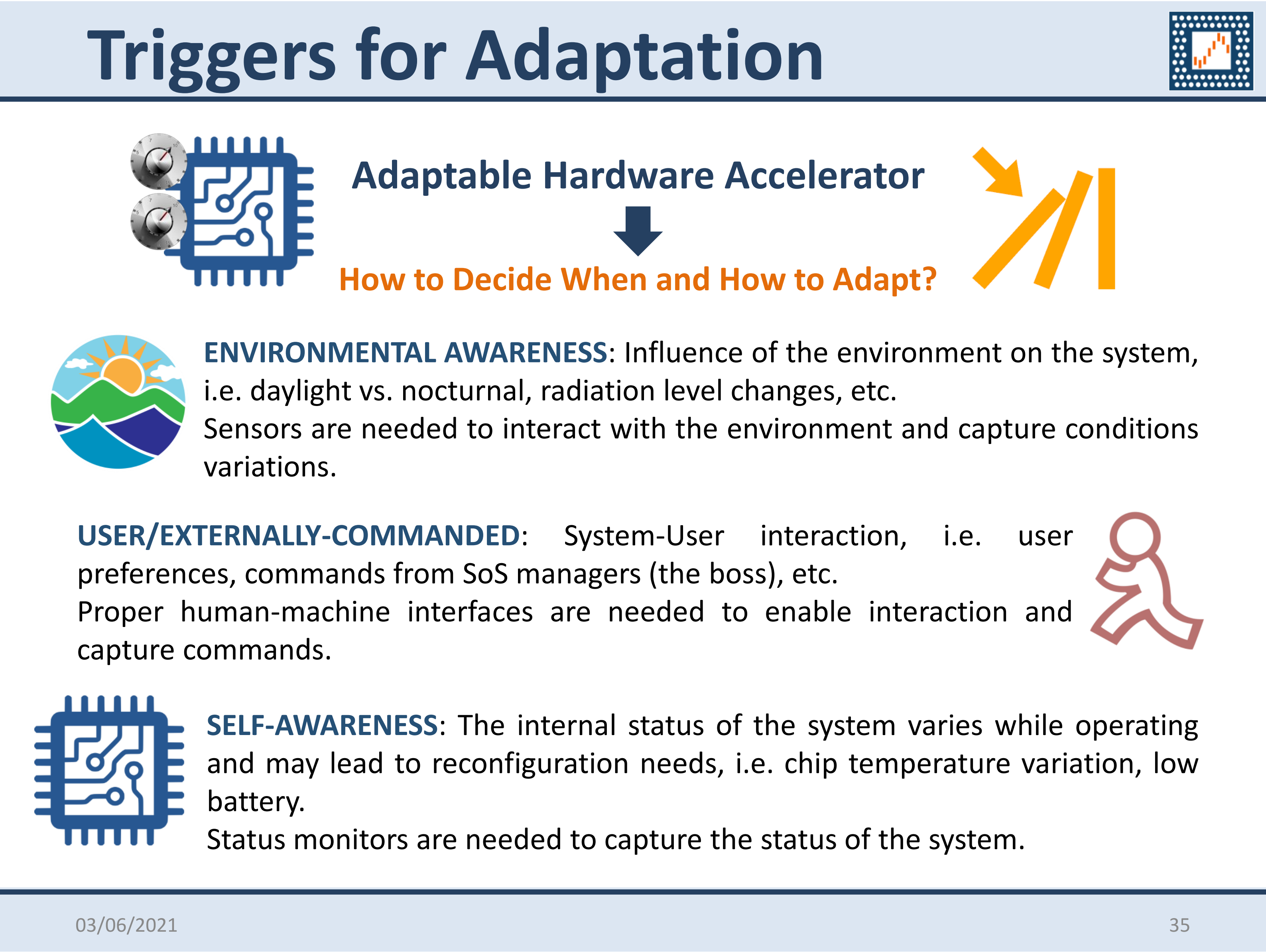
Triggers for Adaptation

Adaptable Hardware Accelerator

How to Decide When and How to Adapt?

03/06/2021

34



Triggers for Adaptation

Adaptable Hardware Accelerator

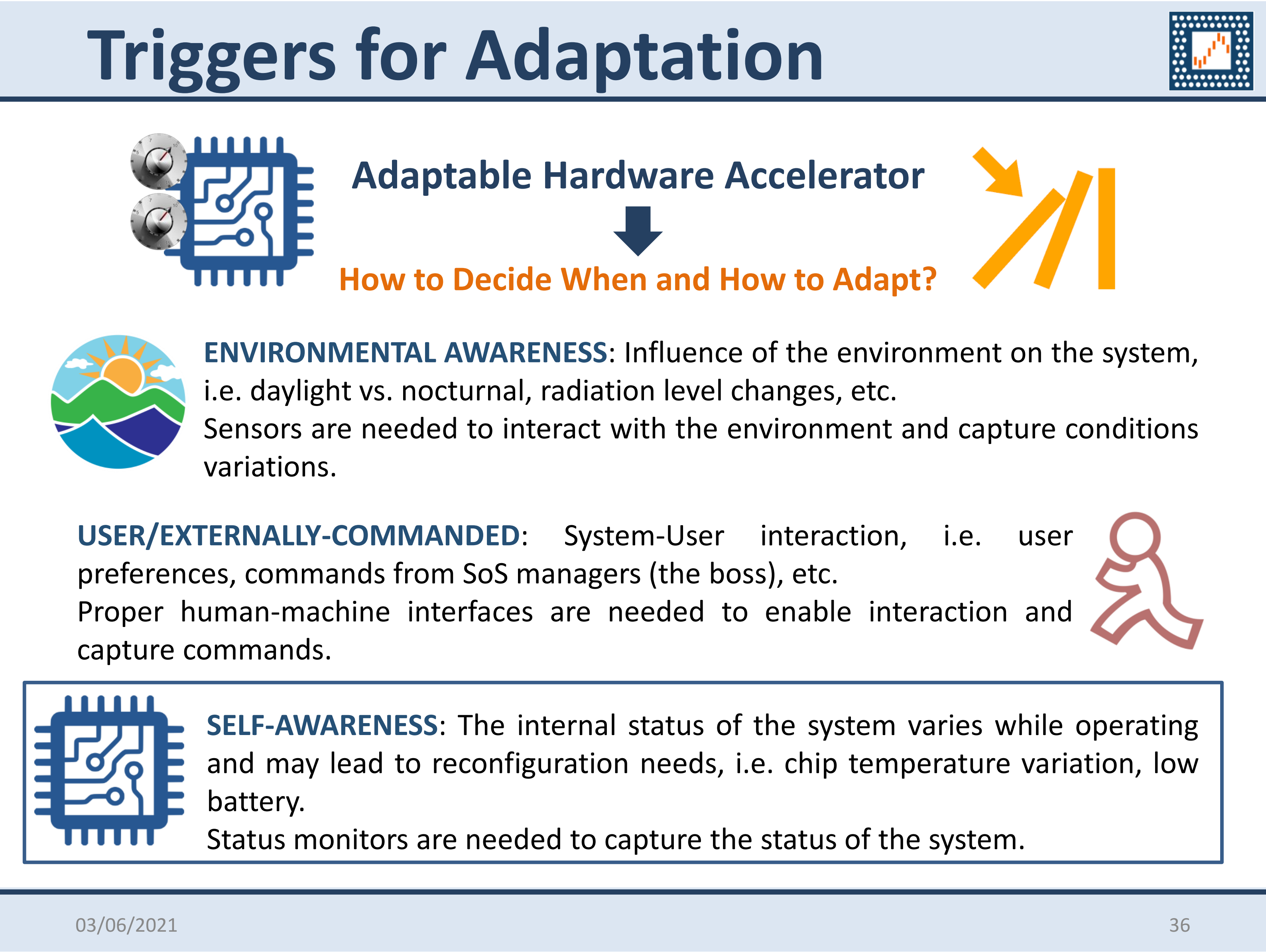
How to Decide When and How to Adapt?

ENVIRONMENTAL AWARENESS: Influence of the environment on the system, i.e. daylight vs. nocturnal, radiation level changes, etc.
Sensors are needed to interact with the environment and capture conditions variations.

USER/EXTERNALLY-COMMANDED: System-User interaction, i.e. user preferences, commands from SoS managers (the boss), etc.
Proper human-machine interfaces are needed to enable interaction and capture commands.

SELF-AWARENESS: The internal status of the system varies while operating and may lead to reconfiguration needs, i.e. chip temperature variation, low battery.
Status monitors are needed to capture the status of the system.

03/06/2021 35



Triggers for Adaptation

Adaptable Hardware Accelerator

How to Decide When and How to Adapt?

ENVIRONMENTAL AWARENESS: Influence of the environment on the system, i.e. daylight vs. nocturnal, radiation level changes, etc.
Sensors are needed to interact with the environment and capture conditions variations.

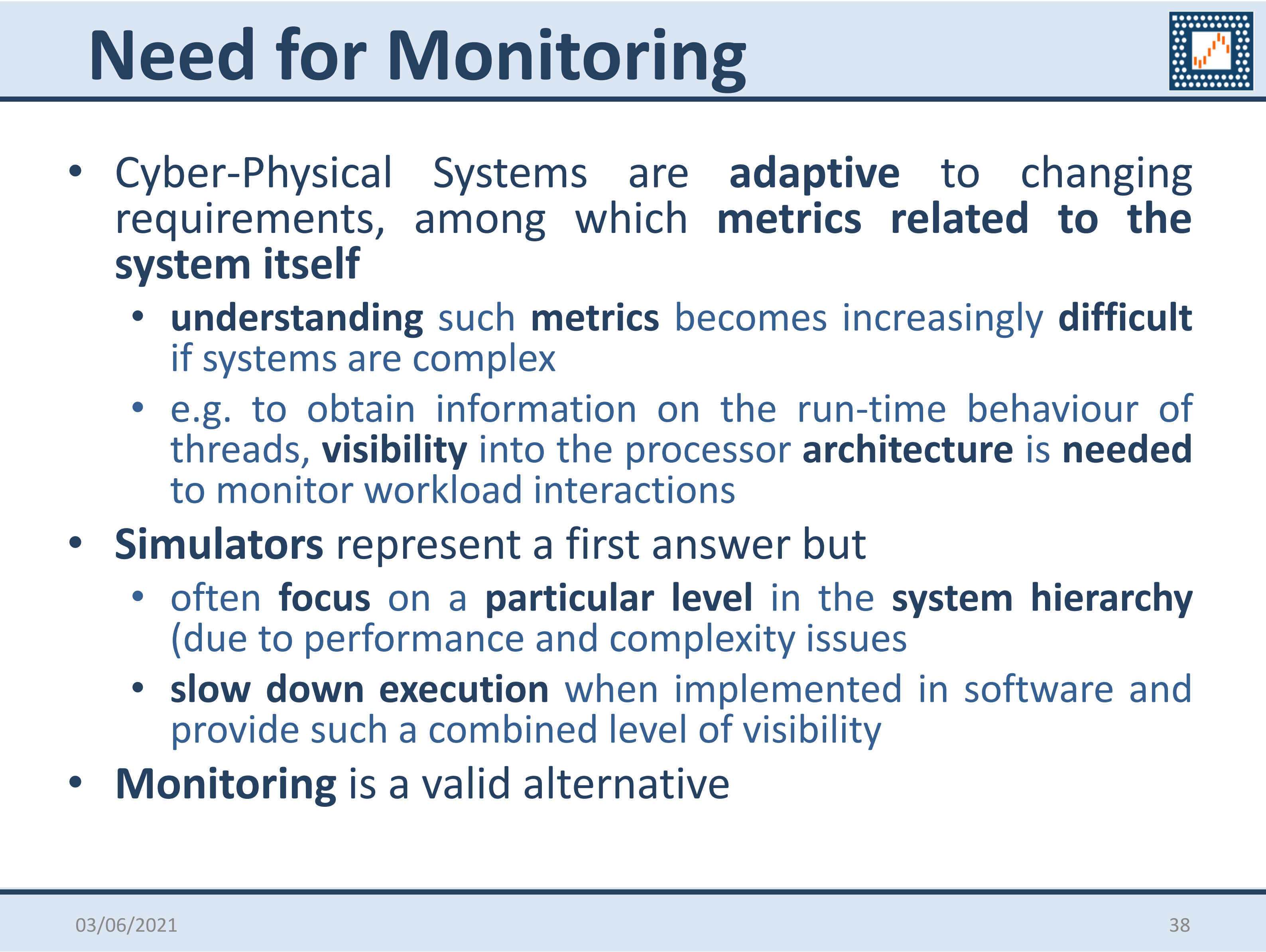
USER/EXTERNALLY-COMMANDED: System-User interaction, i.e. user preferences, commands from SoS managers (the boss), etc.
Proper human-machine interfaces are needed to enable interaction and capture commands.

SELF-AWARENESS: The internal status of the system varies while operating and may lead to reconfiguration needs, i.e. chip temperature variation, low battery.
Status monitors are needed to capture the status of the system.

03/06/2021 36

Need for Monitoring

- Cyber-Physical Systems are **adaptive** to changing requirements, among which **metrics related to the system itself**
  - **understanding** such **metrics** becomes increasingly **difficult** if systems are complex
  - e.g. to obtain information on the run-time behaviour of threads, **visibility** into the processor **architecture** is **needed** to monitor workload interactions

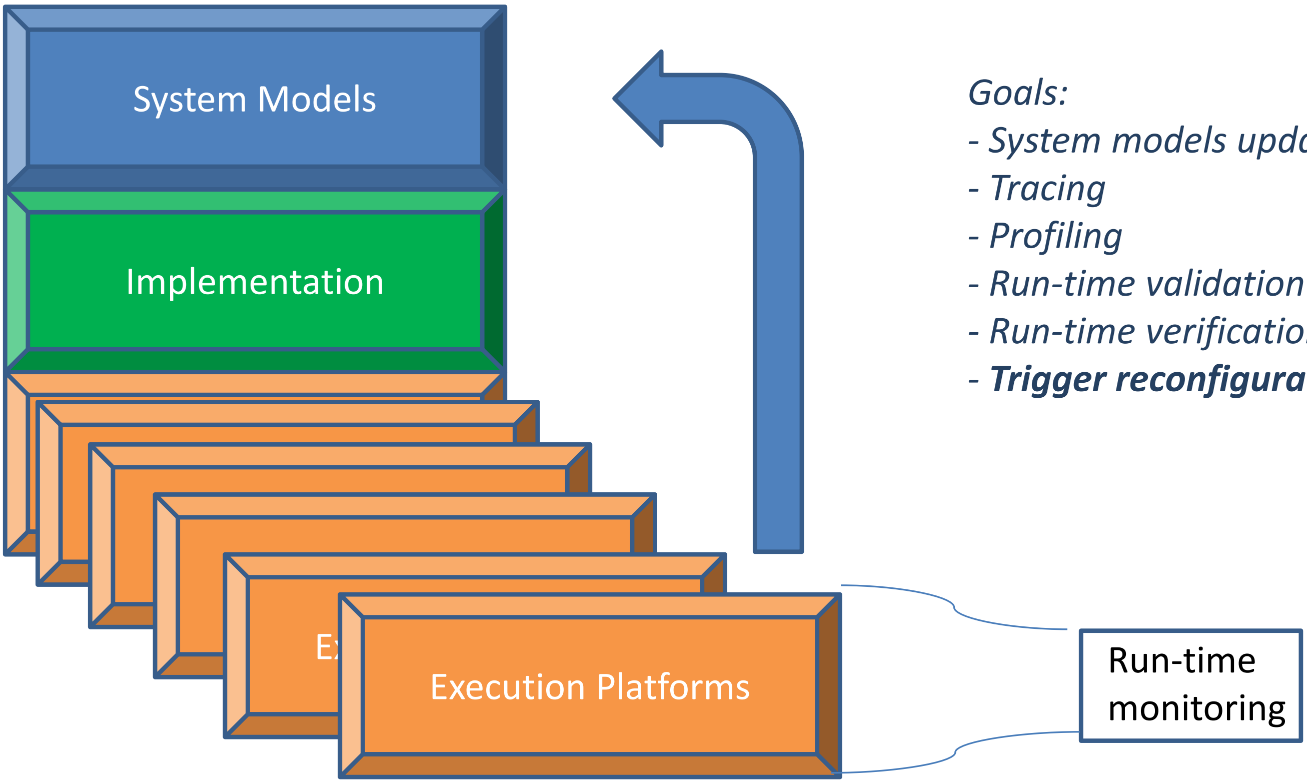


Need for Monitoring

- Cyber-Physical Systems are **adaptive** to changing requirements, among which **metrics related to the system itself**
  - **understanding** such **metrics** becomes increasingly **difficult** if systems are complex
  - e.g. to obtain information on the run-time behaviour of threads, **visibility** into the processor **architecture** is **needed** to monitor workload interactions
- **Simulators** represent a first answer but
  - often **focus** on a **particular level** in the **system hierarchy** (due to performance and complexity issues
  - **slow down execution** when implemented in software and provide such a combined level of visibility
- **Monitoring** is a valid alternative

03/06/2021 38

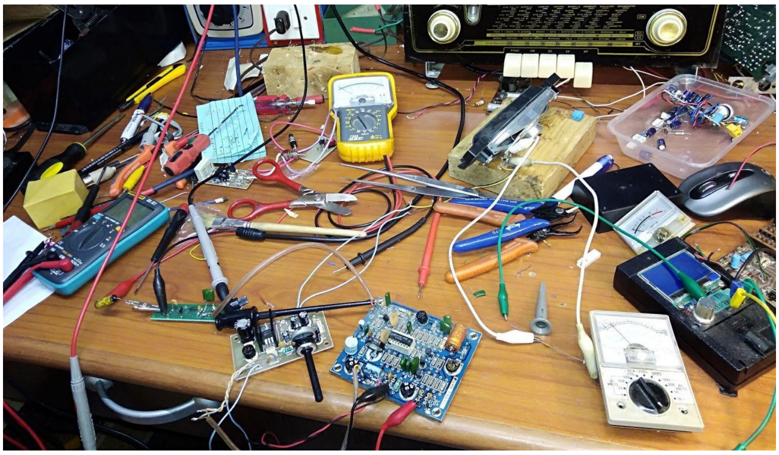
Monitoring goals



Goals:
- System models update
- Tracing
- Profiling
- Run-time validation
- Run-time verification
- Trigger reconfiguration

Issues of Monitoring

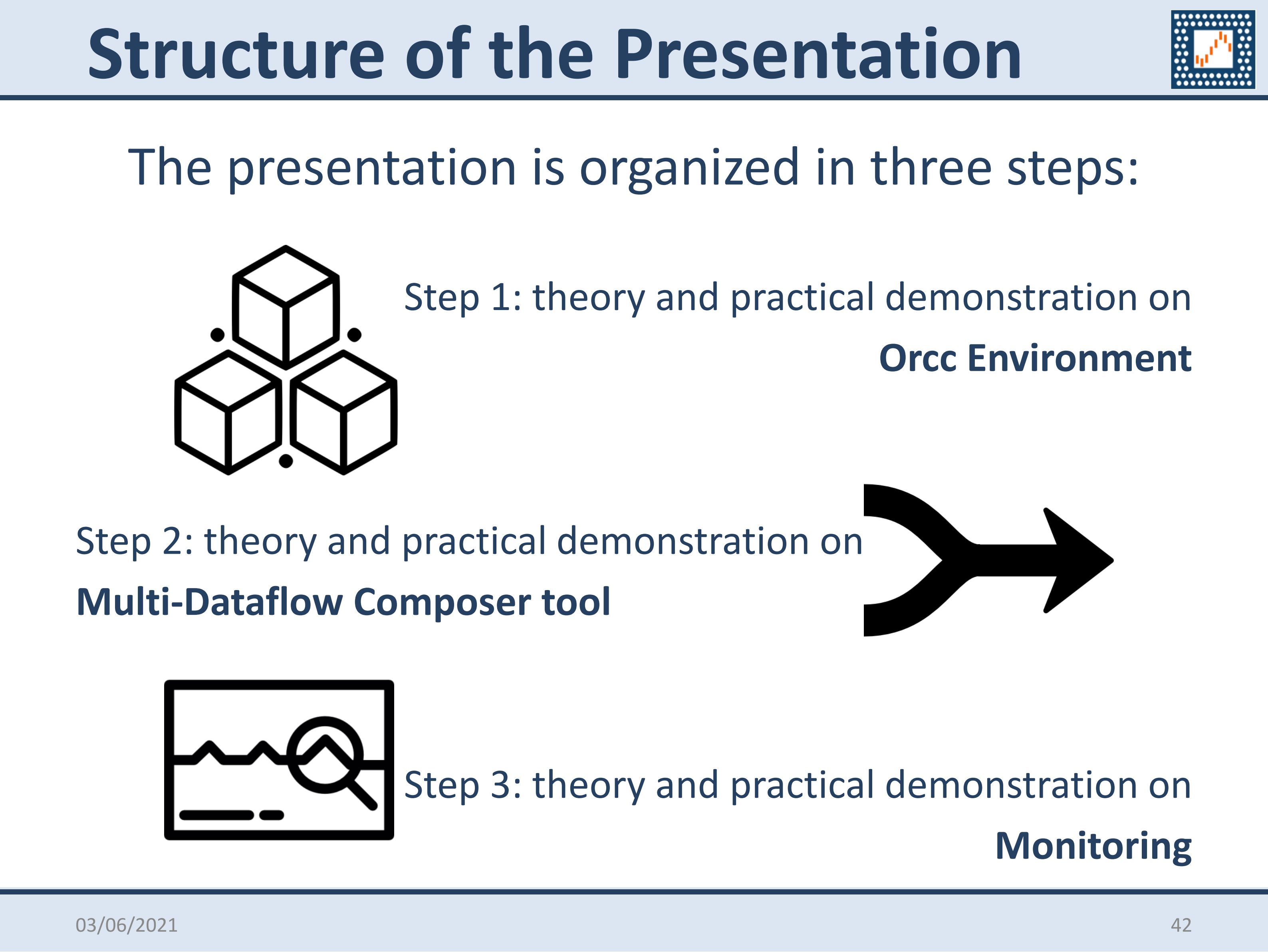
- **What** is the object of monitoring?
- **When** it has to be monitored?
- **How** it is possible to **monitor** it?
- **How** monitored data should be **interpreted**?
- CPS challenges
  - Complexity
  - Adaptivity
  - Heterogeneity



03/06/2021

CPS&IoT'2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

Structure of the Presentation



Structure of the Presentation

The presentation is organized in three steps:

Step 1: theory and practical demonstration on **Orcc Environment**

Step 2: theory and practical demonstration on **Multi-Dataflow Composer tool**

Step 3: theory and practical demonstration on **Monitoring**

03/06/2021

42

CPS&IoT'2021

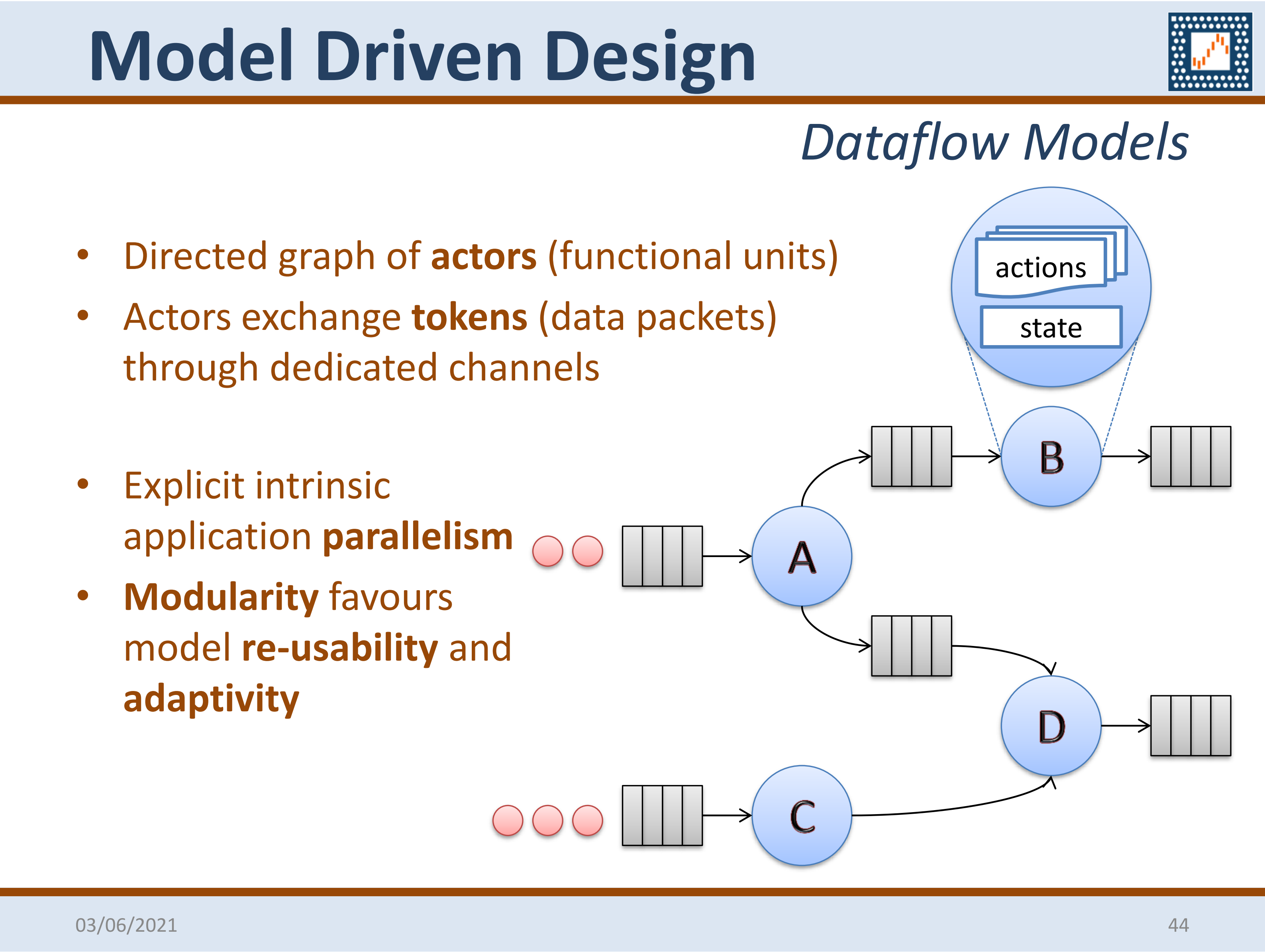
2nd Summer School on Cyber Physical

+ Systems and Internet of Things

Step 1: The Orcc Environment

uniss

UNIVERSITÀ DEGLI STUDI DI SASSARI



Model Driven Design

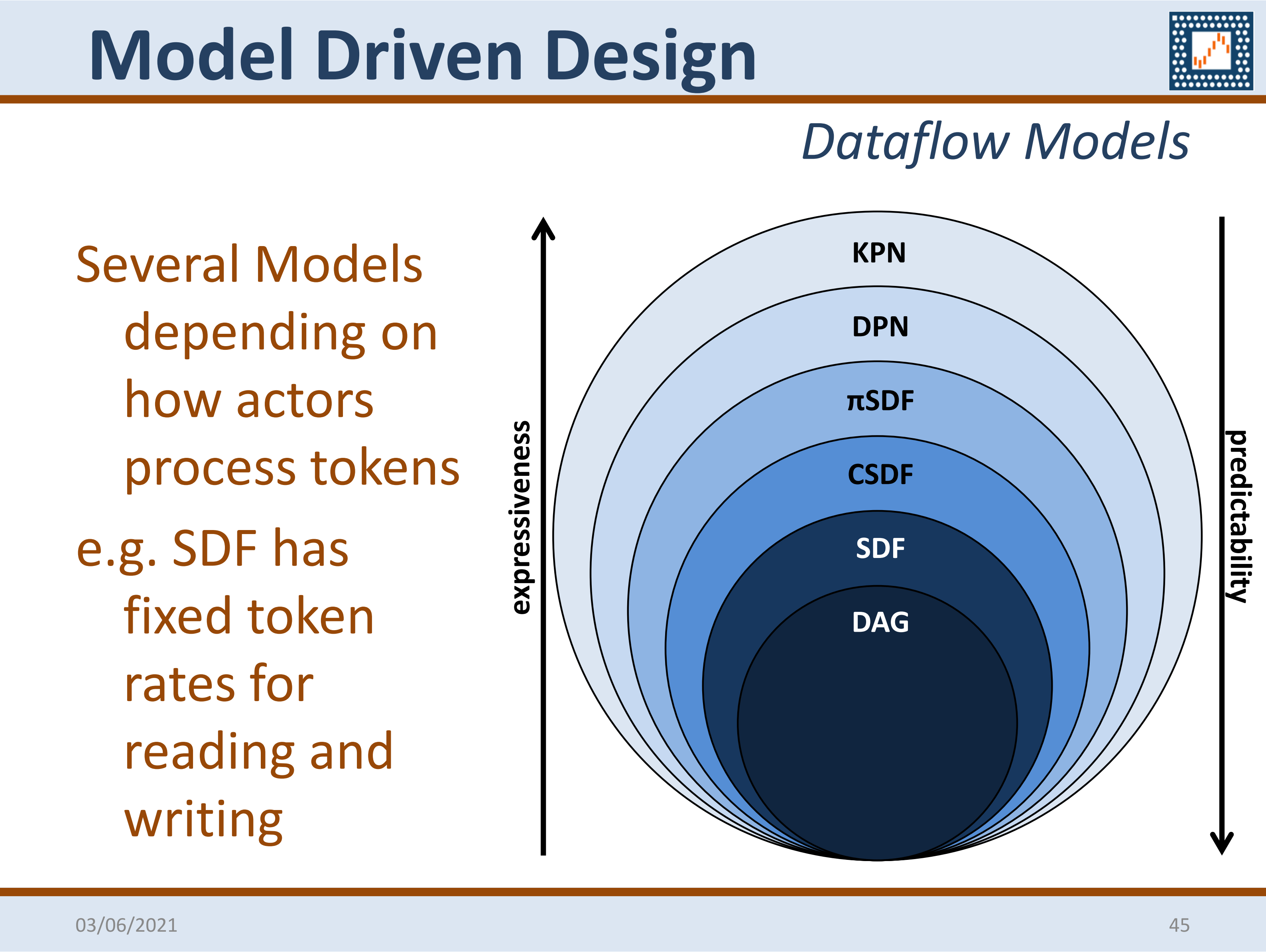
Dataflow Models

- Directed graph of **actors** (functional units)
- Actors exchange **tokens** (data packets) through dedicated channels

- Explicit intrinsic application **parallelism**
- **Modularity** favours model **re-usability** and **adaptivity**

03/06/2021

44



Model Driven Design

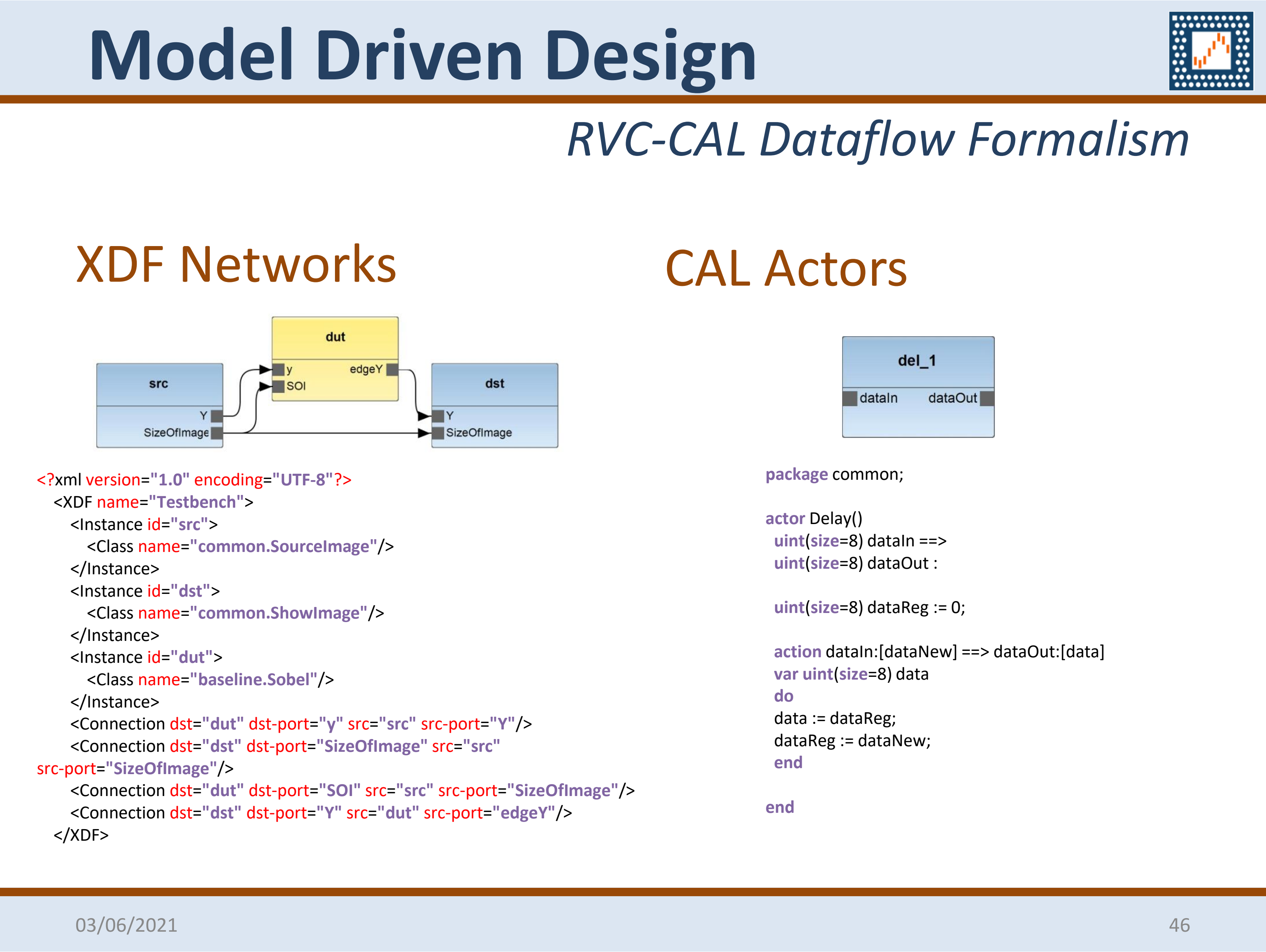
Dataflow Models

Several Models depending on how actors process tokens

e.g. SDF has fixed token rates for reading and writing

03/06/2021

45



Model Driven Design

RVC-CAL Dataflow Formalism

XDF Networks

dut
y
SOI
edgeY
src
Y
SizeOfImage
dst
Y
SizeOfImage

```
<?xml version="1.0" encoding="UTF-8"?>
  <XDF name="Testbench">
    <Instance id="src">
      <Class name="common.SourceImage"/>
    </Instance>
    <Instance id="dst">
      <Class name="common.ShowImage"/>
    </Instance>
    <Instance id="dut">
      <Class name="baseline.Sobel"/>
    </Instance>
    <Connection dst="dut" dst-port="y" src="src" src-port="Y"/>
    <Connection dst="dst" dst-port="SizeOfImage" src="src"
src-port="SizeOfImage"/>
    <Connection dst="dut" dst-port="SOI" src="src" src-port="SizeOfImage"/>
    <Connection dst="dst" dst-port="Y" src="dut" src-port="edgeY"/>
  </XDF>
```

CAL Actors

del_1
dataIn
dataOut

```
package common;

actor Delay()
 uint(size=8) dataIn ==>
 uint(size=8) dataOut :

 uint(size=8) dataReg := 0;

 action dataIn:[dataNew] ==> dataOut:[data]
 var uint(size=8) data
 do
 data := dataReg;
 dataReg := dataNew;
 end

end
```

03/06/2021

46

Test Case

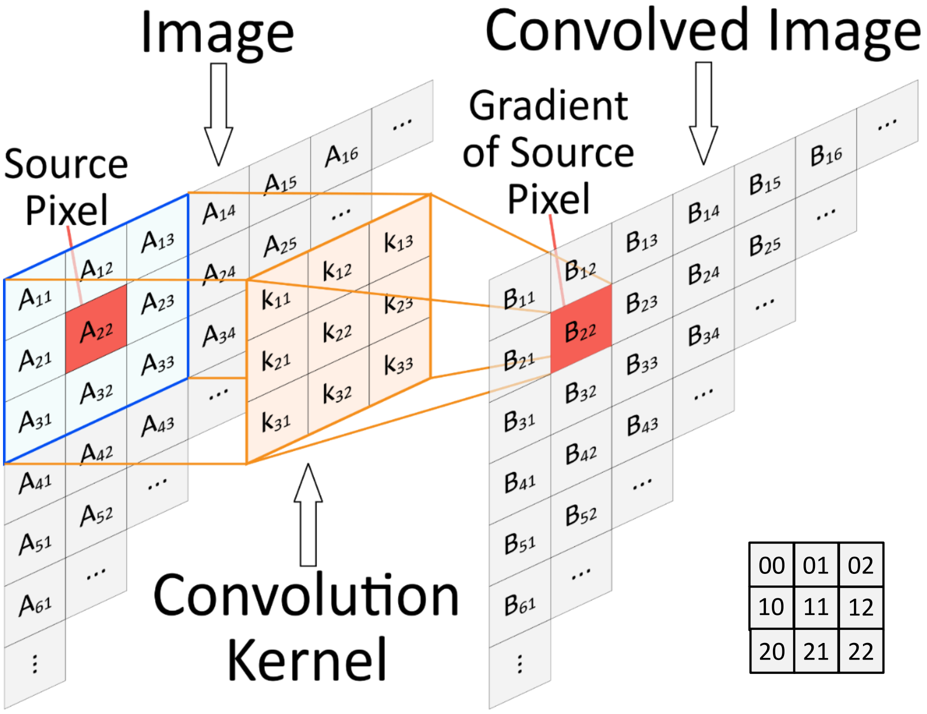
Edge Detection

Sobel Operator

$$\mathbf{G} = \sqrt{{\mathbf{G}_x}^2 + {\mathbf{G}_y}^2}$$

$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

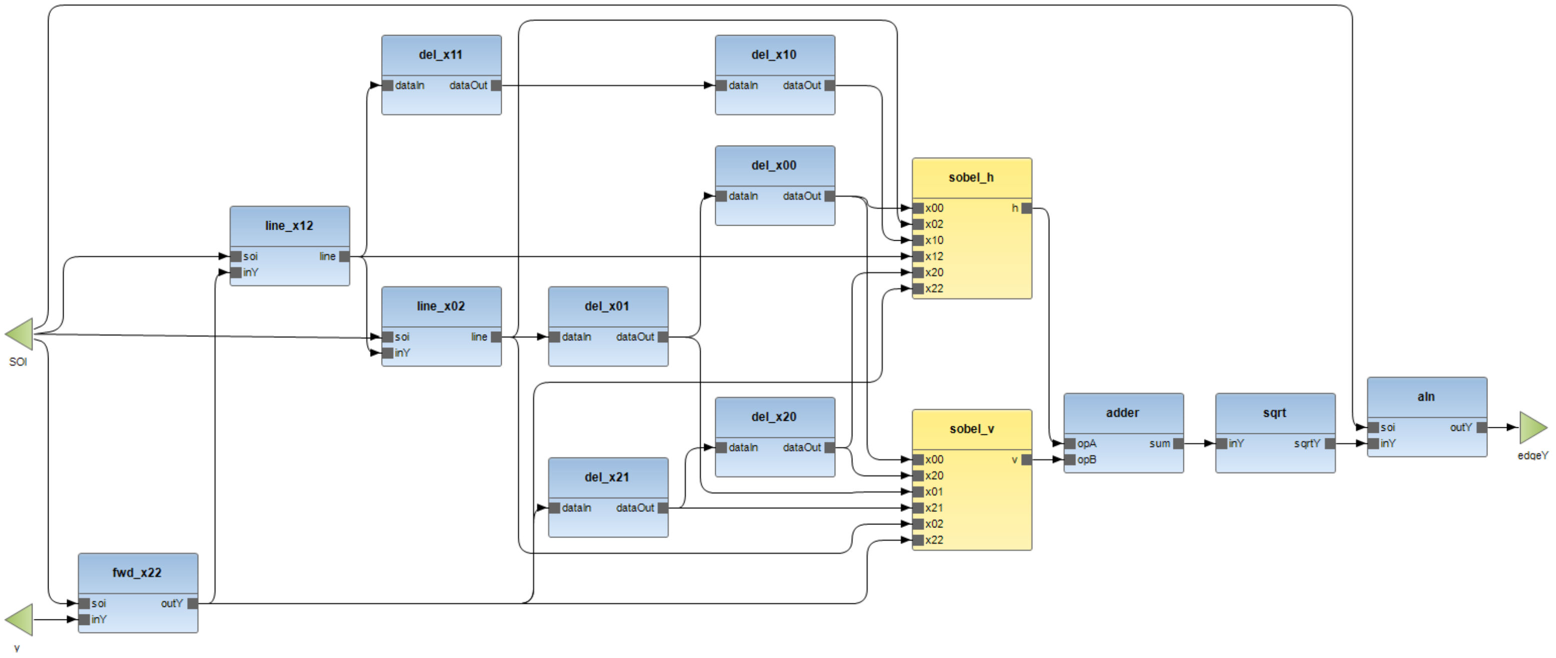
$$\mathbf{G}_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$



00	01	02
10	11	12
20	21	22

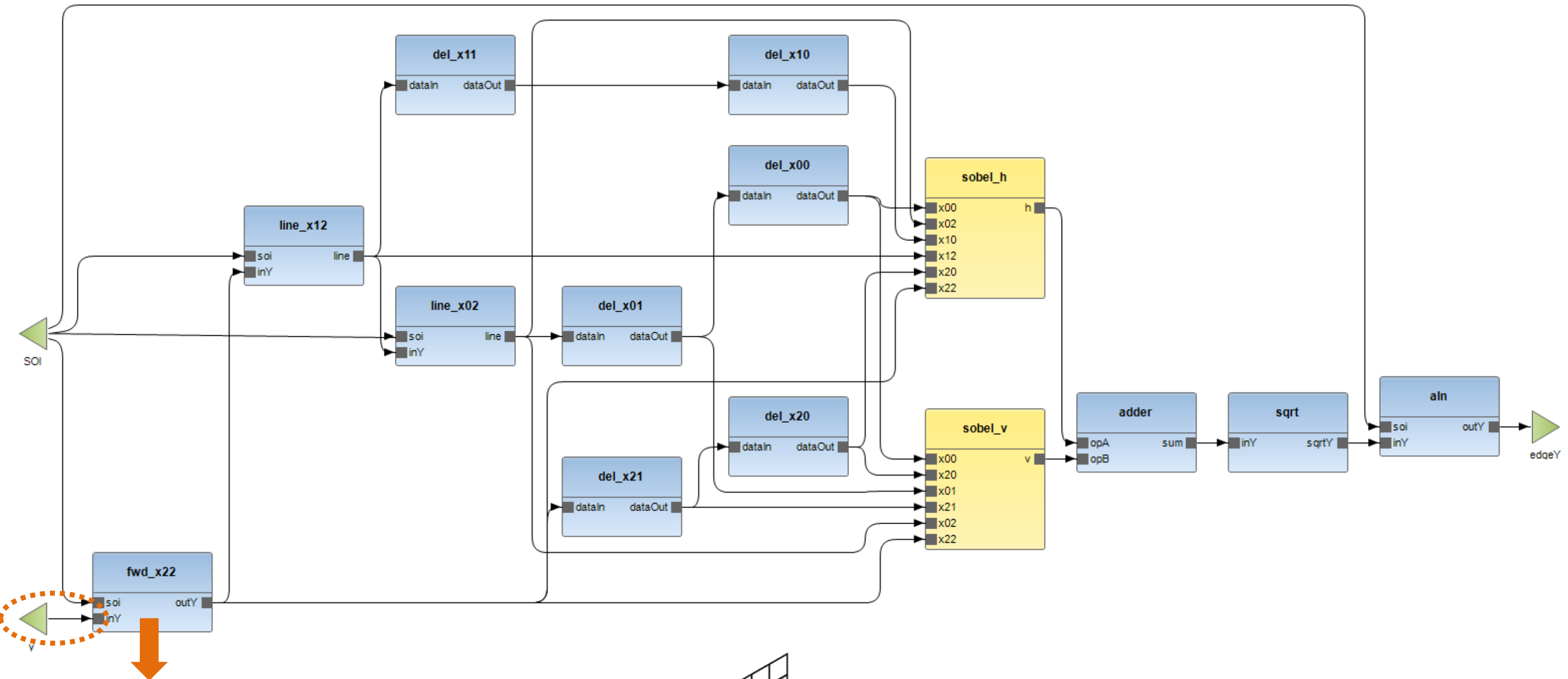
Test Case

Sobel XDF



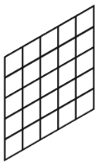
Test Case

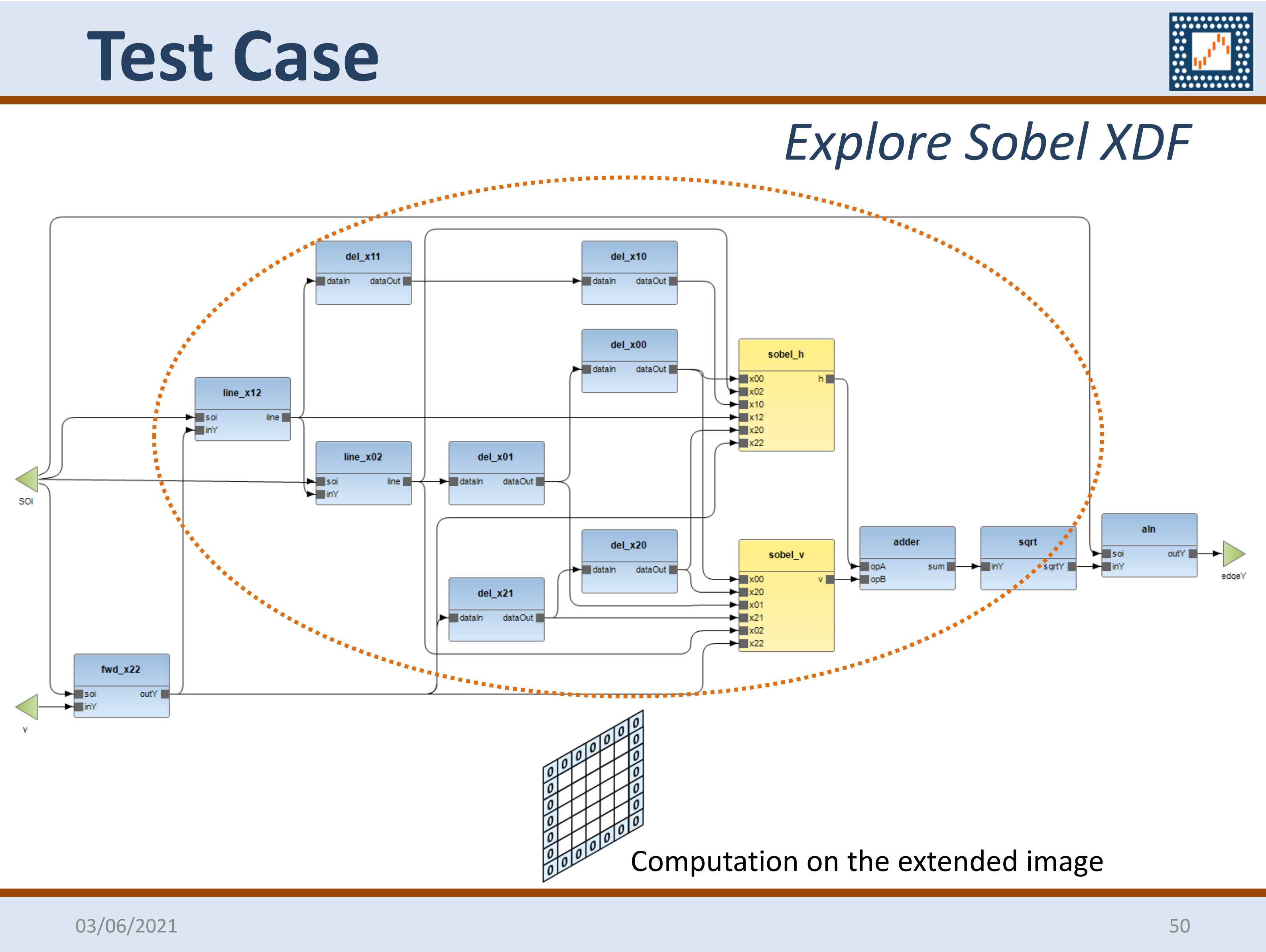
Explore Sobel XDF



Forward3x3.cal actor

Add 2 rows and 2 columns frame all around the input image





Test Case

Explore Sobel XDF

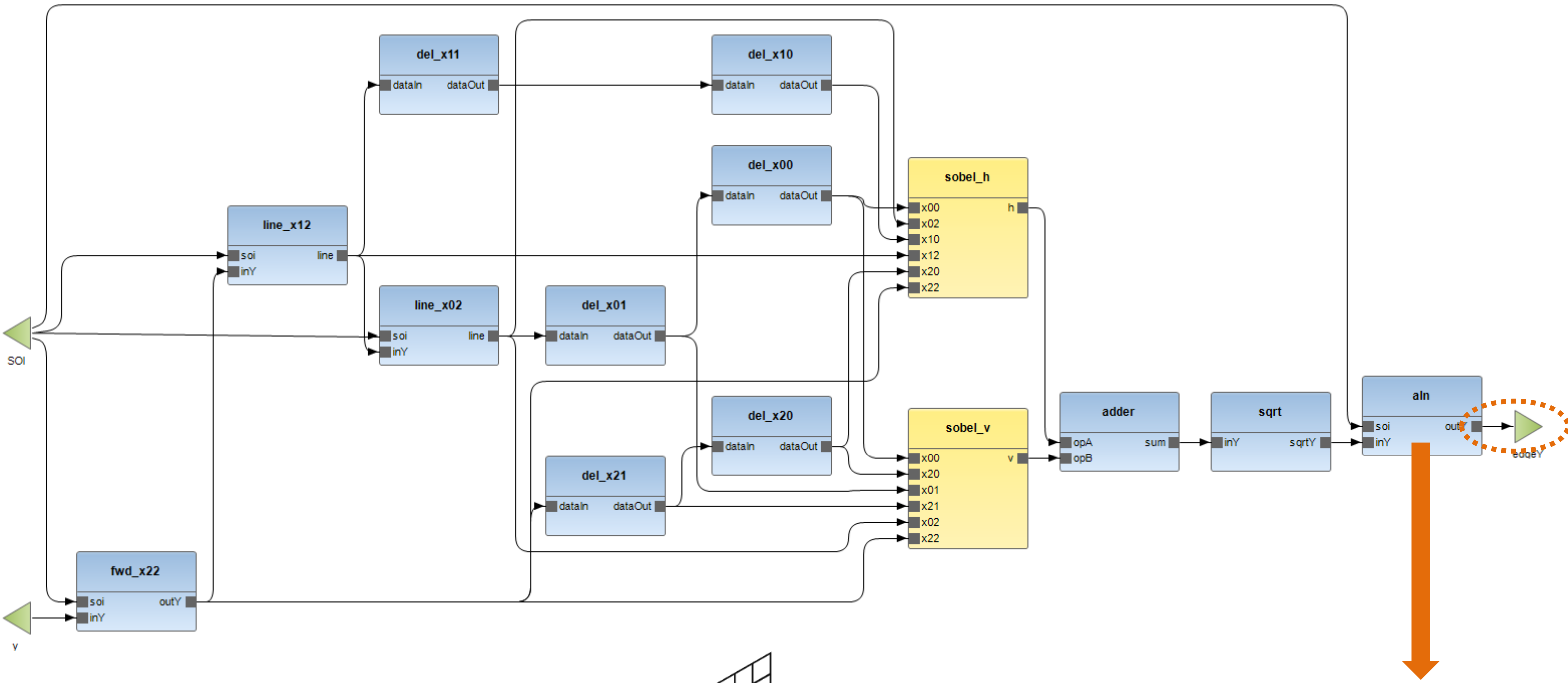
Computation on the extended image

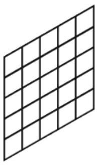
03/06/2021

50

Test Case

Explore Sobel XDF



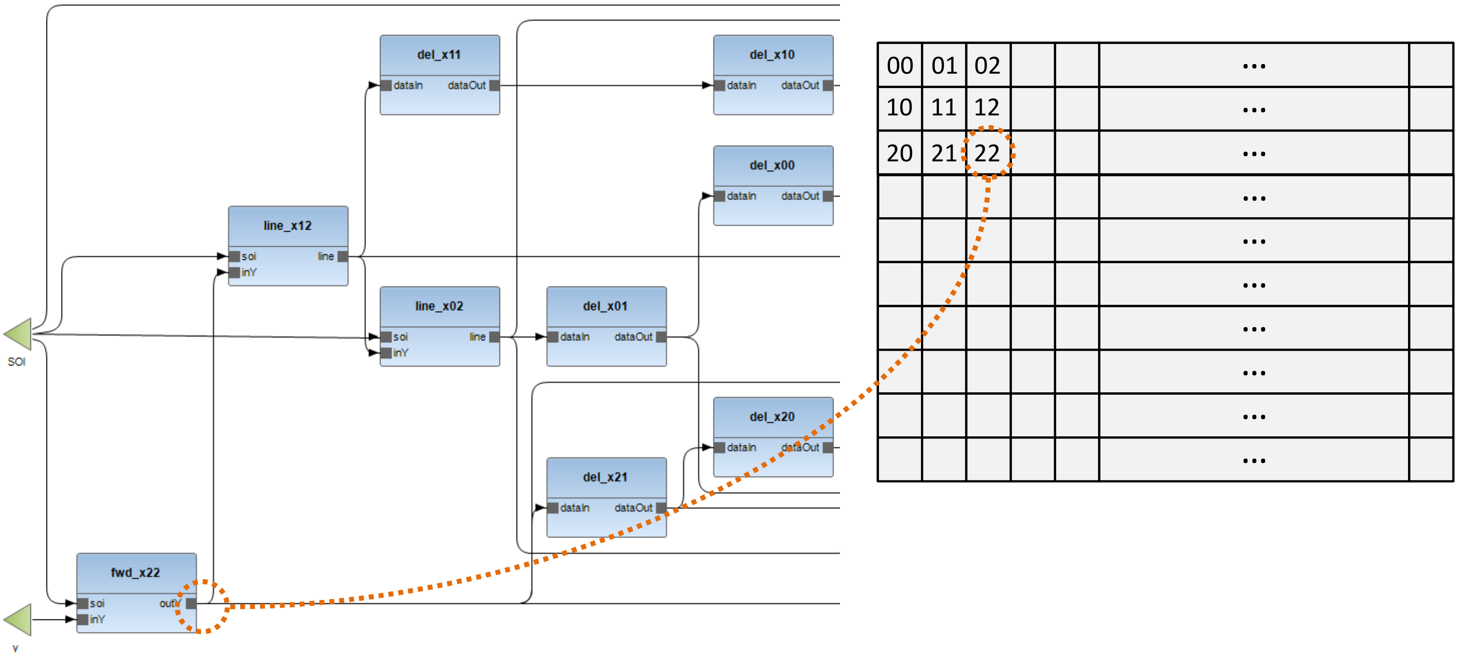


Align3x3.cal actor

Remove 2 rows and 2 columns frame from the input image

Test Case

Explore Sobel XDF

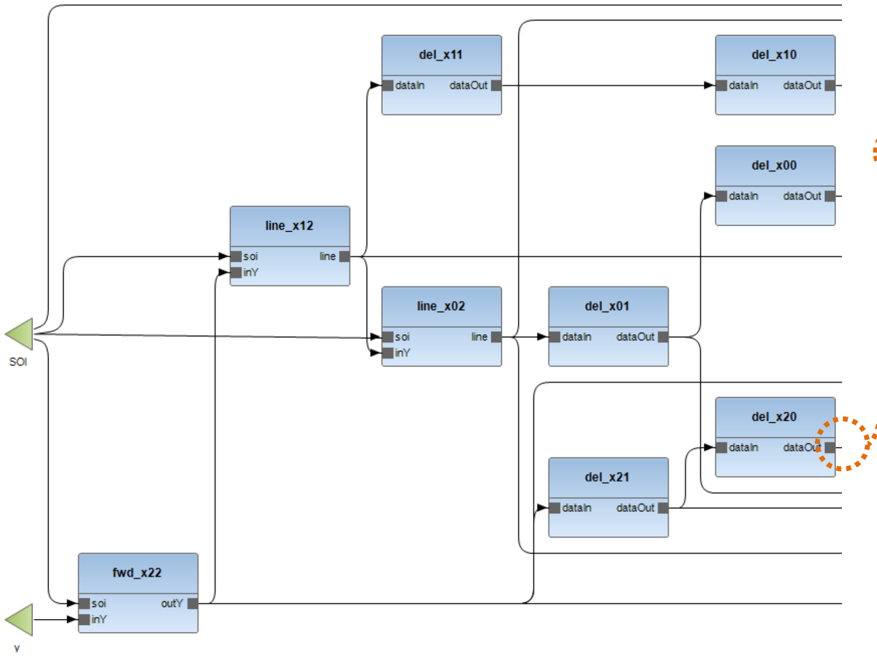


00	01	02			…	
10	11	12			…	
20	21	22			…	
					…	
					…	
					…	
					…	
					…	
					…	
					…	

Since the image comes **pixel by pixel**, it is necessary to **build 3x3 sub-images** on which the **convolution kernel** has to be applied

Test Case

Explore Sobel XDF



00	01	02			…	
10	11	12			…	
20	21	22			…	
					…	
					…	
					…	
					…	
					…	
					…	
					…	

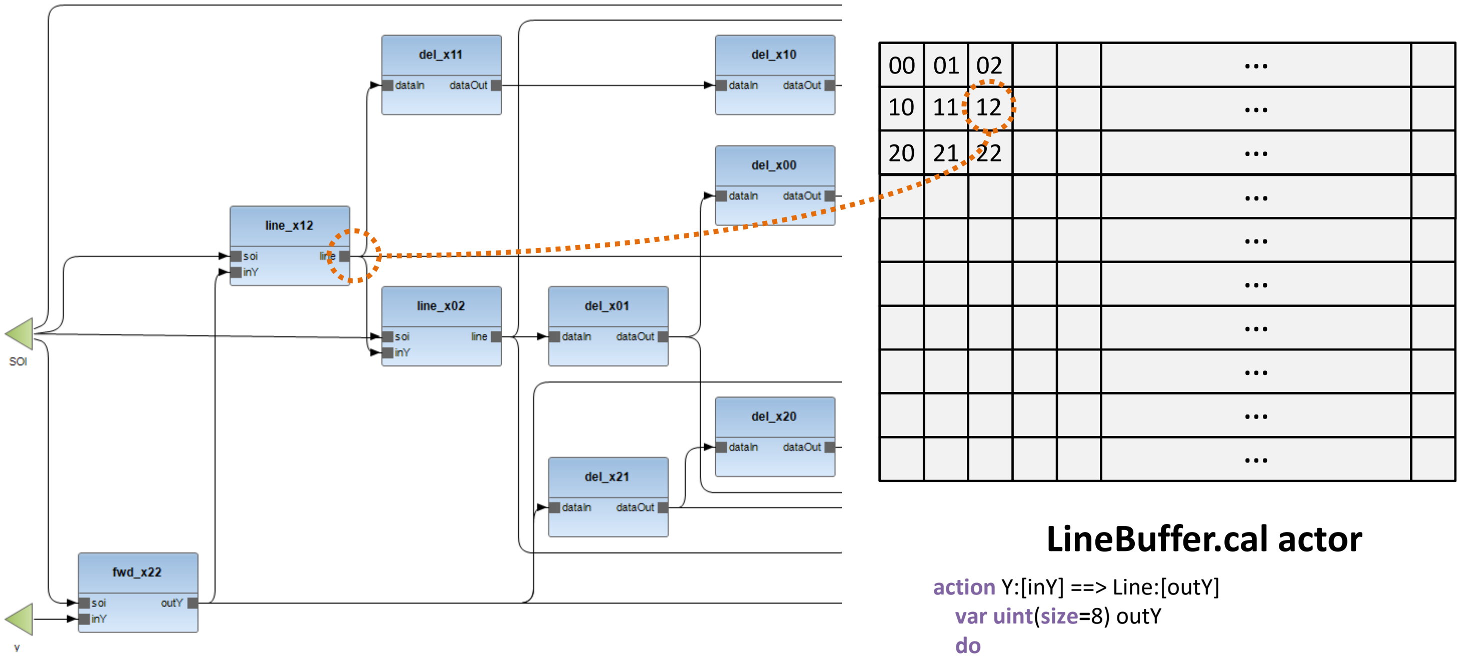
Delay actor **stores one pixel**

Delay.cal actor

```
action dataIn:[dataNew] ==> dataOut:[data]
    var uint(size=8) data
    do
        data := dataReg;
        dataReg := dataNew;
   end
```

Test Case

Explore Sobel XDF



00	01	02			…	
10	11	12			…	
20	21	22			…	
					…	
					…	
					…	
					…	
					…	
					…	
					…	

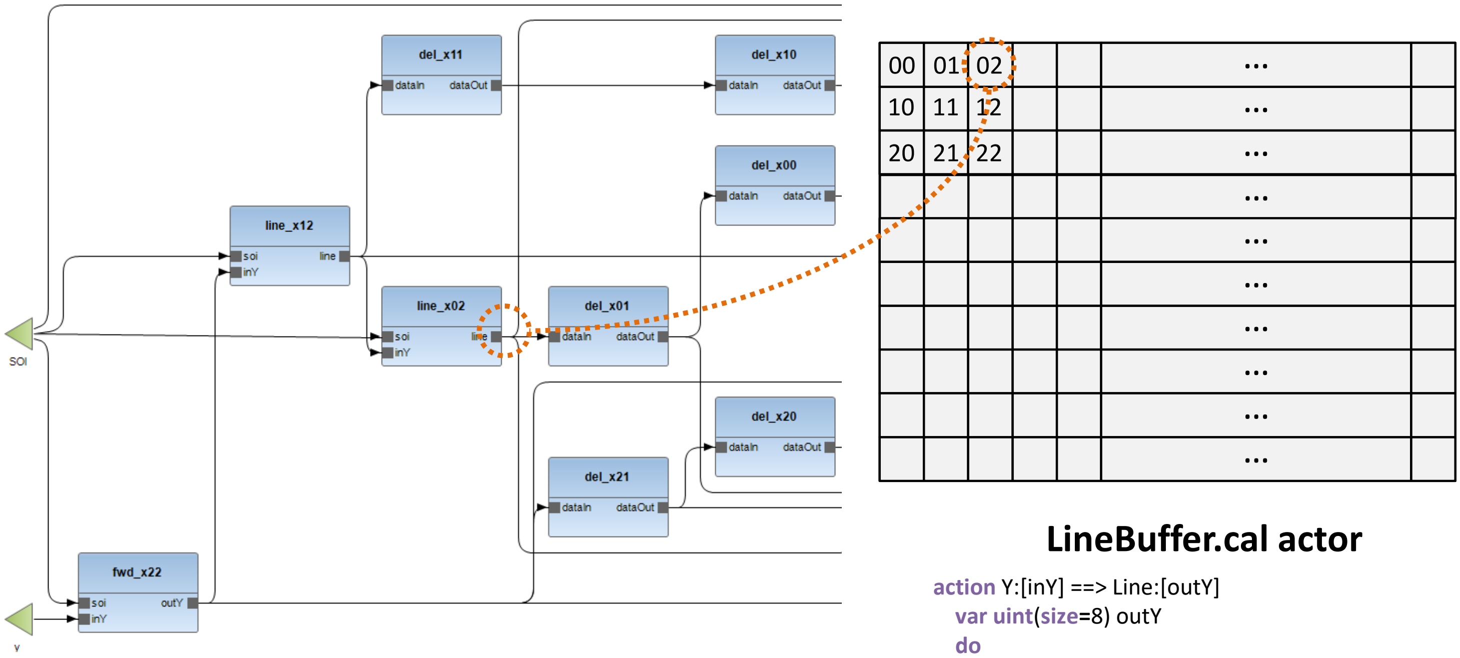
LineBuffer actor **stores one row of pixels**

LineBuffer.cal actor

```
action Y:[inY] ==> Line:[outY]
  var uint(size=8) outY
  do
    outY := lineBuffer[x];
    lineBuffer[x]:= inY;
    if x = width then
      x := 0;
      if y = height then
        y := 0;                    …
```

Test Case

Explore Sobel XDF



00	01	02			...	
10	11	12			...	
20	21	22			...	
					...	
					...	
					...	
					...	
					...	
					...	
					...	

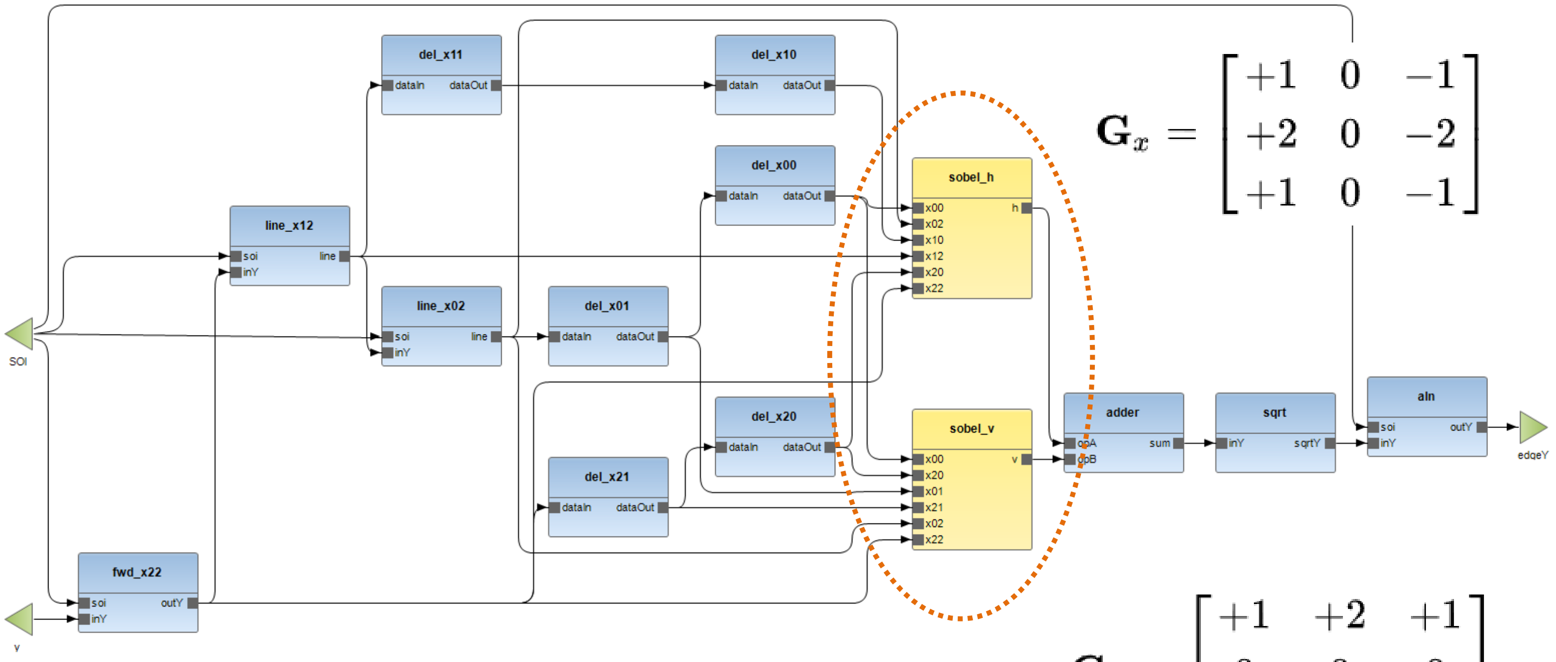
LineBuffer.cal actor

```
action Y:[inY] ==> Line:[outY]
  var uint(size=8) outY
  do
    outY := lineBuffer[x];
    lineBuffer[x]:= inY;
    if x = width then
      x := 0;
      if y = height then
        y := 0;                    ...
```

LineBuffer actor **stores one row of pixels**

Test Case

Explore Sobel XDF



$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

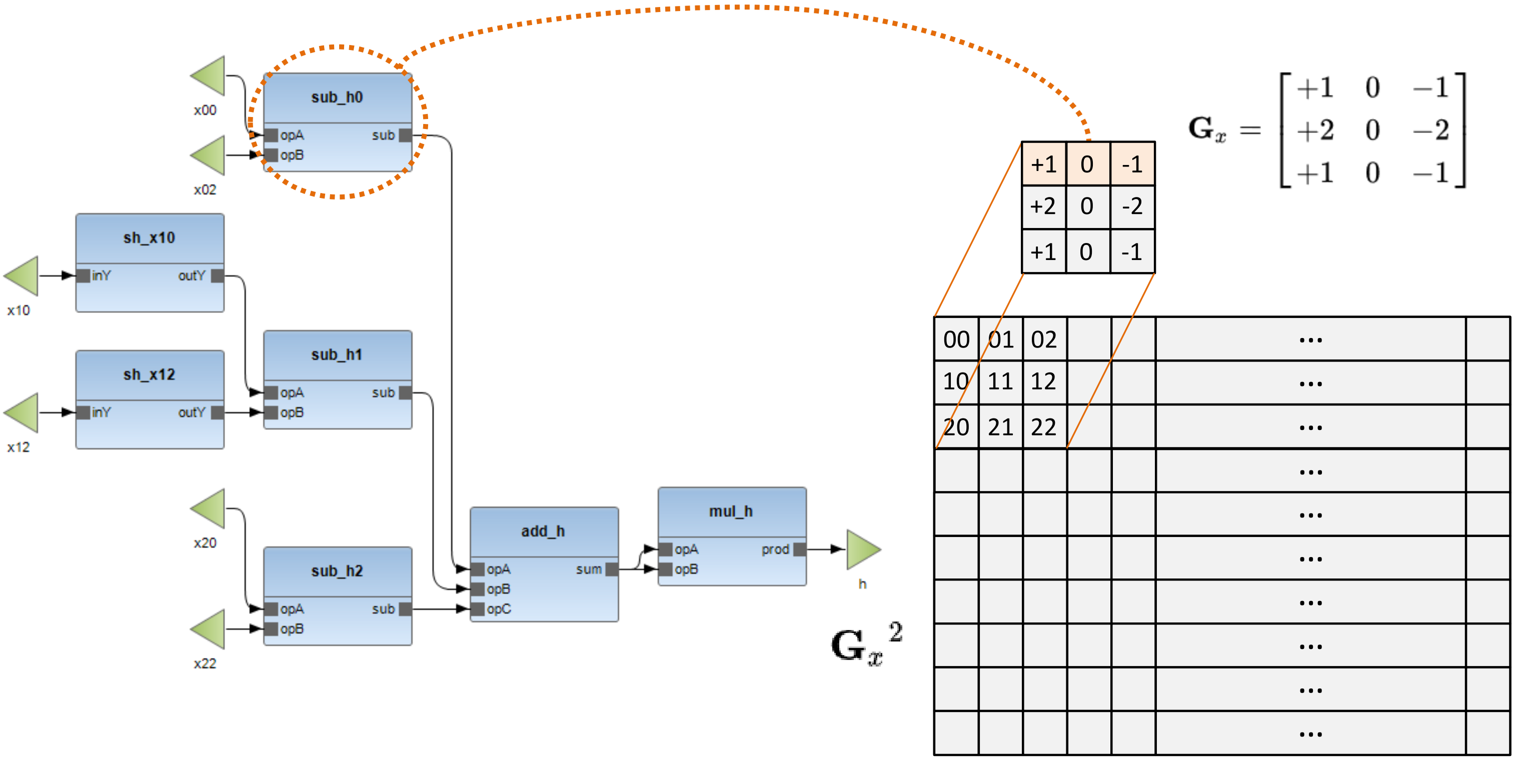
$$\mathbf{G}_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

Sub-networks sobel_h and sobel_v
are used to make the design hierarchical

03/06/2021 56

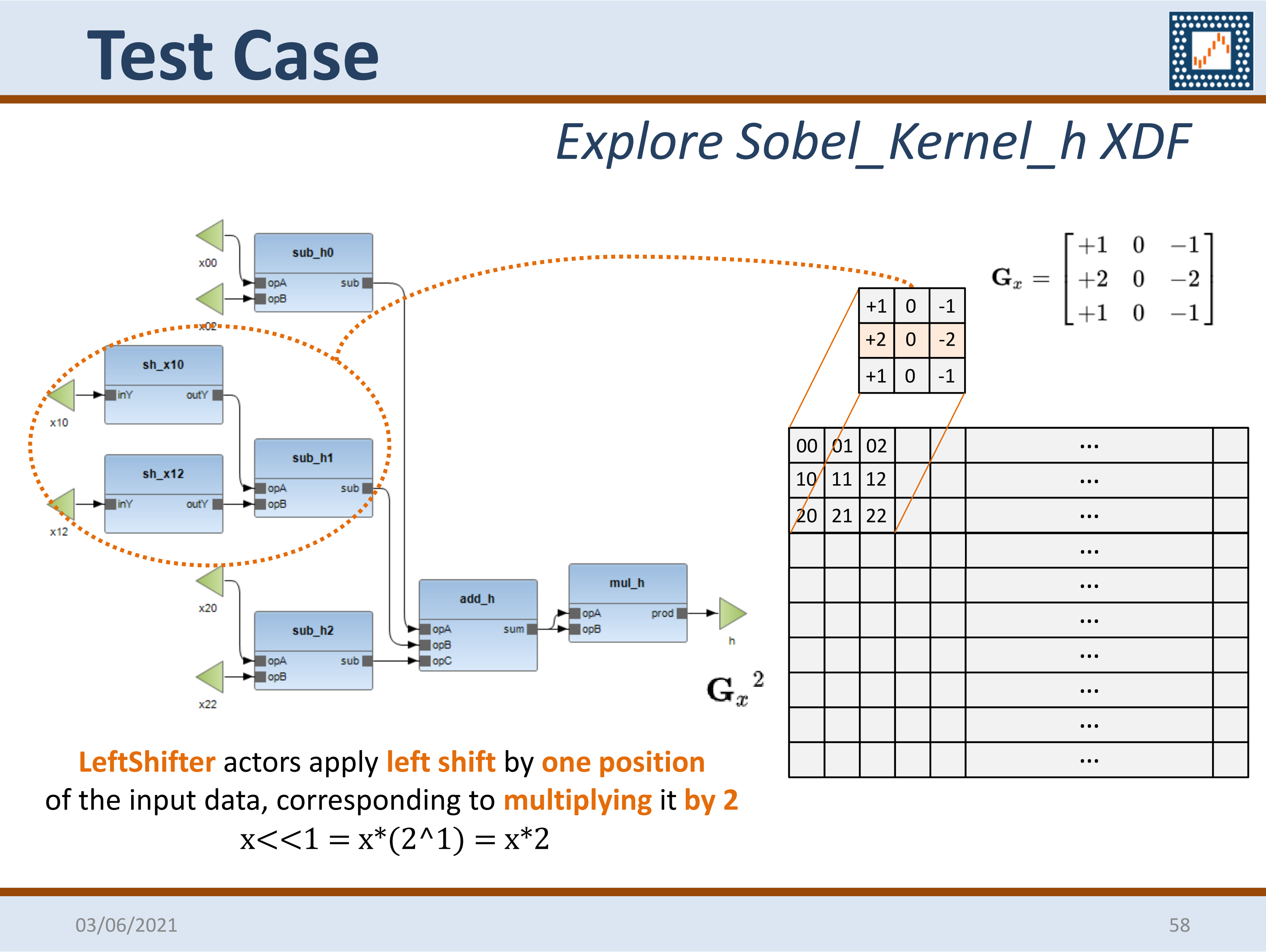
Test Case

Explore Sobel_Kernel_h XDF



$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

$\mathbf{G}_x{}^2$



Test Case

Explore Sobel_Kernel_h XDF

$$\mathbf{G}_x^{\ 2}$$

$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

+1	0	-1
+2	0	-2
+1	0	-1

00	01	02			…	
10	11	12			…	
20	21	22			…	
					…	
					…	
					…	
					…	
					…	
					…	
					…	

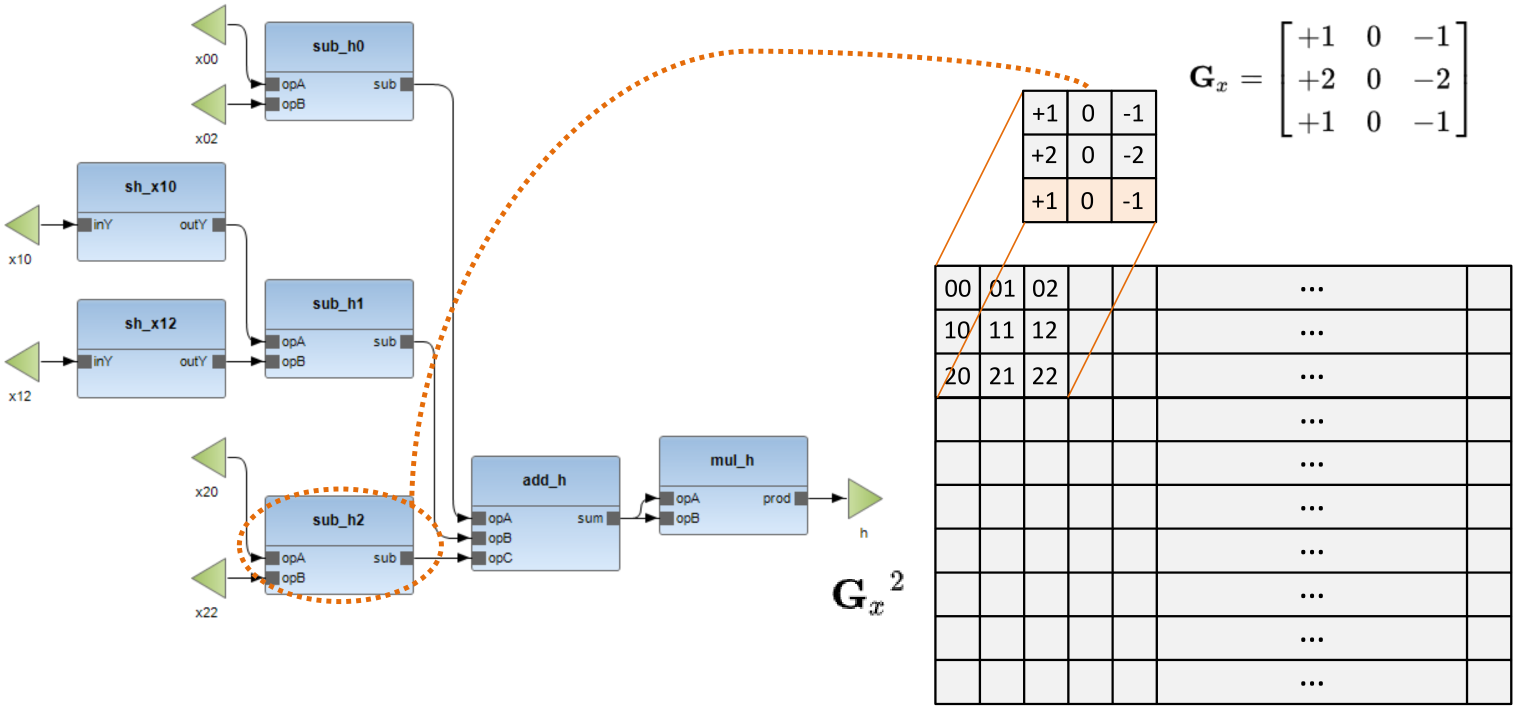
LeftShifter actors apply **left shift** by **one position** of the input data, corresponding to **multiplying** it **by 2**

x<<1 = x*(2^1) = x*2

03/06/2021 58

Test Case

Explore Sobel_Kernel_h XDF



$$\mathbf{G}_x^{\ 2}$$

$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

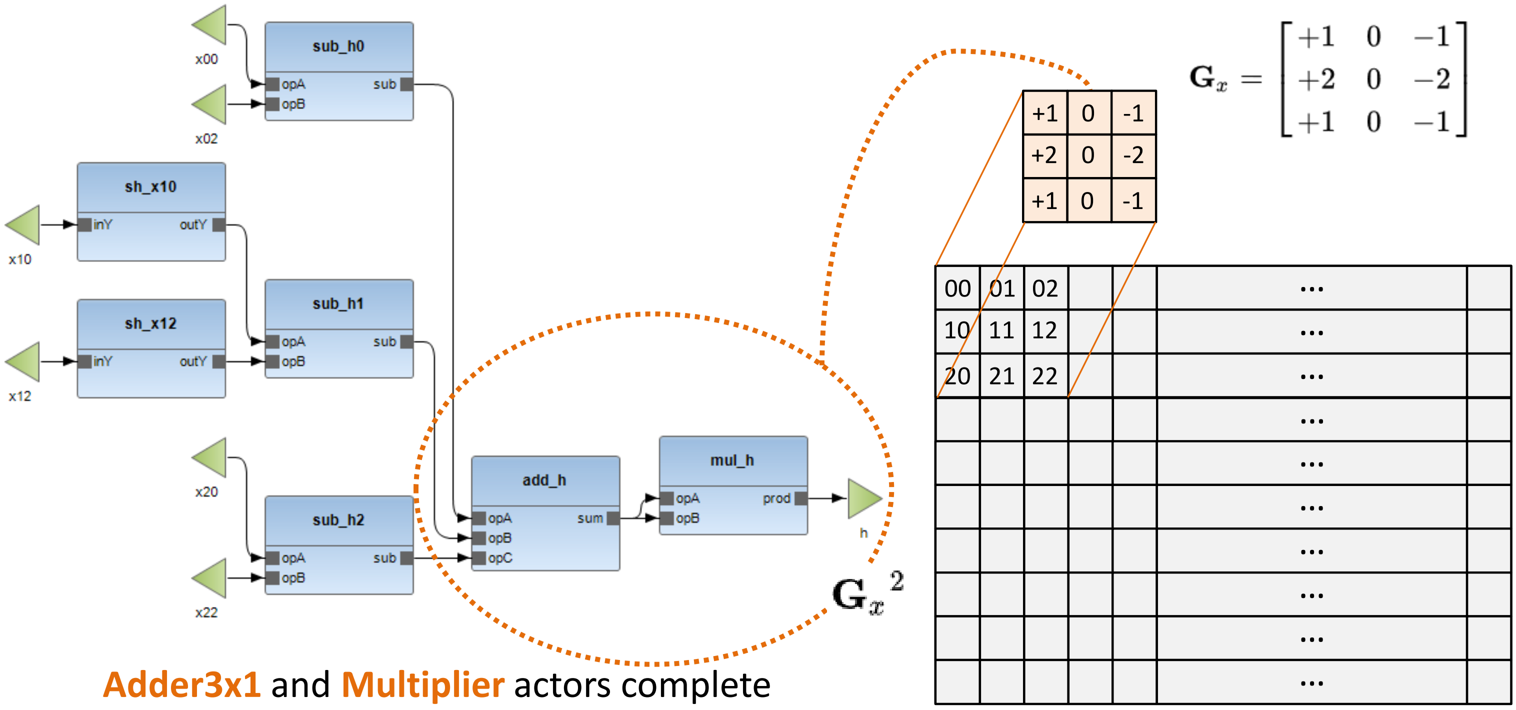
+1	0	-1
+2	0	-2
+1	0	-1

00	01	02			...	
10	11	12			...	
20	21	22			...	
					...	
					...	
					...	
					...	
					...	
					...	
					...	

Test Case

Explore Sobel_Kernel_h XDF

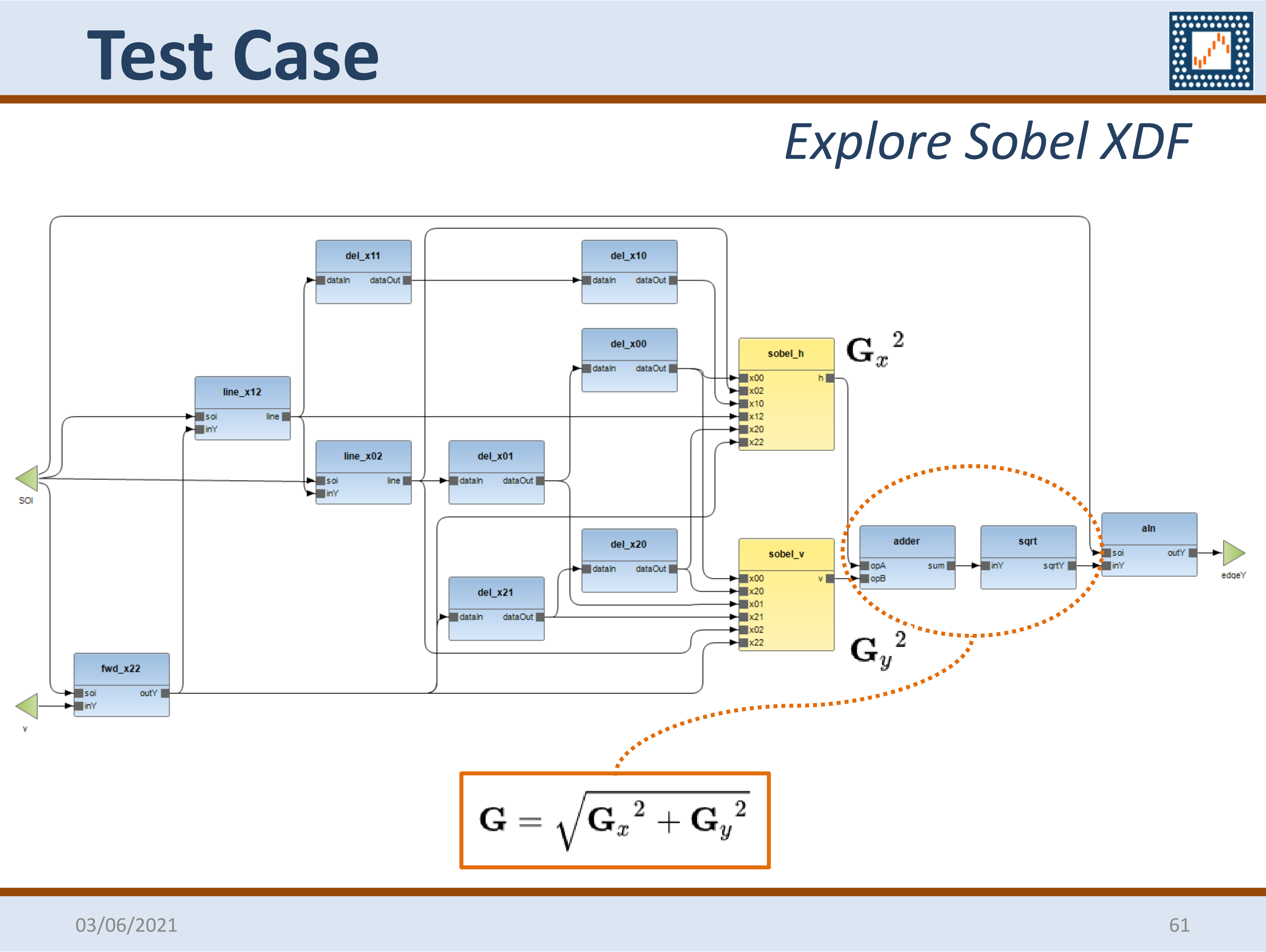
$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$



+1	0	-1
+2	0	-2
+1	0	-1

00	01	02			...	
10	11	12			...	
20	21	22			...	
					...	
					...	
					...	
					...	
					...	
					...	
					...	

Adder3x1 and **Multiplier** actors complete the **squared gradient computation**



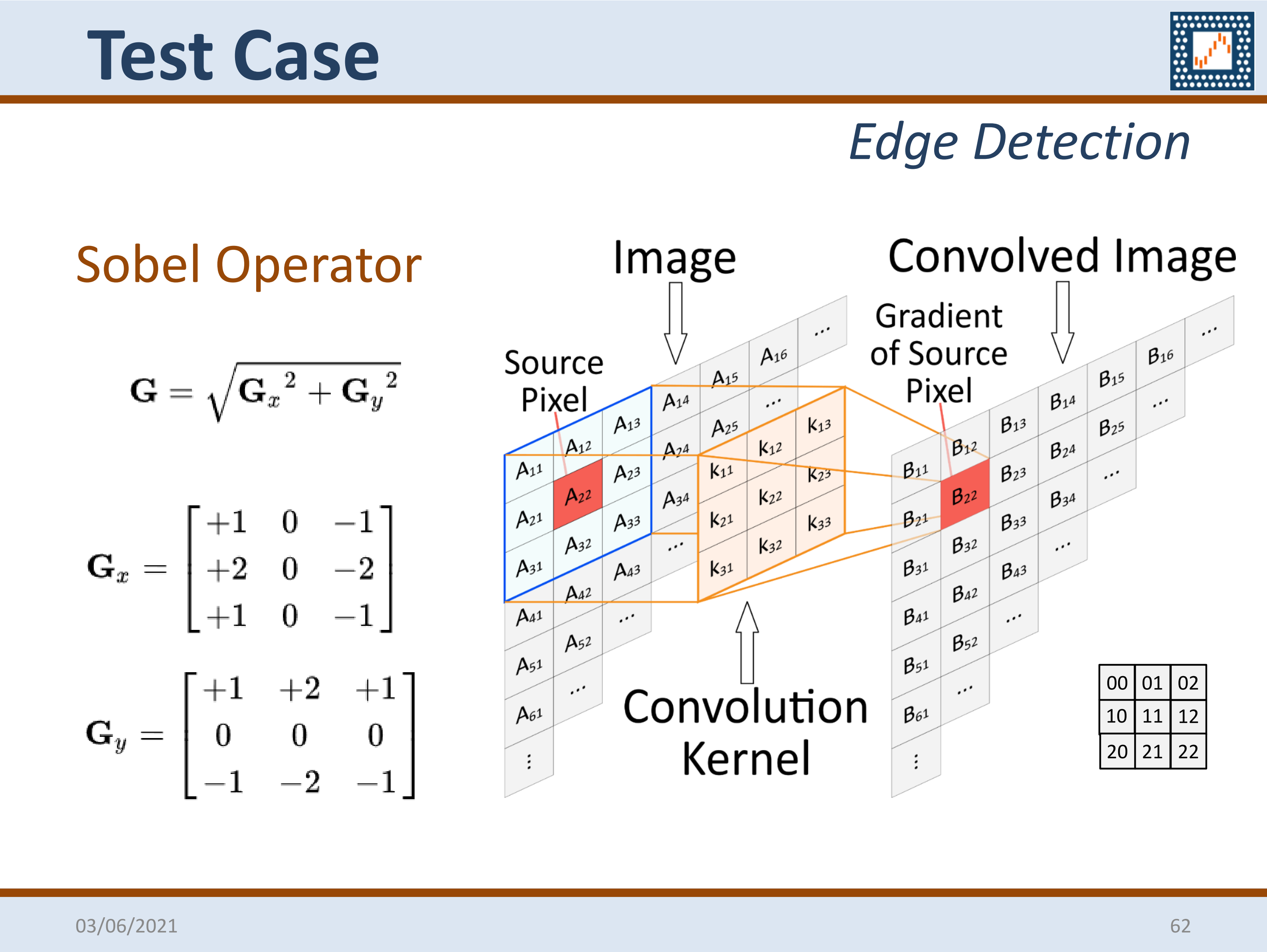
Test Case

Explore Sobel XDF

$\mathbf{G}_x{}^2$

$\mathbf{G}_y{}^2$

$$\mathbf{G} = \sqrt{\mathbf{G}_x{}^2 + \mathbf{G}_y{}^2}$$



Test Case

Edge Detection

Sobel Operator

$$\mathbf{G} = \sqrt{\mathbf{G}_x{}^2 + \mathbf{G}_y{}^2}$$

$$\mathbf{G}_x = \begin{bmatrix} +1 & 0 & -1 \\ +2 & 0 & -2 \\ +1 & 0 & -1 \end{bmatrix}$$

$$\mathbf{G}_y = \begin{bmatrix} +1 & +2 & +1 \\ 0 & 0 & 0 \\ -1 & -2 & -1 \end{bmatrix}$$

Image

Convolved Image

Source Pixel

Gradient of Source Pixel

Convolution Kernel

00	01	02
10	11	12
20	21	22

03/06/2021

62

Test Case

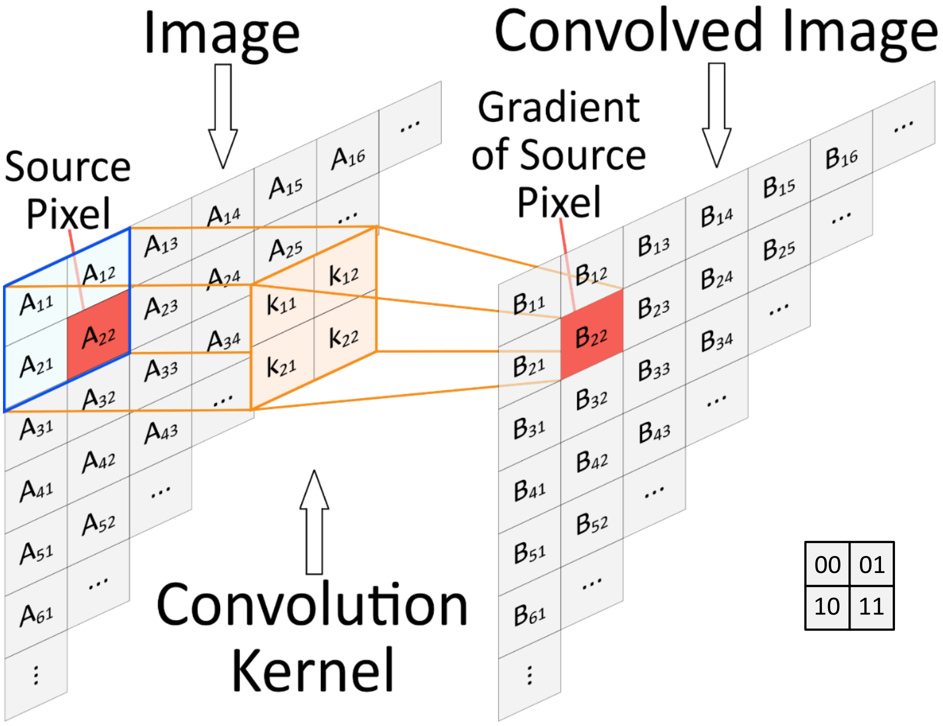
Derive Roberts from Sobel

Roberts Operator

$$\mathbf{G} = \sqrt{{\mathbf{G}_x}^2 + {\mathbf{G}_y}^2}$$

$$G_x = \begin{bmatrix} 0 & +1 \\ -1 & 0 \end{bmatrix}$$

$$G_y = \begin{bmatrix} +1 & 0 \\ 0 & -1 \end{bmatrix}$$



00	01
10	11

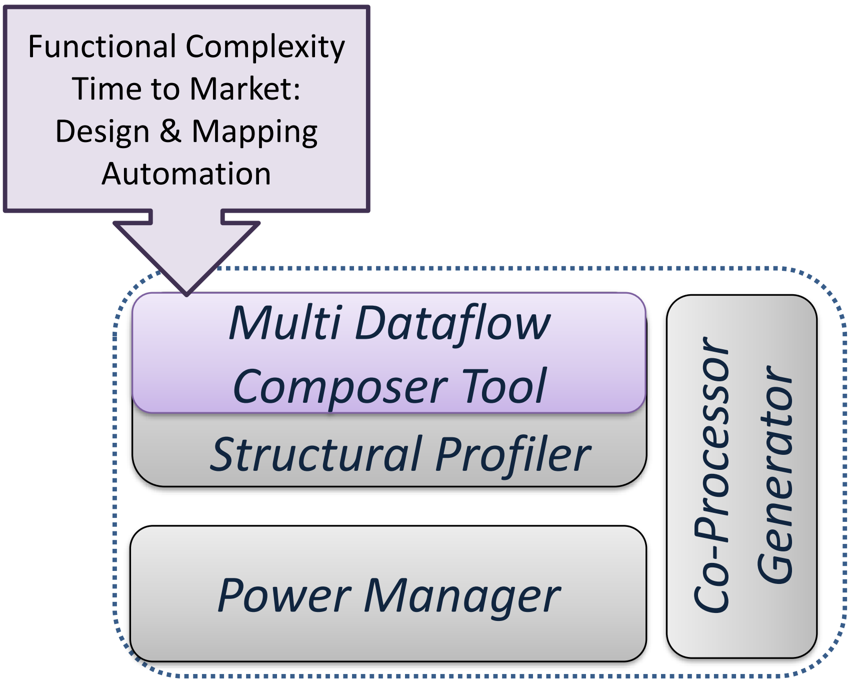
CPS&IoT'2021
2nd Summer School on Cyber Physical +
Systems and Internet of Things

Step 2: the Multi-Dataflow Composer tool

Baseline MDC Datapath Merging

uniss
UNIVERSITÀ DEGLI STUDI DI SASSARI

Baseline: Dataflow to HW



Functional Complexity
Time to Market:
Design & Mapping
Automation

Multi Dataflow Composer Tool

Structural Profiler

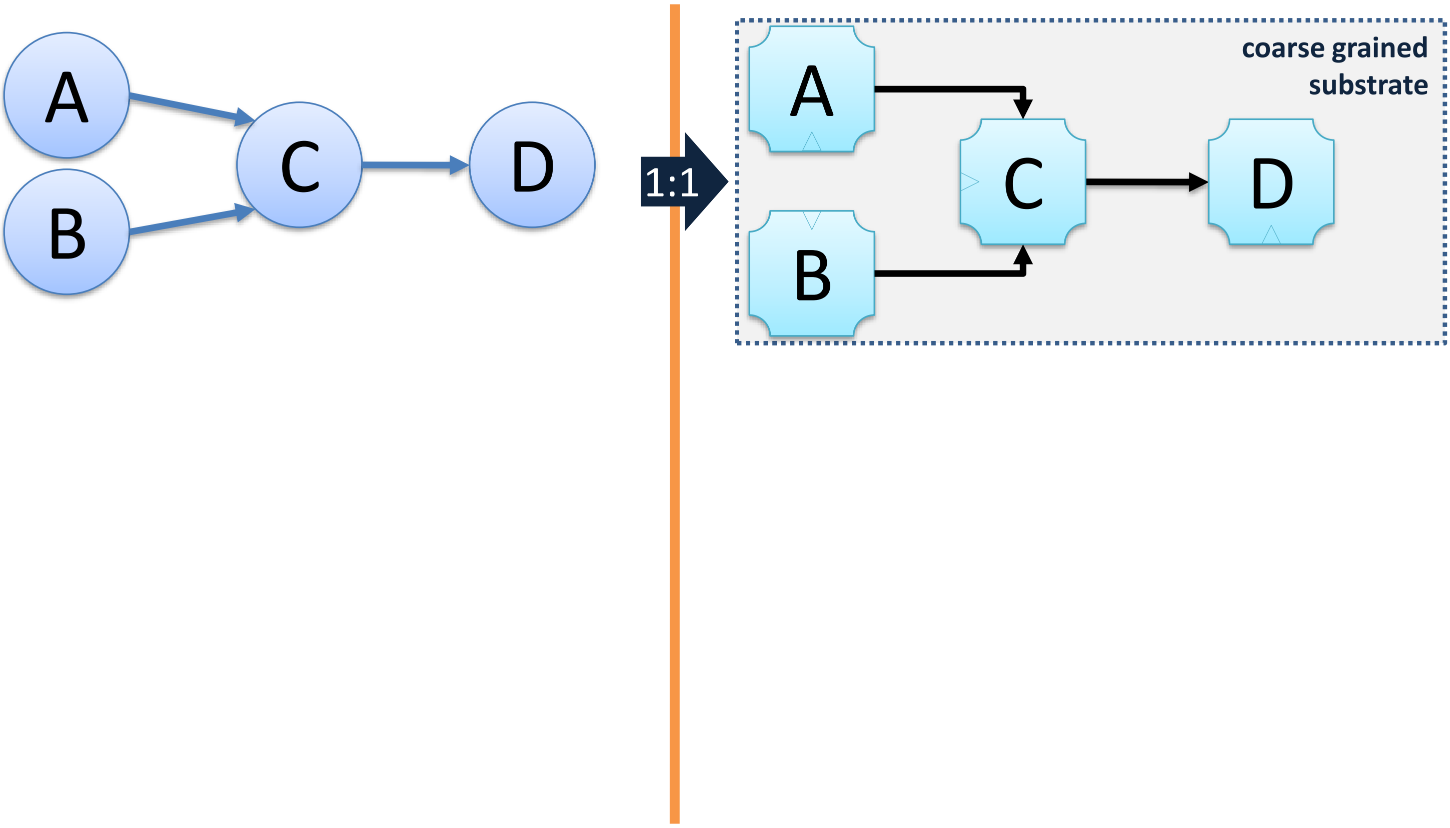
Power Manager

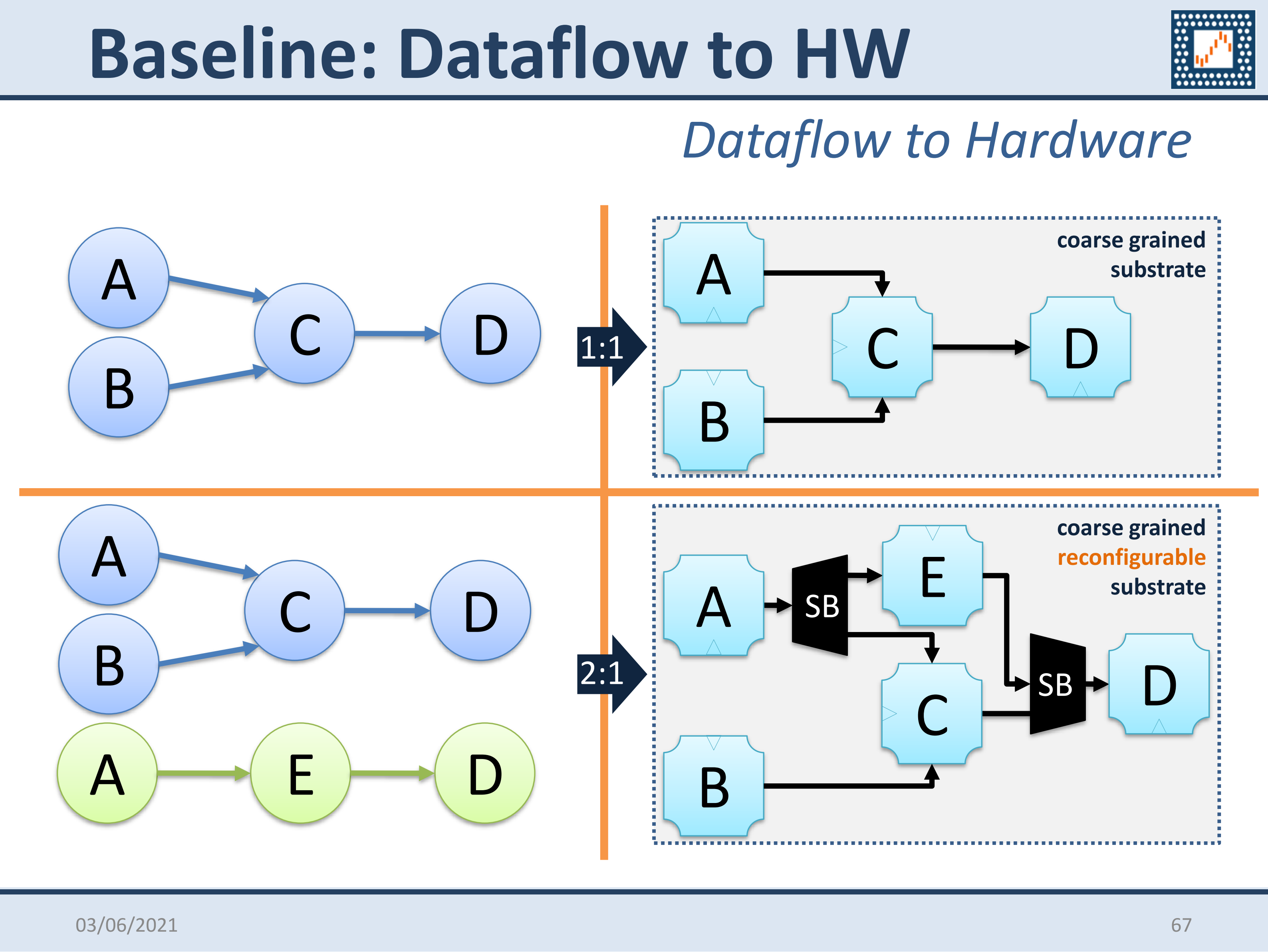
Co-Processor Generator

MDC design suite
http://sites.unica.it/rpct/

Baseline: Dataflow to HW

Dataflow to Hardware





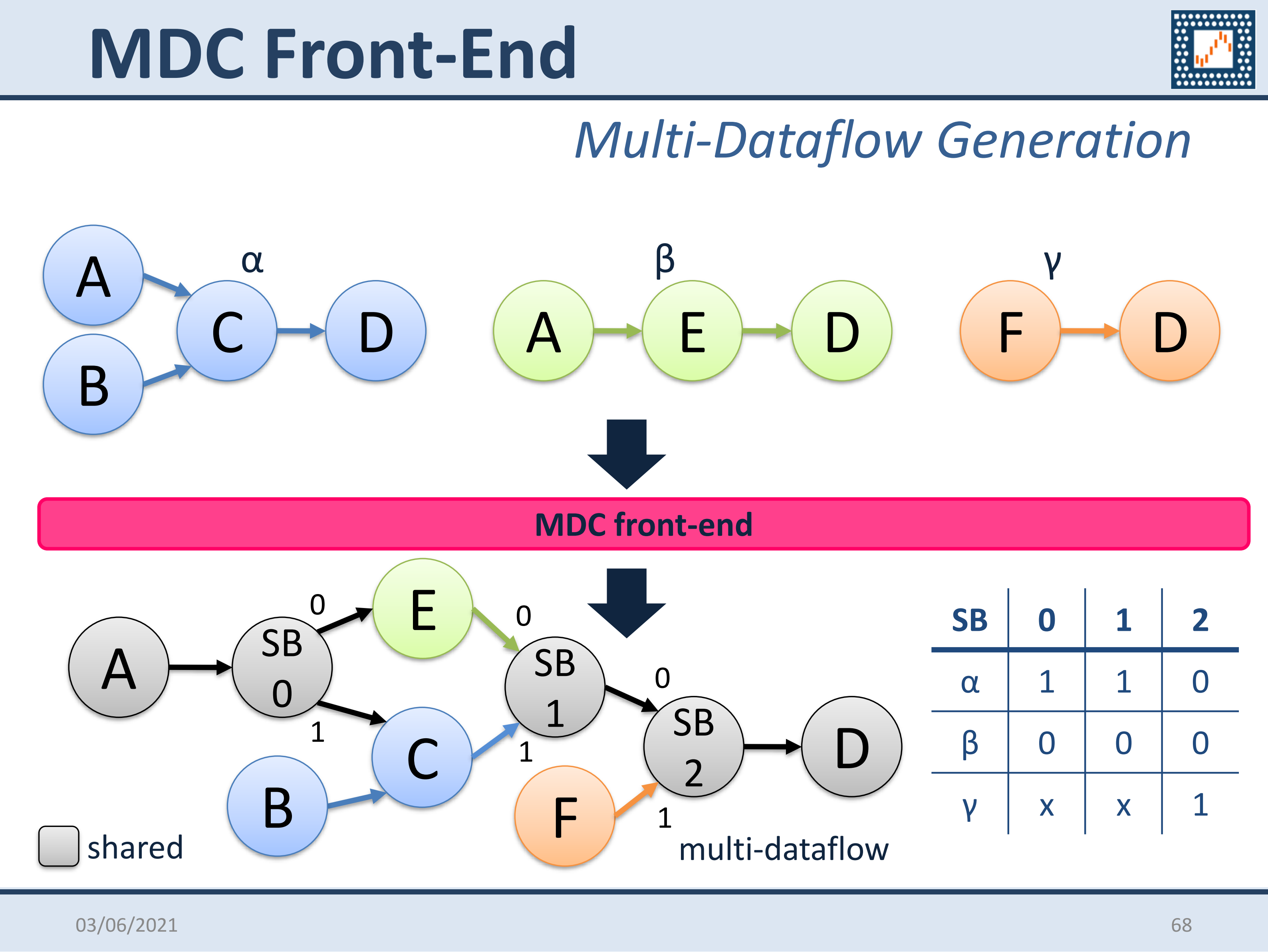
Baseline: Dataflow to HW

Dataflow to Hardware

03/06/2021

67

©MECO.net



MDC Front-End

Multi-Dataflow Generation

MDC front-end

☐ shared

multi-dataflow

SB	0	1	2
α	1	1	0
β	0	0	0
γ	x	x	1

03/06/2021

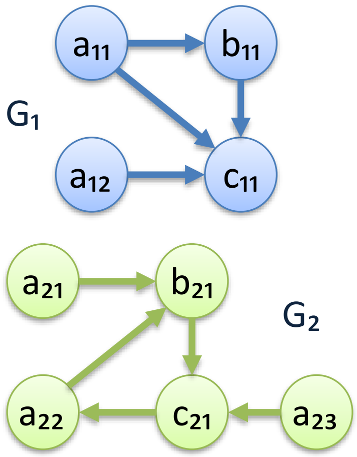
68

MDC Front-End

Datapath Merging Problem: Graph Model

GRAPHS

$G_i = (V_i, E_i)$

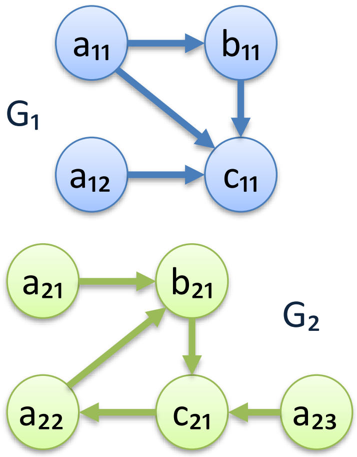


MDC Front-End

Datapath Merging Problem: Graph Model

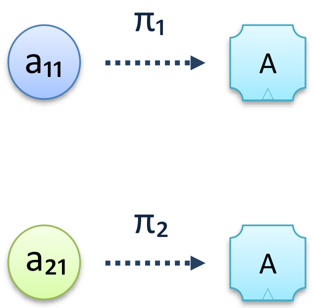
GRAPHS

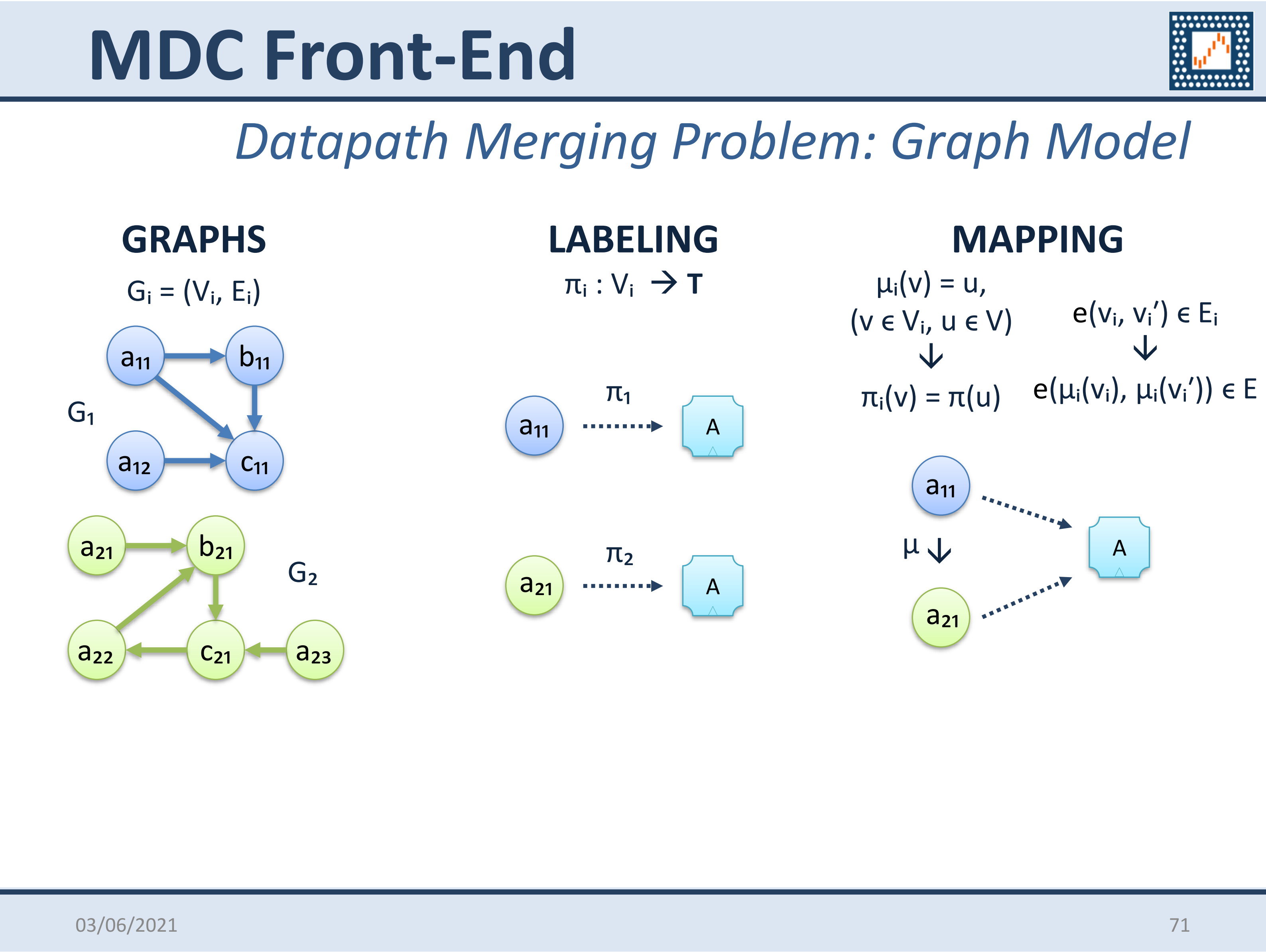
$G_i = (V_i, E_i)$



LABELING

$\pi_i : V_i \rightarrow \mathbf{T}$





MDC Front-End

Datapath Merging Problem: Graph Model

GRAPHS

$G_i = (V_i, E_i)$

LABELING

$\pi_i : V_i \rightarrow \mathbf{T}$

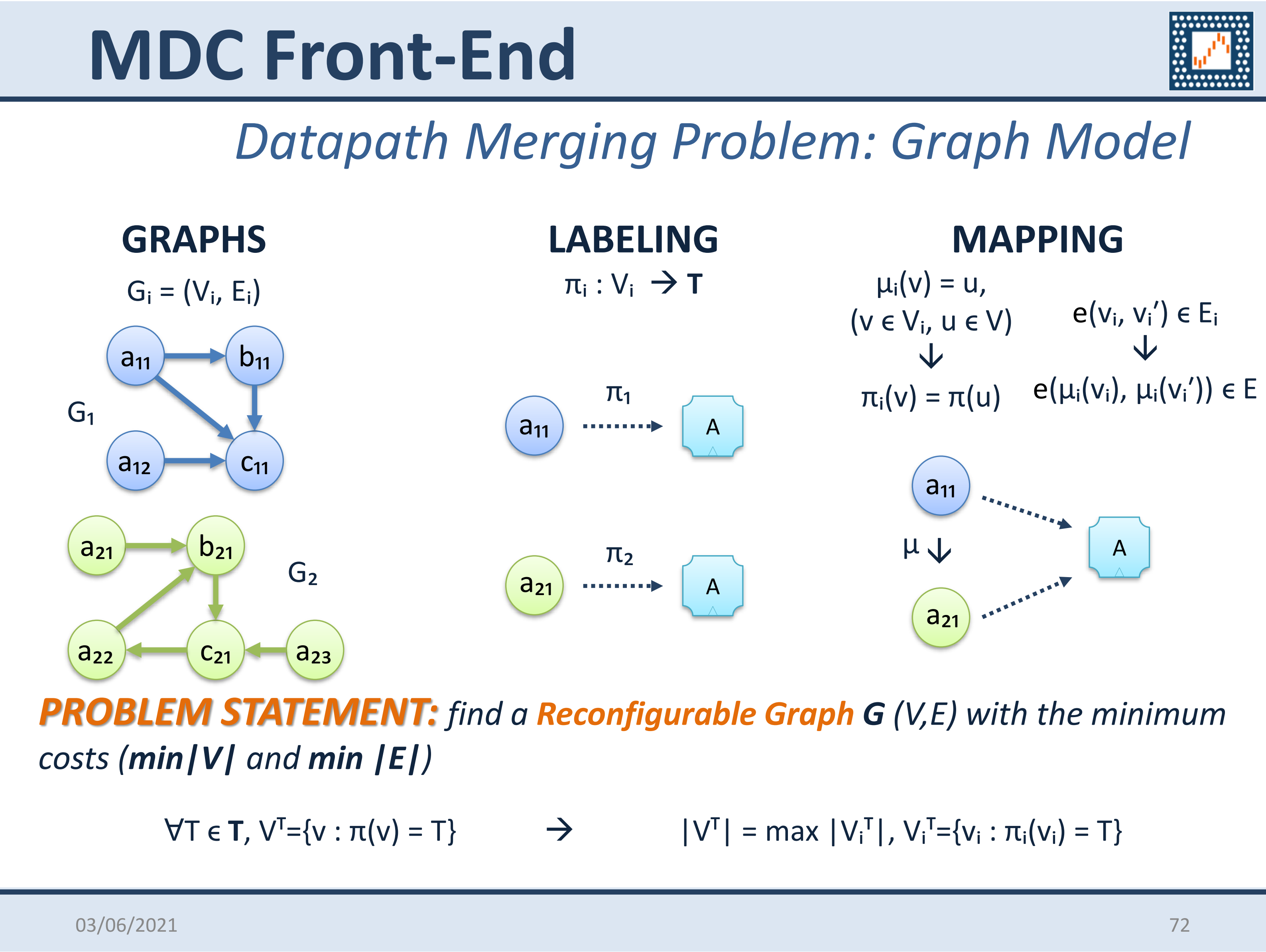
MAPPING

$\mu_i(v) = u,$
$(v \in V_i, u \in V)$
$\downarrow$
$\pi_i(v) = \pi(u)$

$e(v_i, v_i') \in E_i$
$\downarrow$
$e(\mu_i(v_i), \mu_i(v_i')) \in E$

03/06/2021

71



MDC Front-End

Datapath Merging Problem: Graph Model

GRAPHS

$G_i = (V_i, E_i)$

LABELING

$\pi_i : V_i \rightarrow \mathbf{T}$

MAPPING

$\mu_i(v) = u,$
$(v \in V_i, u \in V)$
$\downarrow$
$\pi_i(v) = \pi(u)$

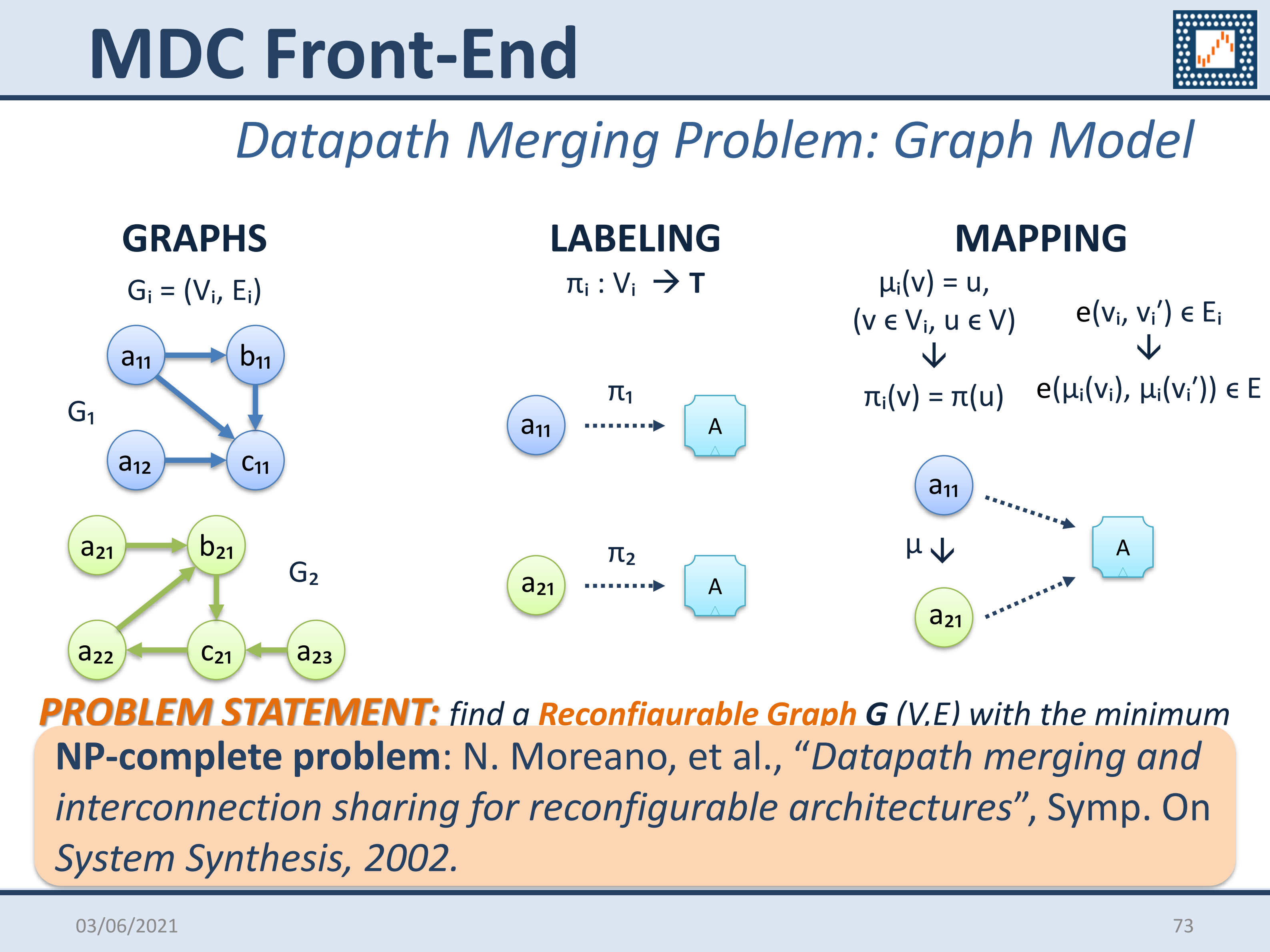
$e(v_i, v_i') \in E_i$
$\downarrow$
$e(\mu_i(v_i), \mu_i(v_i')) \in E$

PROBLEM STATEMENT: *find a* ***Reconfigurable Graph G*** *(V,E) with the minimum costs (**min|V|** and **min |E|**)*

$\forall T \in \mathbf{T}, V^T=\{v : \pi(v) = T\}$ → $|V^T| = \max |V_i^T|, V_i^T=\{v_i : \pi_i(v_i) = T\}$

03/06/2021 72

©MECO.net



MDC Front-End

Datapath Merging Problem: Graph Model

GRAPHS

$G_i = (V_i, E_i)$

LABELING

$\pi_i : V_i \rightarrow \mathbf{T}$

MAPPING

$\mu_i(v) = u,$
$(v \in V_i, u \in V)$
$\downarrow$
$\pi_i(v) = \pi(u)$

$e(v_i, v_i') \in E_i$
$\downarrow$
$e(\mu_i(v_i), \mu_i(v_i')) \in E$

PROBLEM STATEMENT: *find a* ***Reconfigurable Graph*** ***G*** *(V,E) with the minimum*

NP-complete problem: N. Moreano, et al., "*Datapath merging and interconnection sharing for reconfigurable architectures*", Symp. On *System Synthesis, 2002.*

03/06/2021

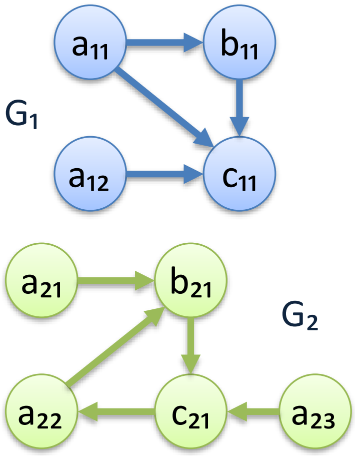
73

Datapath Merging Problem

Moreano Algorithm

merging $\mathbf{G_1 = (V_1, E_1)}$ and $\mathbf{G_2 = (V_2, E_2)}$

FEASIBLE EDGE MAPPING between $\{e_1(u,v),e_2(w,z)\}$ in E_1xE_2, where $u,v \in V_1$ and $w,z \in V_2$, if: $\pi_1(u) = \pi_2(w)$ and $\pi_1(v) = \pi_2(z)$



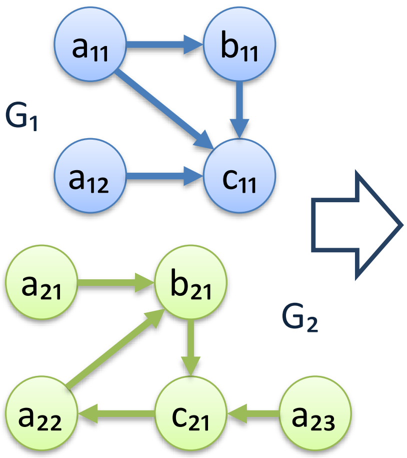
GRAPHS

Datapath Merging Problem

Moreano Algorithm

merging $\mathbf{G_1 = (V_1, E_1)}$ and $\mathbf{G_2 = (V_2, E_2)}$

FEASIBLE EDGE MAPPING between $\mathbf{\{e_1(u,v),e_2(w,z)\}}$ in $\mathbf{E_1xE_2}$, where $\mathbf{u,v \in V_1}$ and $\mathbf{w,z \in V_2}$, if: $\mathbf{\pi_1(u) = \pi_2(w)}$ and $\mathbf{\pi_1(v) = \pi_2 (z)}$



$a_{11}b_{11}$
$a_{21}b_{21}$

$a_{11}c_{11}$
$a_{23}c_{21}$

$b_{11}c_{11}$
$b_{21}c_{21}$

$a_{11}b_{11}$
$a_{22}b_{21}$

$a_{12}c_{11}$
$a_{23}c_{21}$

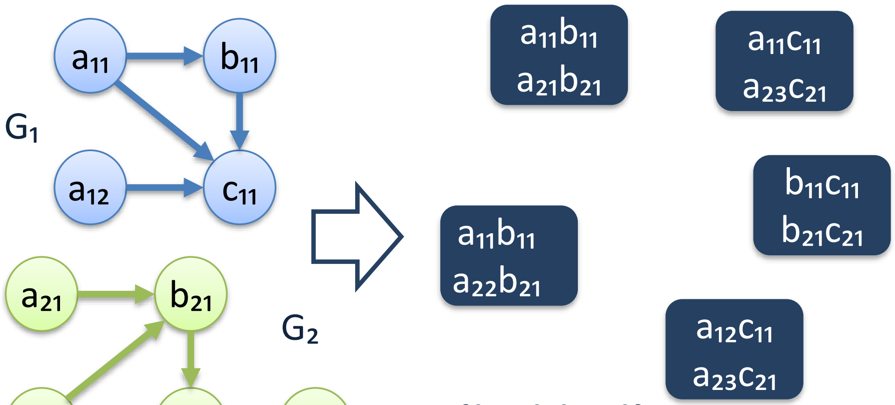
GRAPHS

Datapath Merging Problem

Moreano Algorithm

merging $\mathbf{G_1 = (V_1, E_1)}$ and $\mathbf{G_2 = (V_2, E_2)}$

FEASIBLE EDGE MAPPING between $\mathbf{\{e_1(u,v),e_2(w,z)\}}$ in $\mathbf{E_1xE_2}$, where $\mathbf{u,v \in V_1}$ and $\mathbf{w,z \in V_2}$, if: $\mathbf{\pi_1(u) = \pi_2(w)}$ and $\mathbf{\pi_1(v) = \pi_2(z)}$



$a_{11}b_{11}$ $a_{21}b_{21}$

$a_{11}c_{11}$ $a_{23}c_{21}$

$b_{11}c_{11}$ $b_{21}c_{21}$

$a_{11}b_{11}$ $a_{22}b_{21}$

$a_{12}c_{11}$ $a_{23}c_{21}$

GRAPHS

$\mathbf{\{(u,v),(w,z)\}}$ not comaptible with $\mathbf{\{(u',v'),(w',z')\}}$ if:

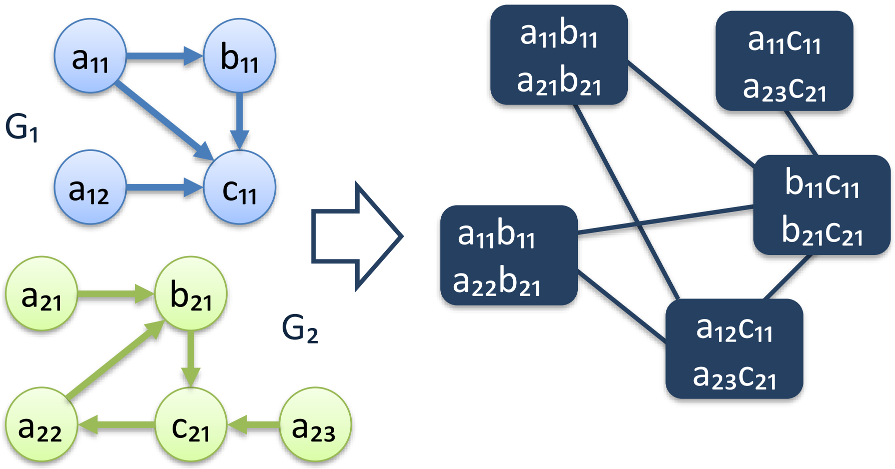
1. **u = u'** and **w ≠ w'**
2. **v = v'** and **z ≠ z'**
3. **u ≠ u'** and **w = w'**
4. **v ≠ v'** and **z = z'**

Datapath Merging Problem

Moreano Algorithm

merging **$G_1 = (V_1, E_1)$** and **$G_2 = (V_2, E_2)$**

FEASIBLE EDGE MAPPING between **$\{e_1(u,v),e_2(w,z)\}$** in **E_1xE_2**, where **$u,v \in V_1$** and **$w,z \in V_2$**, if: **$\pi_1(u) = \pi_2(w)$** and **$\pi_1(v) = \pi_2(z)$**


a_{11}
b_{11}
G_1
a_{12}
c_{11}
a_{21}
b_{21}
G_2
a_{22}
c_{21}
a_{23}
$a_{11}b_{11}$ $a_{21}b_{21}$
$a_{11}c_{11}$ $a_{23}c_{21}$
$b_{11}c_{11}$ $b_{21}c_{21}$
$a_{11}b_{11}$ $a_{22}b_{21}$
$a_{12}c_{11}$ $a_{23}c_{21}$

GRAPHS

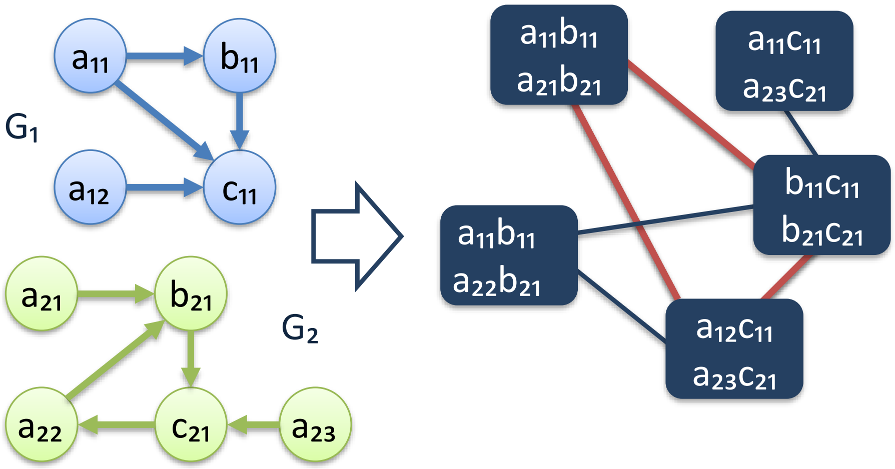
COMPATIBILITY GRAPH

Datapath Merging Problem

Moreano Algorithm

merging $\mathbf{G_1 = (V_1, E_1)}$ and $\mathbf{G_2 = (V_2, E_2)}$

FEASIBLE EDGE MAPPING between $\mathbf{\{e_1(u,v),e_2(w,z)\}}$ in $\mathbf{E_1 x E_2}$, where $\mathbf{u,v \in V_1}$ and $\mathbf{w,z \in V_2}$, if: $\mathbf{\pi_1(u) = \pi_2(w)}$ and $\mathbf{\pi_1(v) = \pi_2(z)}$



G_1
a_{11}
b_{11}
a_{12}
c_{11}
a_{21}
b_{21}
G_2
a_{22}
c_{21}
a_{23}
$a_{11}b_{11}$ $a_{21}b_{21}$
$a_{11}c_{11}$ $a_{23}c_{21}$
$b_{11}c_{11}$ $b_{21}c_{21}$
$a_{11}b_{11}$ $a_{22}b_{21}$
$a_{12}c_{11}$ $a_{23}c_{21}$

GRAPHS

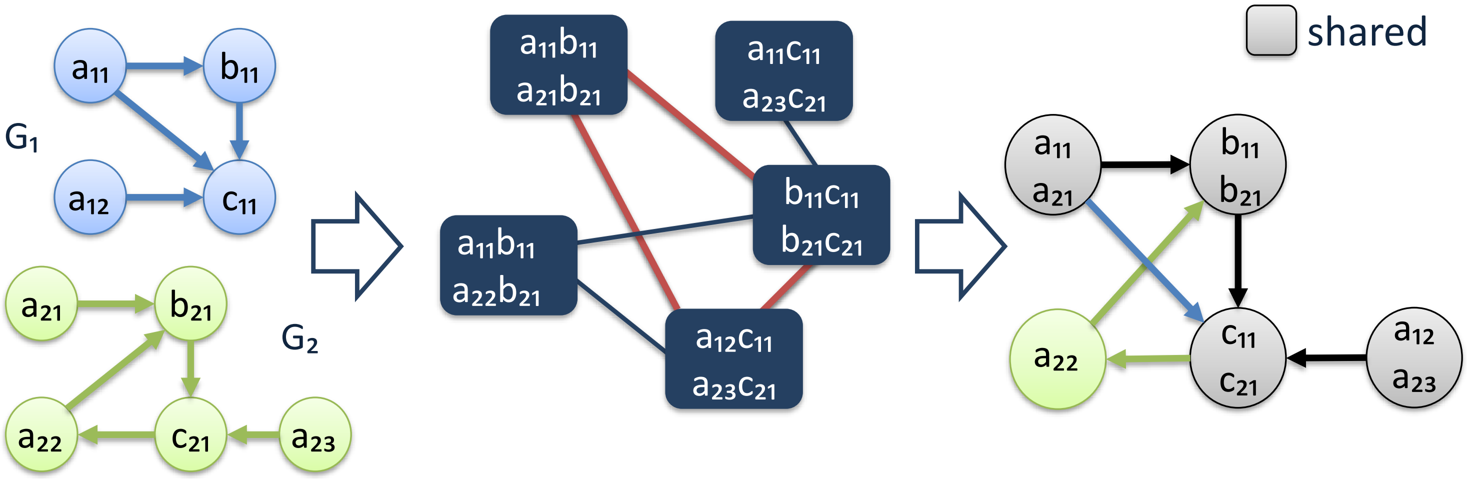
maximum clique on COMPATIBILITY GRAPH

Datapath Merging Problem

Moreano Algorithm

merging **$G_1 = (V_1, E_1)$** and **$G_2 = (V_2, E_2)$**

FEASIBLE EDGE MAPPING between **$\{e_1(u,v),e_2(w,z)\}$** in **E_1xE_2**, where **$u,v \in V_1$** and **$w,z \in V_2$**, if: **$\pi_1(u) = \pi_2(w)$** and **$\pi_1(v) = \pi_2(z)$**



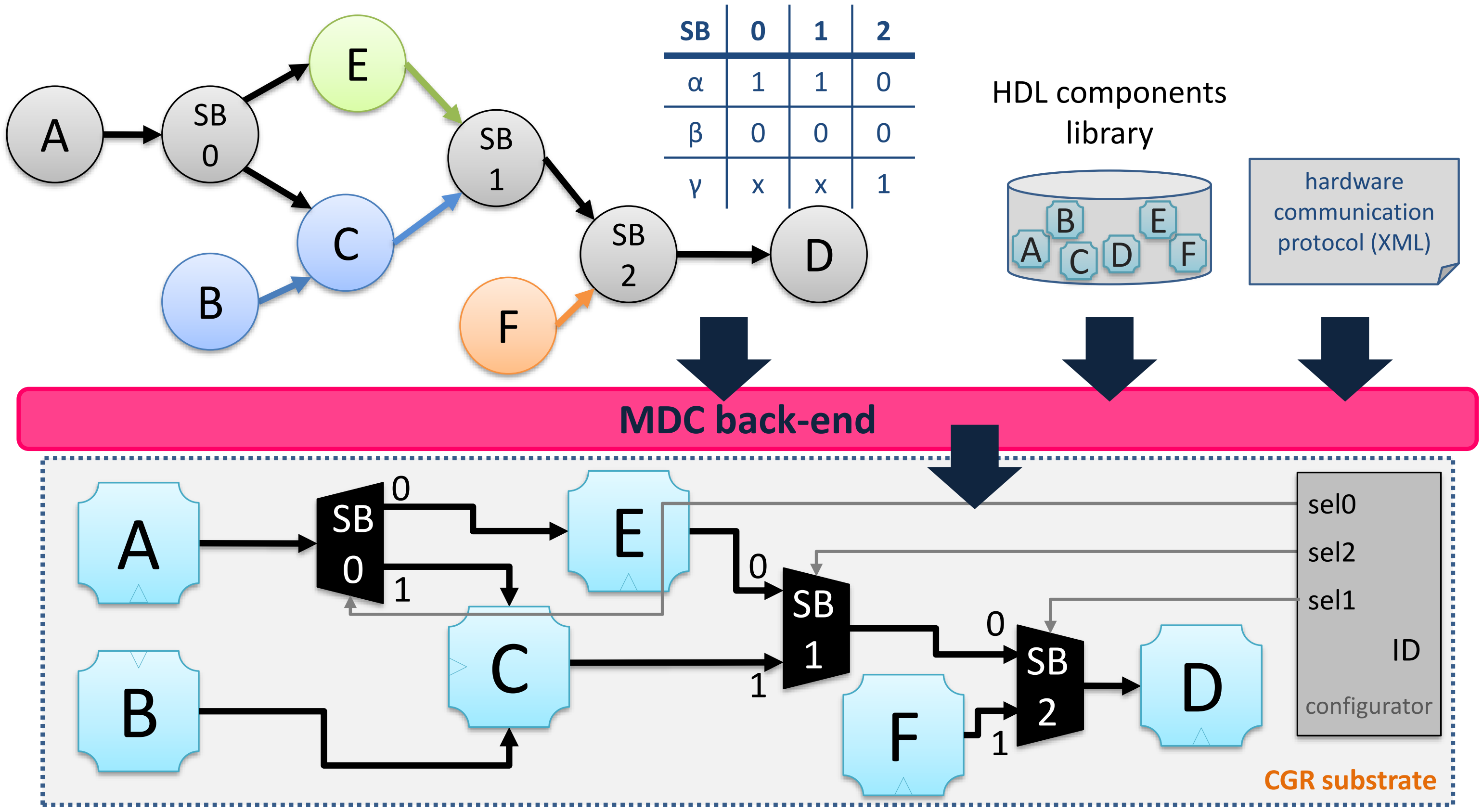
GRAPHS

maximum clique on COMPATIBILITY GRAPH

RECONFIGURABLE GRAPH

MDC Back-End

Platform Composer



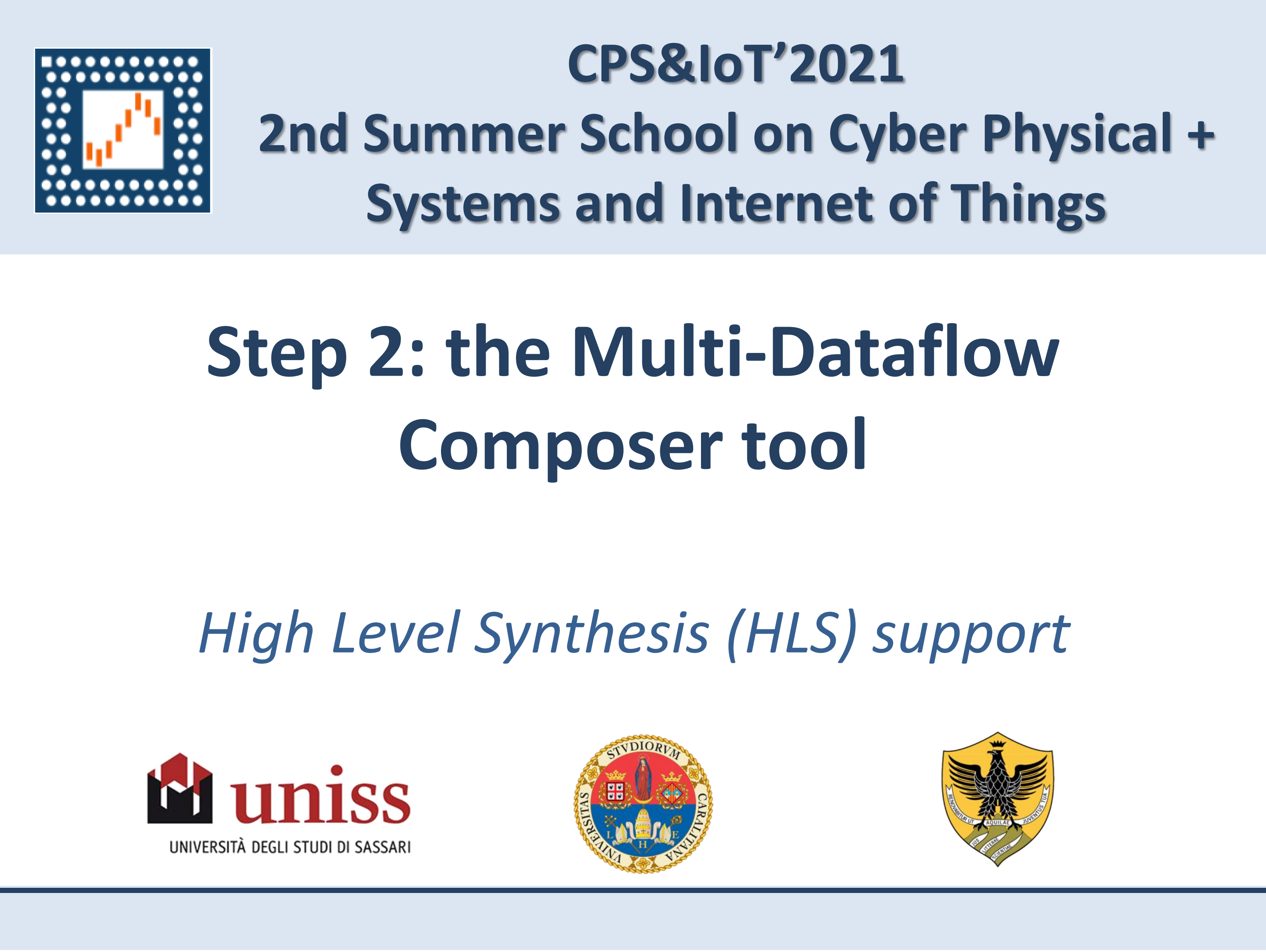
SB	0	1	2
α	1	1	0
β	0	0	0
γ	x	x	1

HDL components library

hardware communication protocol (XML)

MDC back-end

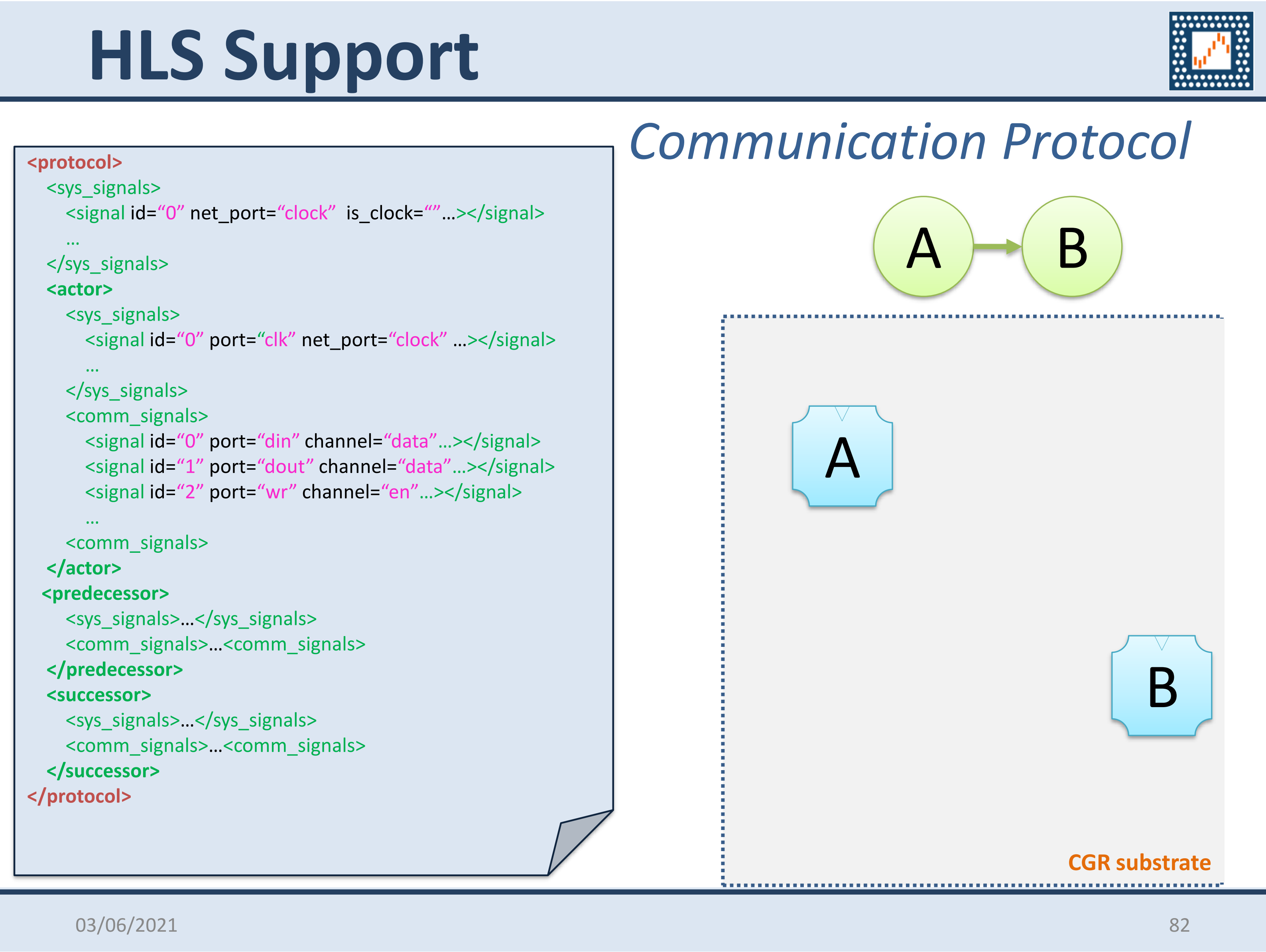
CGR substrate



CPS&IoT'2021
2nd Summer School on Cyber Physical +
Systems and Internet of Things

Step 2: the Multi-Dataflow Composer tool

High Level Synthesis (HLS) support

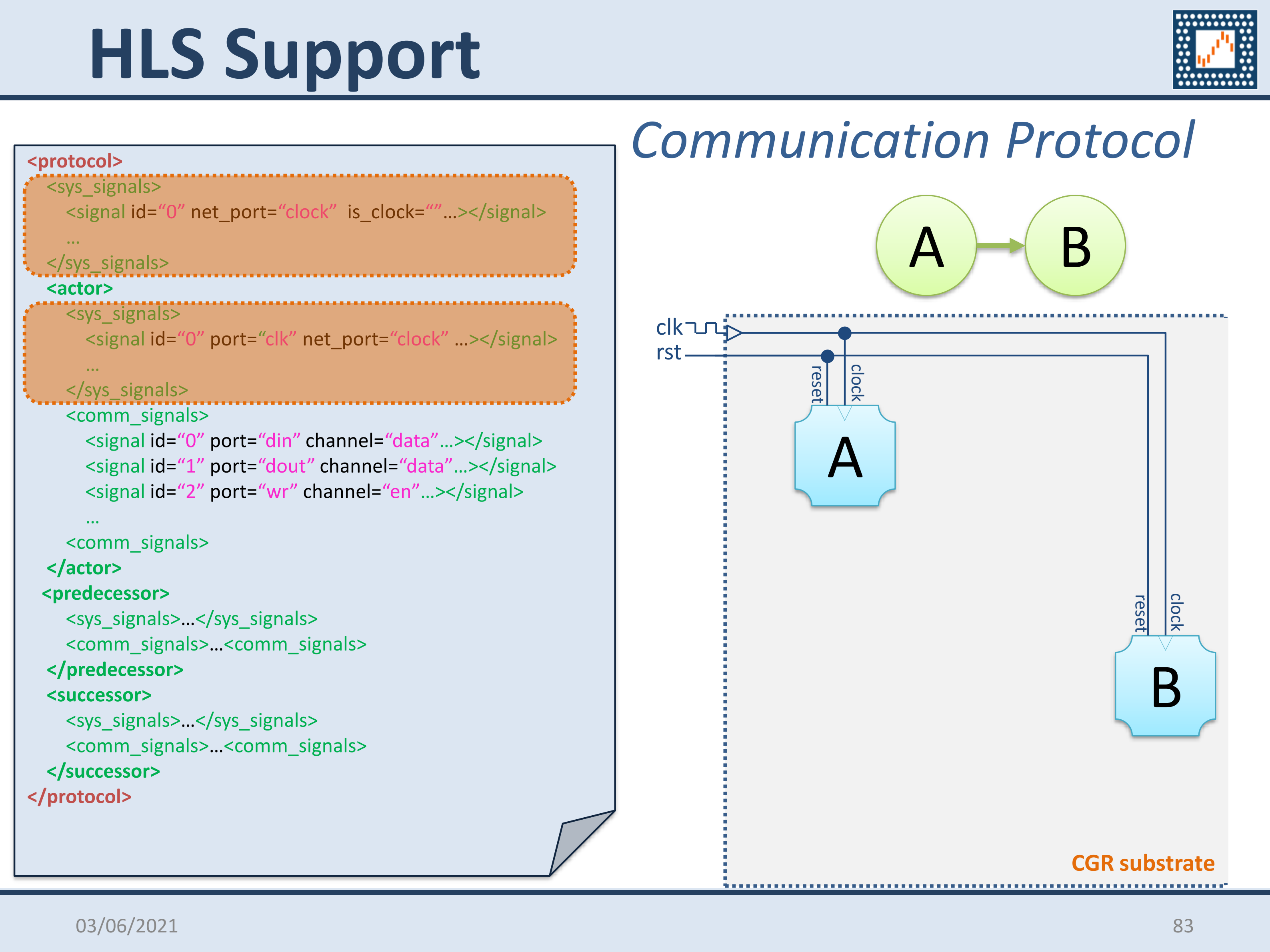


HLS Support

Communication Protocol

```
<protocol>
  <sys_signals>
    <signal id="0" net_port="clock"  is_clock=""…></signal>
    …
  </sys_signals>
  <actor>
    <sys_signals>
      <signal id="0" port="clk" net_port="clock" …></signal>
      …
    </sys_signals>
    <comm_signals>
      <signal id="0" port="din" channel="data"…></signal>
      <signal id="1" port="dout" channel="data"…></signal>
      <signal id="2" port="wr" channel="en"…></signal>
      …
    <comm_signals>
  </actor>
  <predecessor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </predecessor>
  <successor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </successor>
</protocol>
```

A
B
A
B
CGR substrate



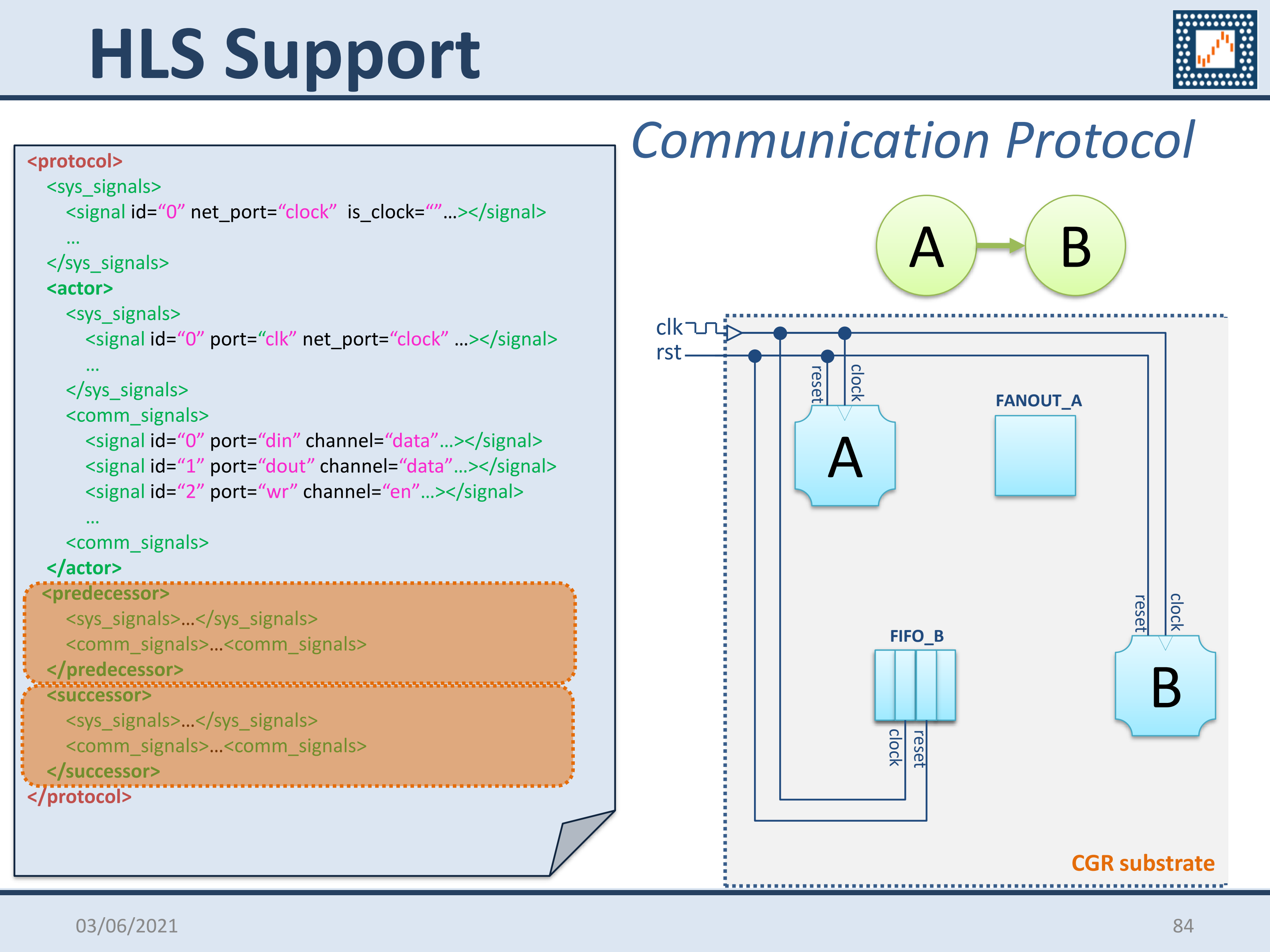
HLS Support

Communication Protocol

```
<protocol>
  <sys_signals>
    <signal id="0" net_port="clock"  is_clock=""…></signal>
    …
  </sys_signals>
  <actor>
    <sys_signals>
      <signal id="0" port="clk" net_port="clock" …></signal>
      …
    </sys_signals>
    <comm_signals>
      <signal id="0" port="din" channel="data"…></signal>
      <signal id="1" port="dout" channel="data"…></signal>
      <signal id="2" port="wr" channel="en"…></signal>
      …
    <comm_signals>
  </actor>
 <predecessor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </predecessor>
  <successor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </successor>
</protocol>
```

03/06/2021

83



HLS Support

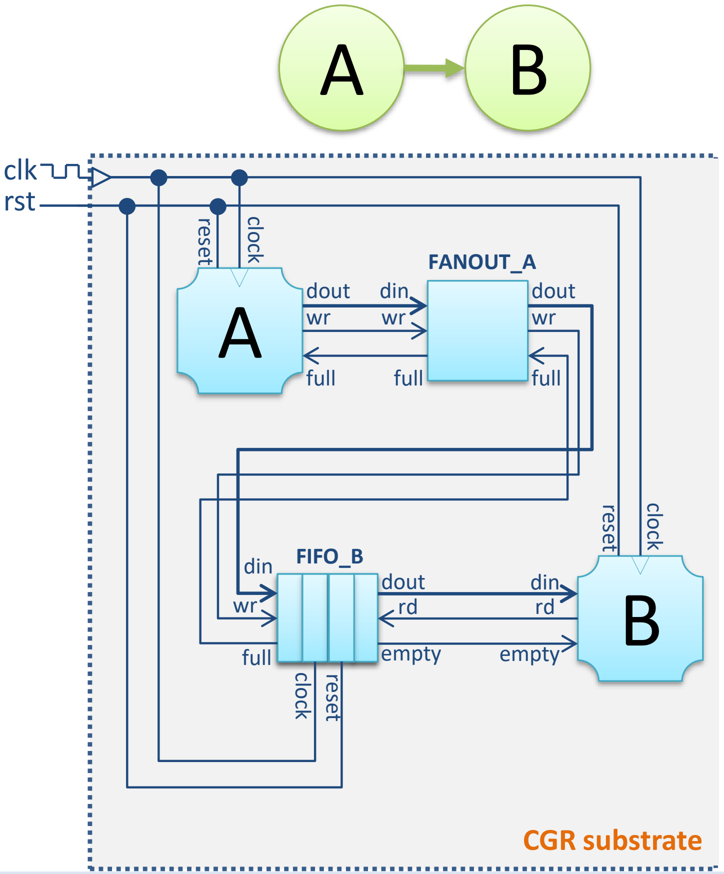
Communication Protocol

```
<protocol>
  <sys_signals>
    <signal id=“0” net_port=“clock”  is_clock=“”…></signal>
    …
  </sys_signals>
  <actor>
    <sys_signals>
      <signal id=“0” port=“clk” net_port=“clock” …></signal>
      …
    </sys_signals>
    <comm_signals>
      <signal id=“0” port=“din” channel=“data”…></signal>
      <signal id=“1” port=“dout” channel=“data”…></signal>
      <signal id=“2” port=“wr” channel=“en”…></signal>
      …
    <comm_signals>
  </actor>
  <predecessor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </predecessor>
  <successor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </successor>
</protocol>
```

HLS Support

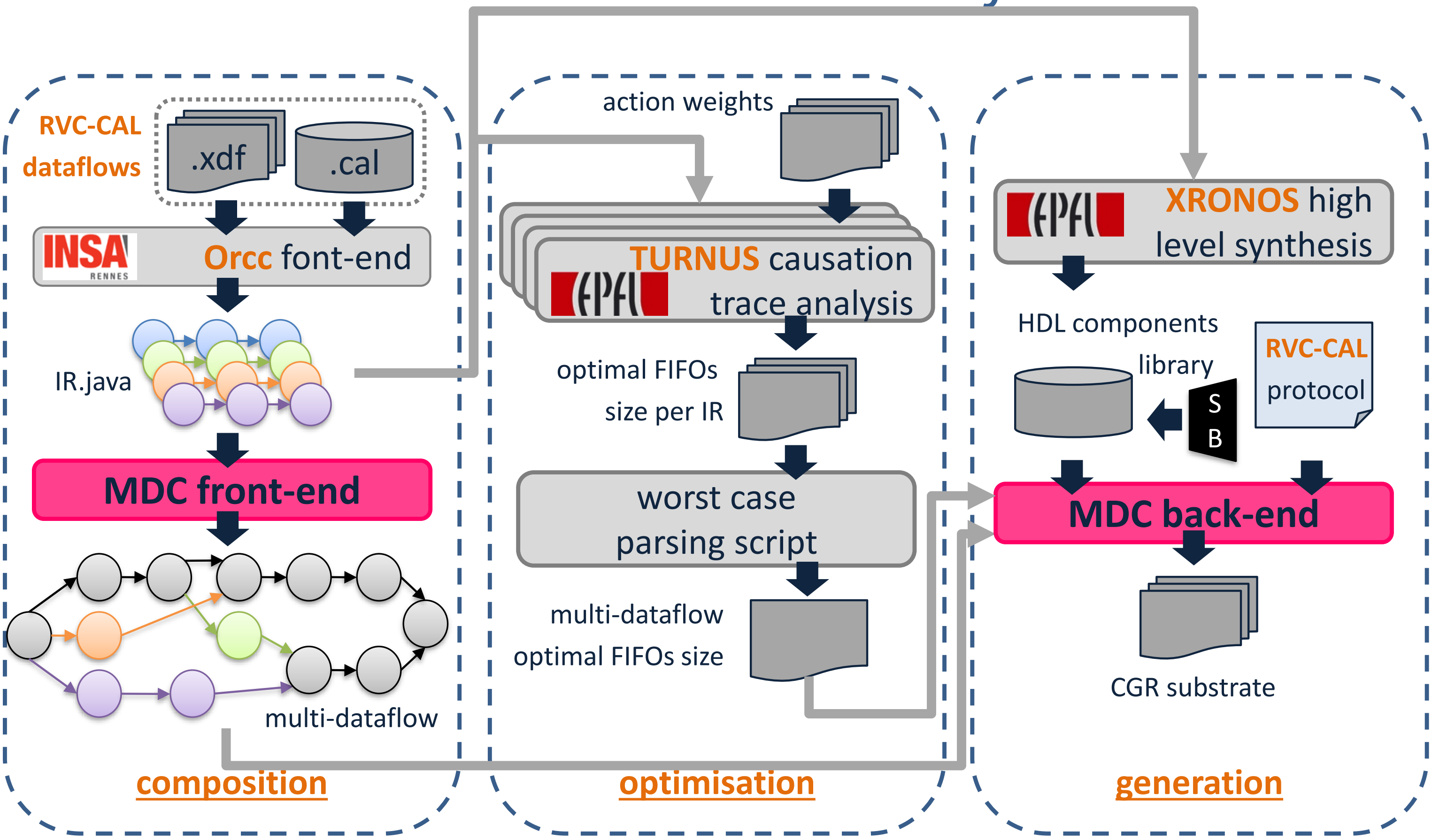
Communication Protocol

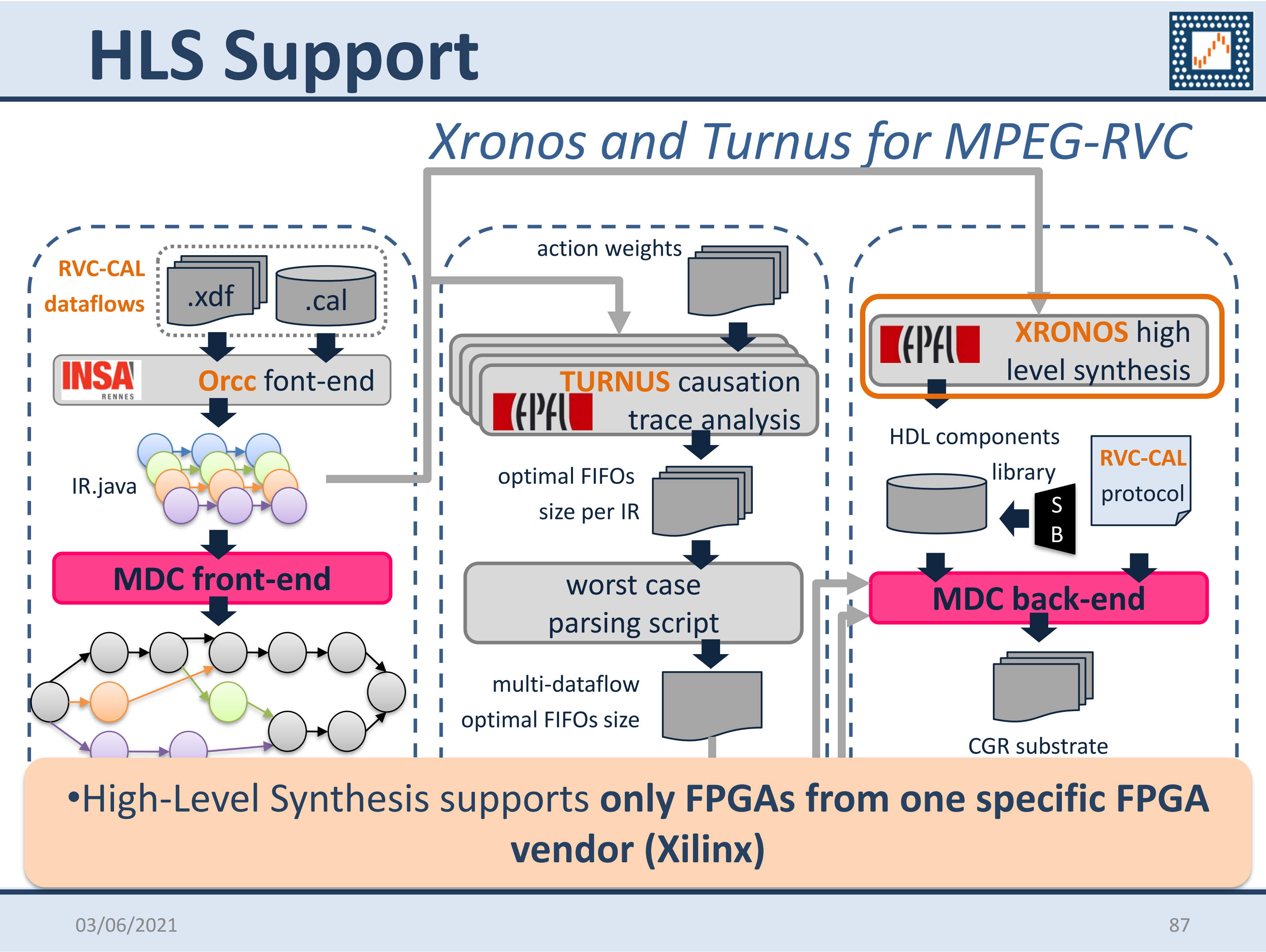
```
<protocol>
  <sys_signals>
    <signal id="0" net_port="clock"  is_clock=""…></signal>
    …
  </sys_signals>
  <actor>
    <sys_signals>
      <signal id="0" port="clk" net_port="clock" …></signal>
      …
    </sys_signals>
    <comm_signals>
      <signal id="0" port="din" channel="data"…></signal>
      <signal id="1" port="dout" channel="data"…></signal>
      <signal id="2" port="wr" channel="en"…></signal>
      …
    <comm_signals>
  </actor>
 <predecessor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </predecessor>
  <successor>
    <sys_signals>…</sys_signals>
    <comm_signals>…<comm_signals>
  </successor>
</protocol>
```



HLS Support

Xronos and Turnus for MPEG-RVC





HLS Support

Xronos and Turnus for MPEG-RVC

- High-Level Synthesis supports **only FPGAs from one specific FPGA vendor (Xilinx)**

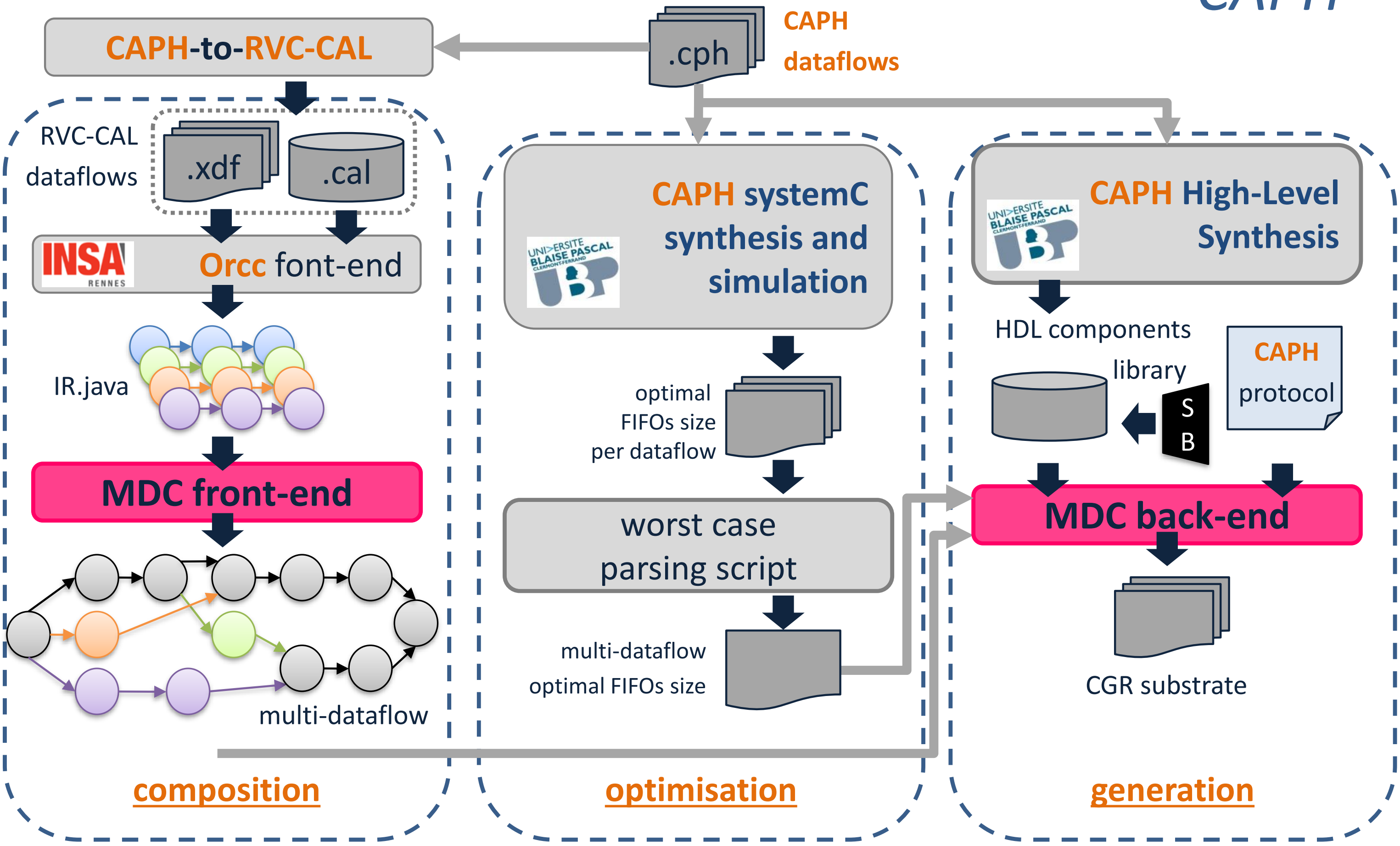
03/06/2021

87

©MECO.net

HLS Support

CAPH



CAPH-to-RVC-CAL

.cph

CAPH dataflows

RVC-CAL dataflows

.xdf

.cal

INSA RENNES

Orcc font-end

IR.java

MDC front-end

multi-dataflow

composition

CAPH systemC synthesis and simulation

optimal FIFOs size per dataflow

worst case parsing script

multi-dataflow optimal FIFOs size

optimisation

CAPH High-Level Synthesis

HDL components library

CAPH protocol

S B

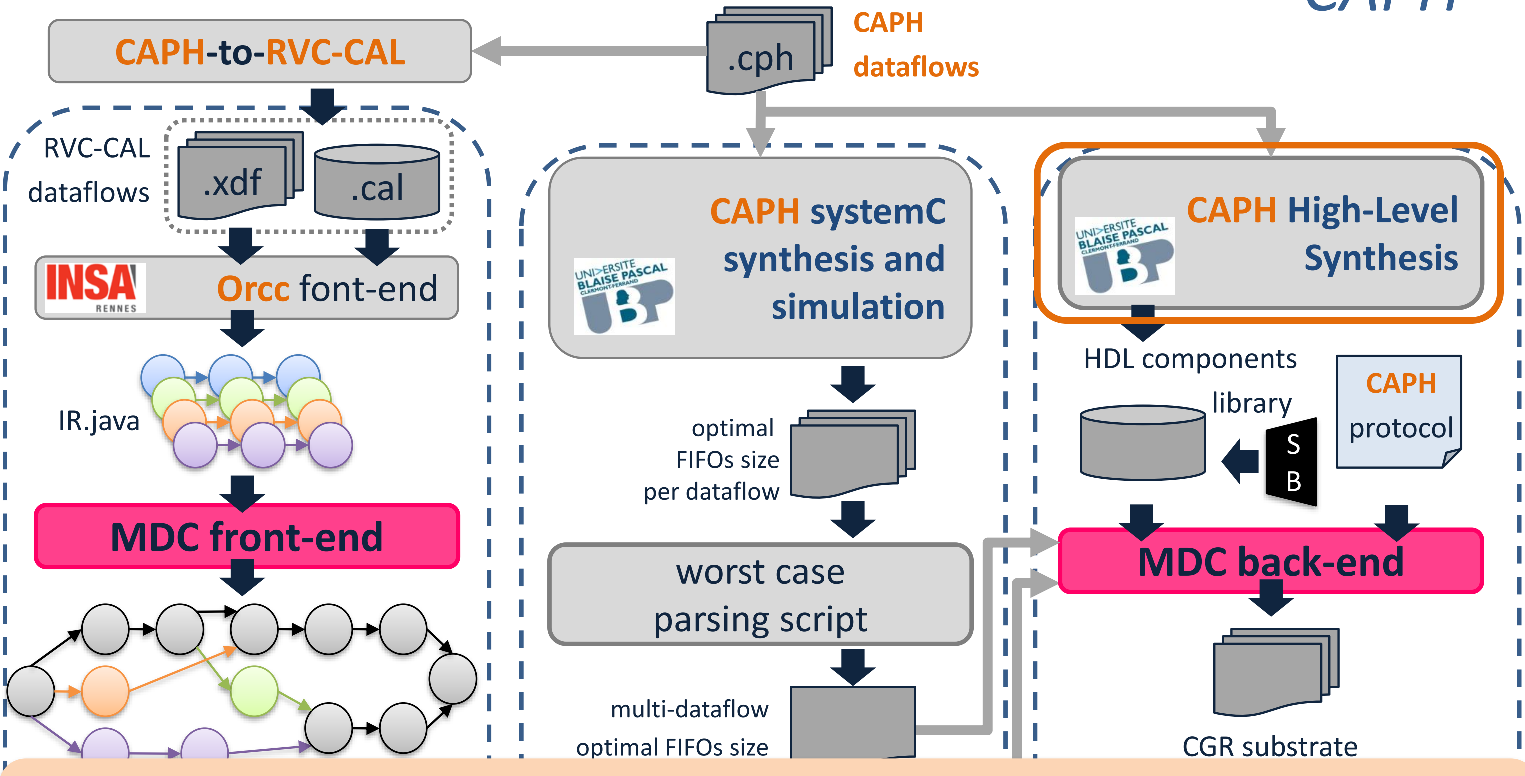
MDC back-end

CGR substrate

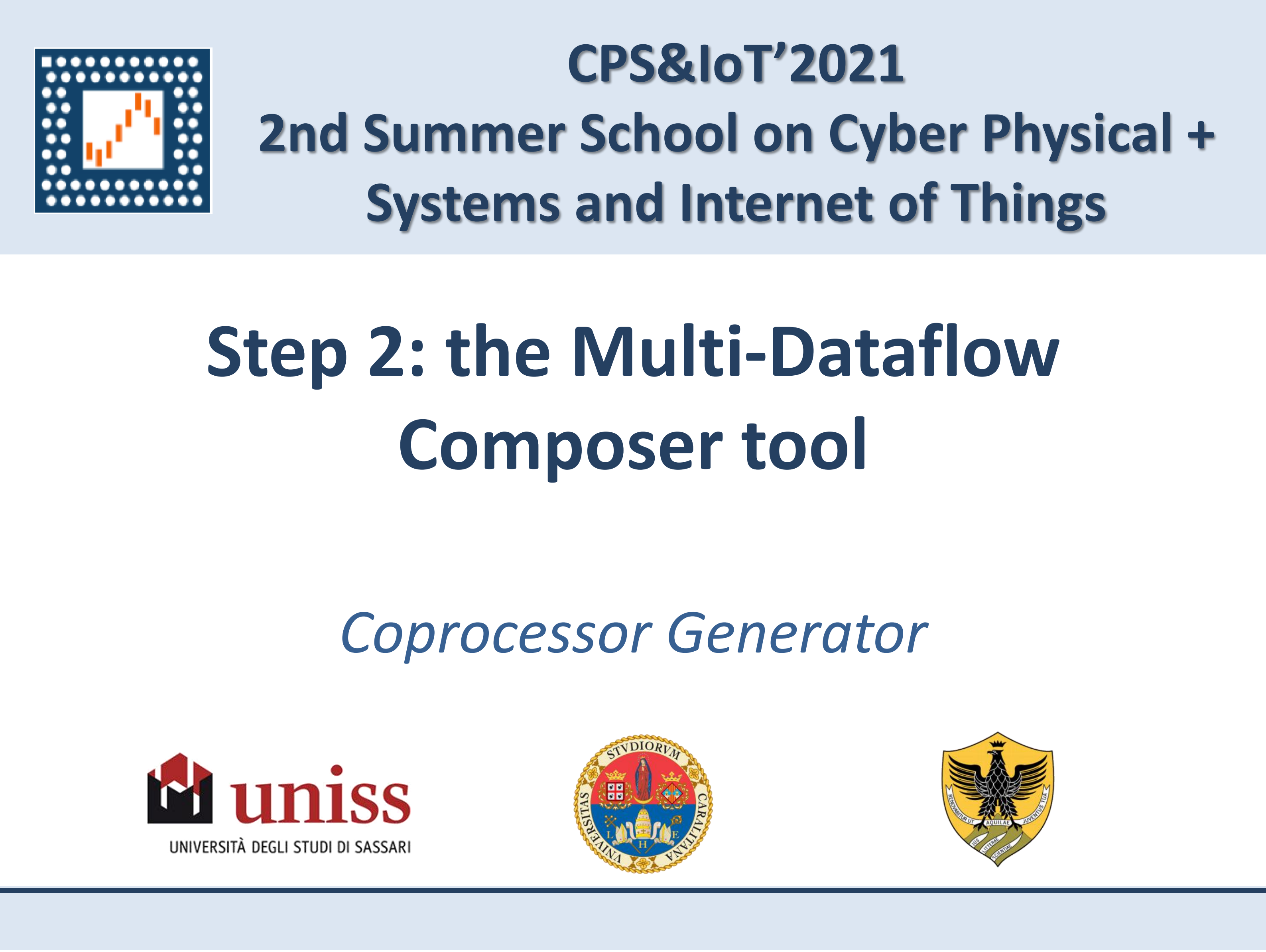
generation

HLS Support

CAPH



- **Platform Agnostic** High-Level Synthesis: it supports any kind of **FPGA** from **any vendor,** as well as **ASIC design flows**



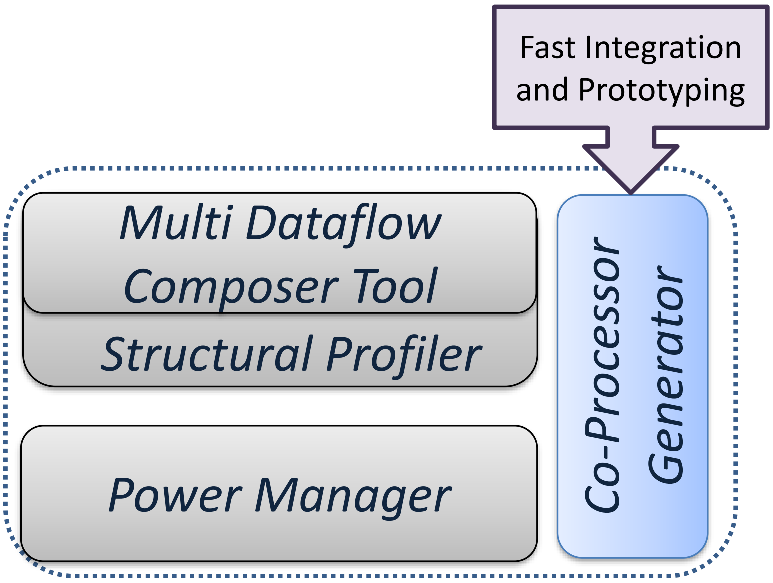
CPS&IoT'2021
2nd Summer School on Cyber Physical +
Systems and Internet of Things

Step 2: the Multi-Dataflow Composer tool

Coprocessor Generator

Co-processor Generator

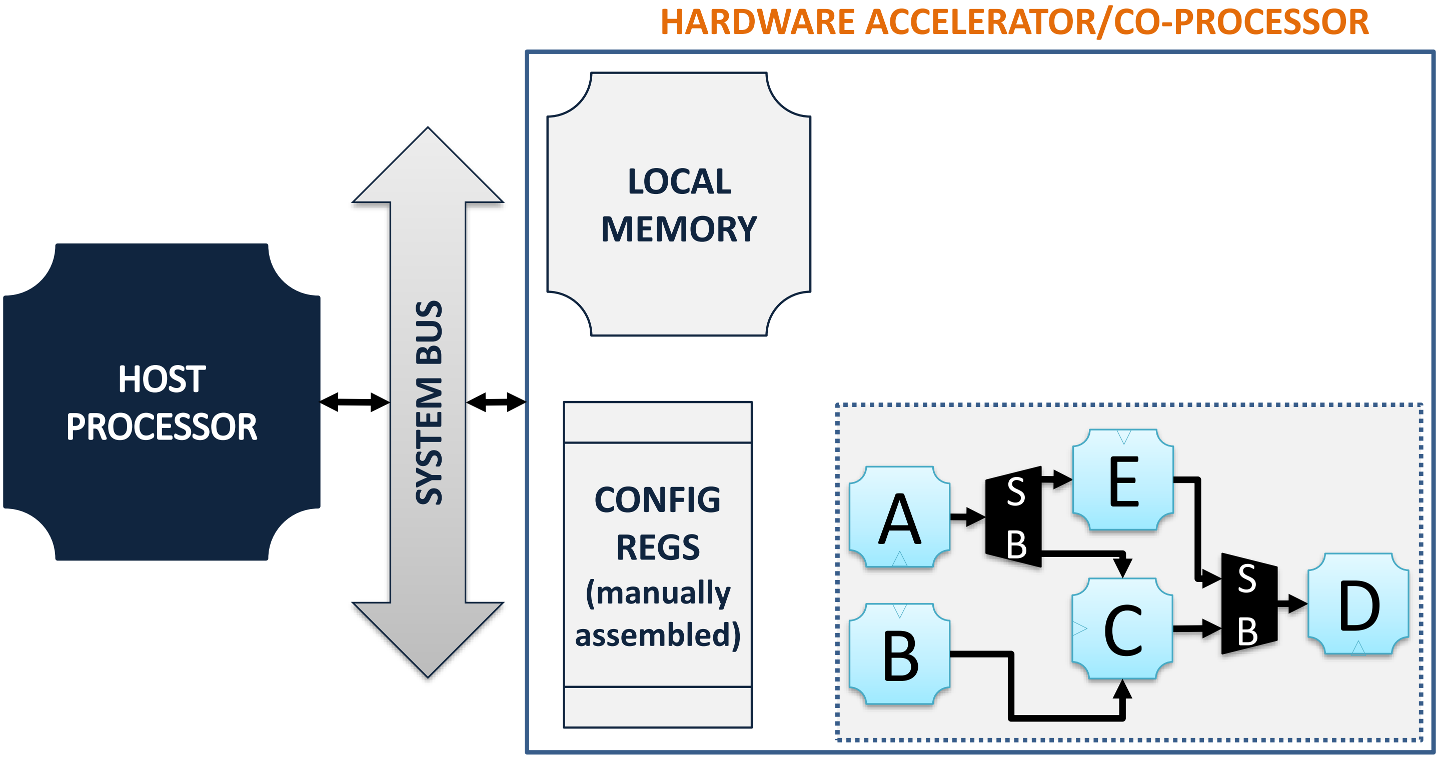
Ready to use Xilinx IPs


Fast Integration and Prototyping
Multi Dataflow Composer Tool
Structural Profiler
Power Manager
Co-Processor Generator

MDC design suite

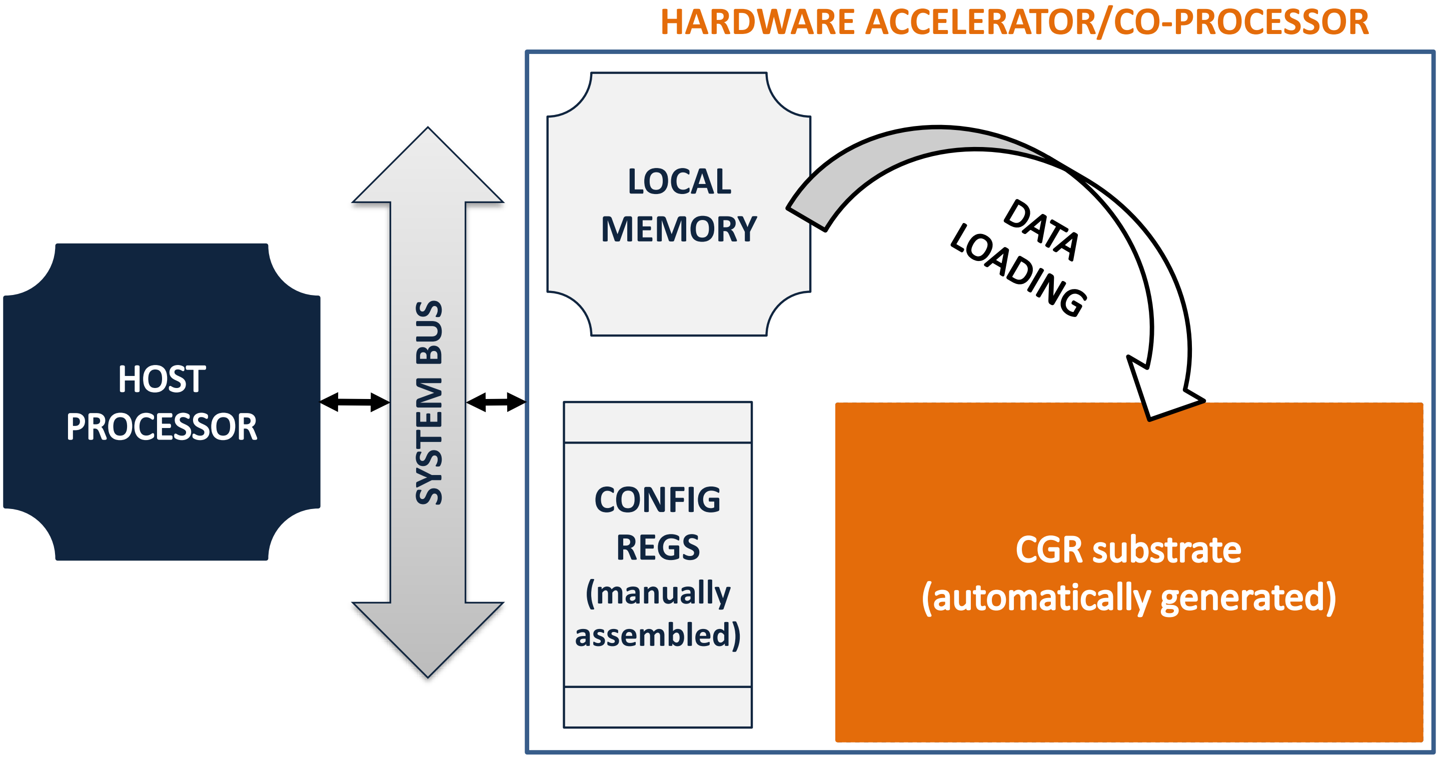
http://sites.unica.it/rpct/

Co-Processor Generator


HARDWARE ACCELERATOR/CO-PROCESSOR
LOCAL MEMORY
HOST PROCESSOR
SYSTEM BUS
CONFIG REGS (manually assembled)
A
B
SB
E
C
SB
D

03/06/2021

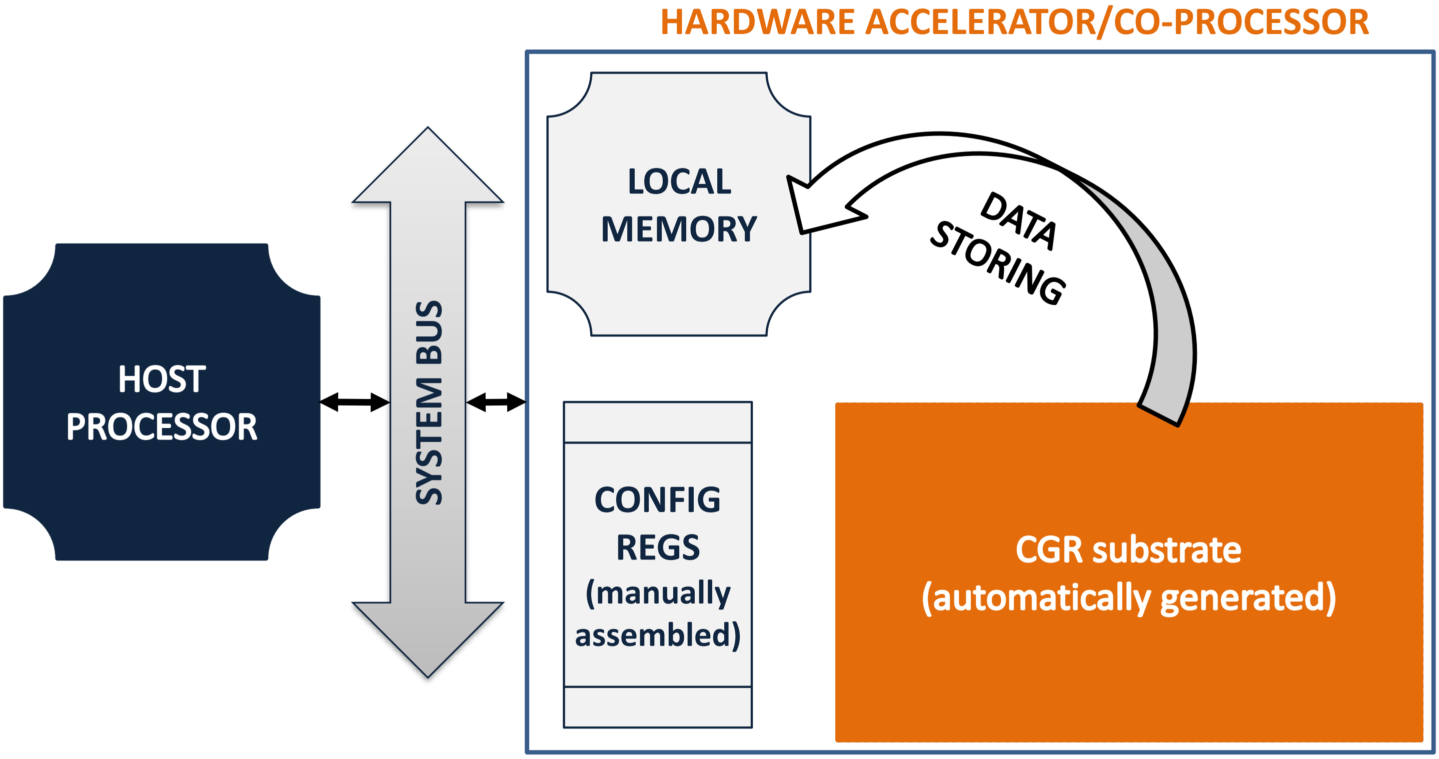
Co-Processor Generator


HARDWARE ACCELERATOR/CO-PROCESSOR
HOST PROCESSOR
SYSTEM BUS
LOCAL MEMORY
DATA LOADING
CONFIG REGS (manually assembled)
CGR substrate (automatically generated)

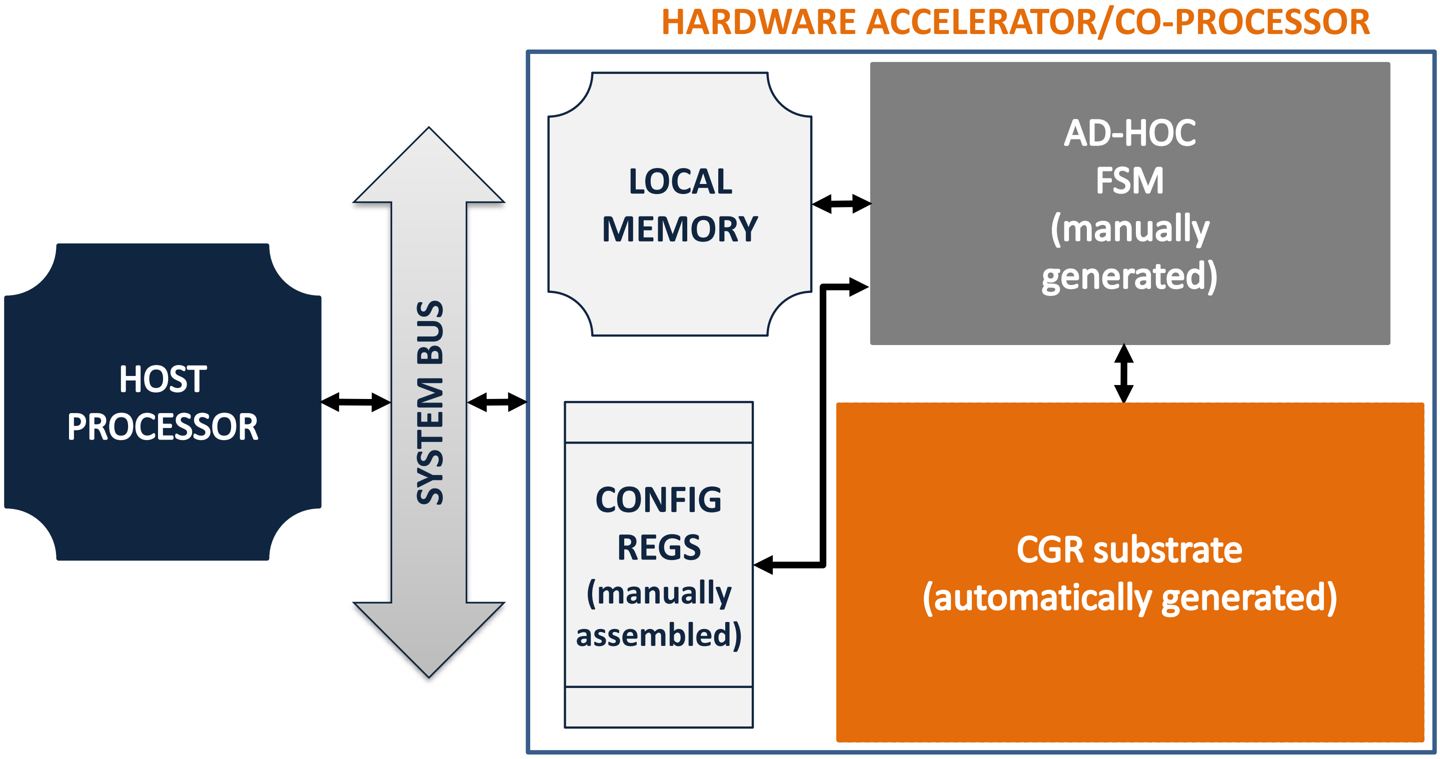
03/06/2021

93

Co-Processor Generator


HARDWARE ACCELERATOR/CO-PROCESSOR
HOST PROCESSOR
SYSTEM BUS
LOCAL MEMORY
DATA STORING
CONFIG REGS (manually assembled)
CGR substrate (automatically generated)

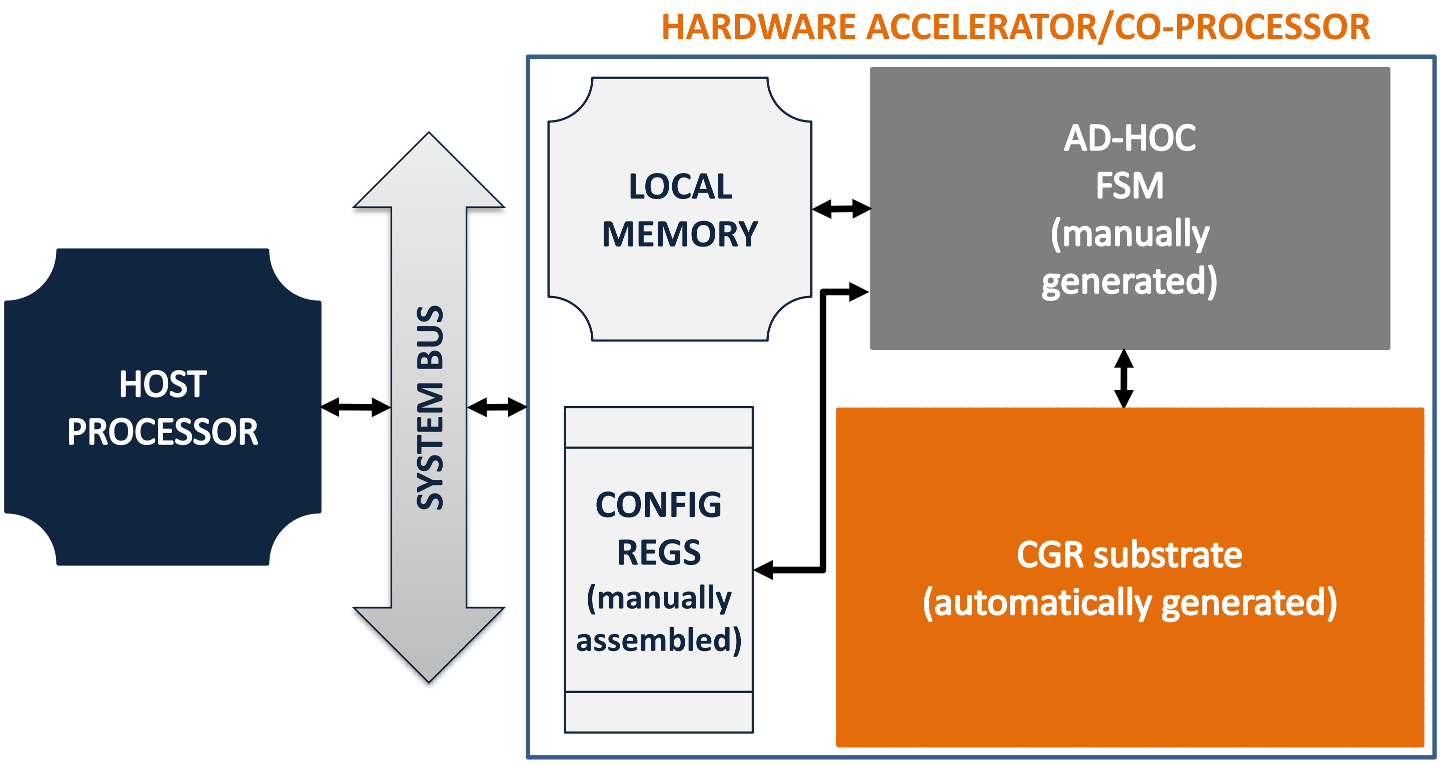
Co-Processor Generator


HARDWARE ACCELERATOR/CO-PROCESSOR
HOST PROCESSOR
SYSTEM BUS
LOCAL MEMORY
AD-HOC FSM (manually generated)
CONFIG REGS (manually assembled)
CGR substrate (automatically generated)

03/06/2021

95

Co-Processor Generator



HARDWARE ACCELERATOR/CO-PROCESSOR

HOST PROCESSOR

SYSTEM BUS

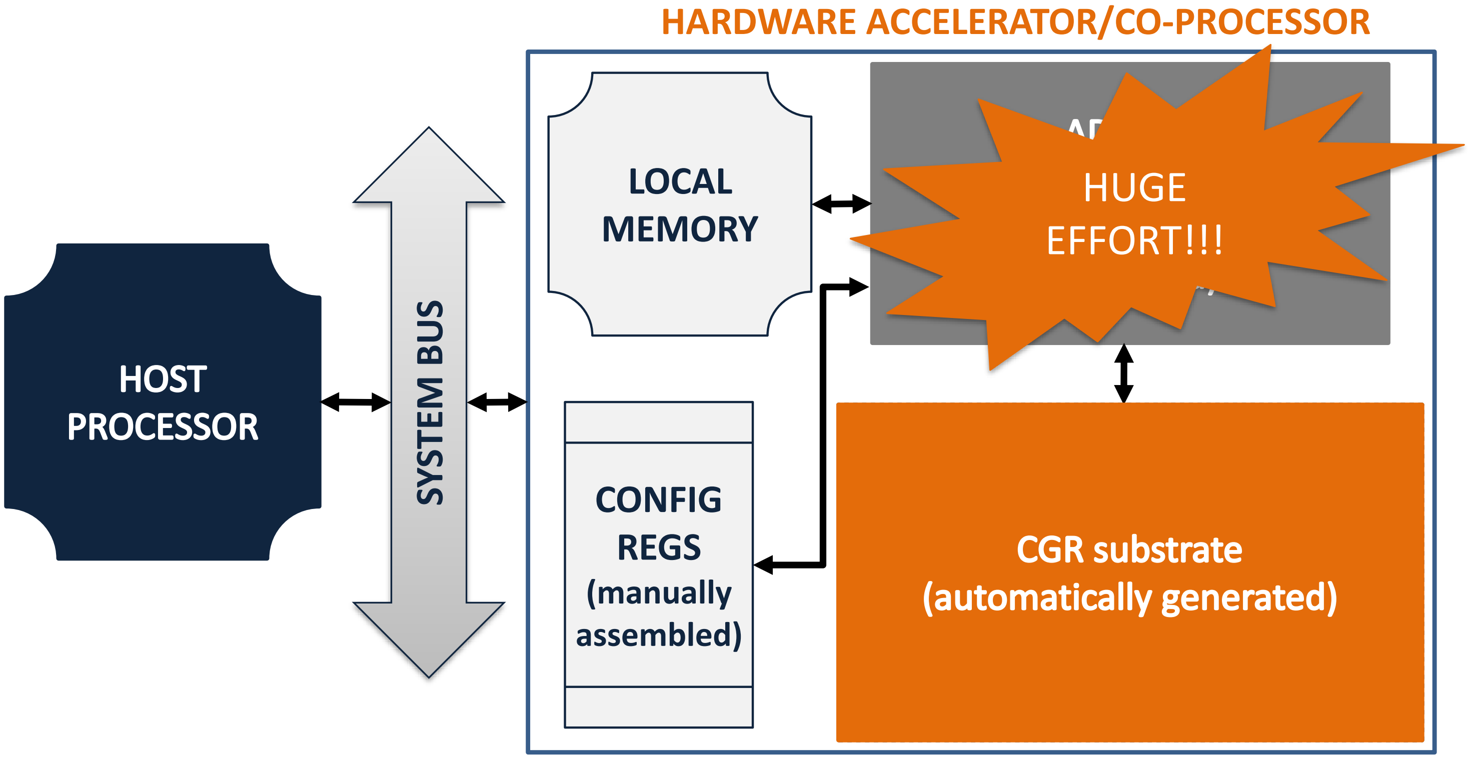
LOCAL MEMORY

AD-HOC FSM (manually generated)

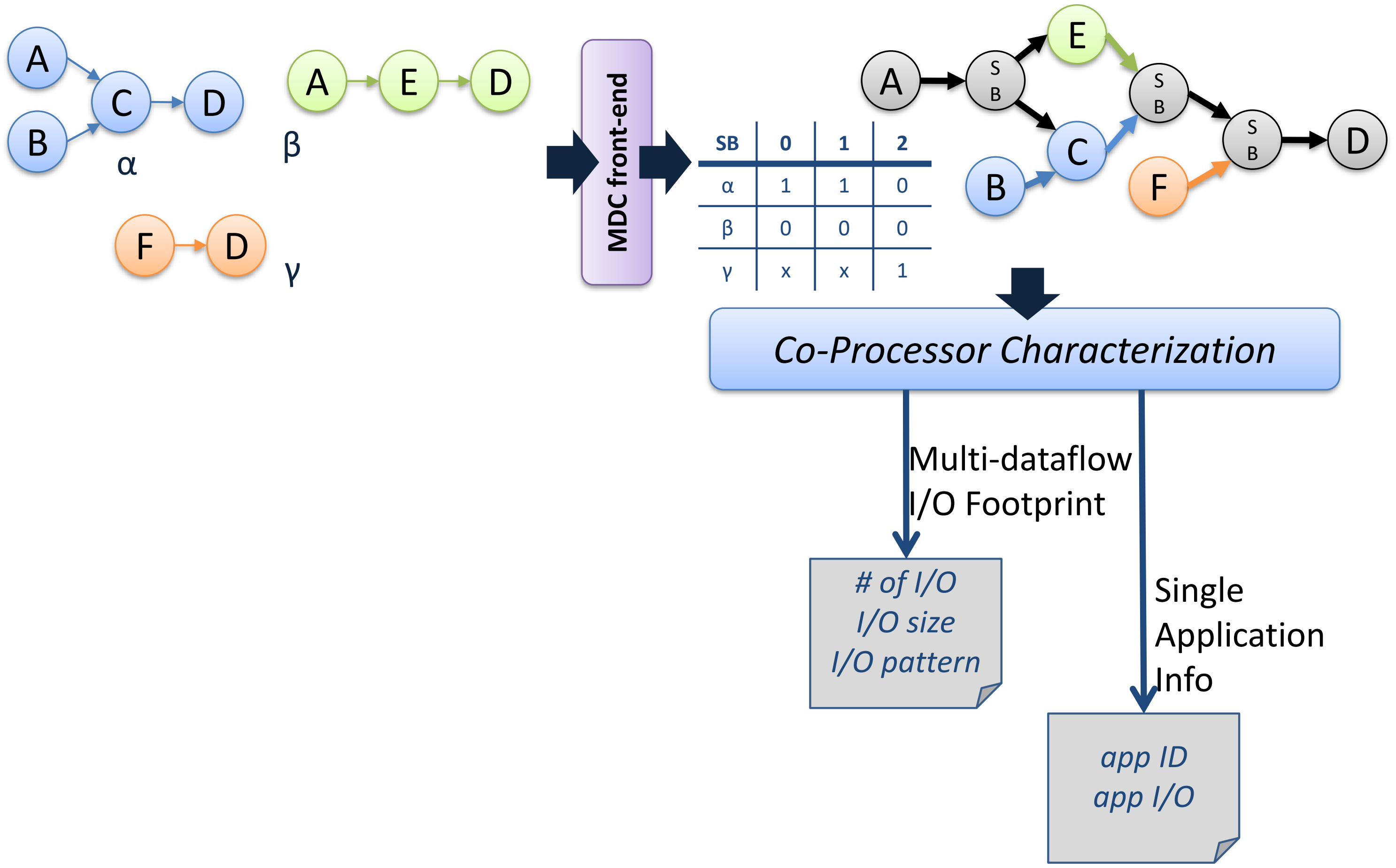
CONFIG REGS (manually assembled)

CGR substrate (automatically generated)

Co-Processor Generator


HARDWARE ACCELERATOR/CO-PROCESSOR
LOCAL MEMORY
HUGE EFFORT!!!
HOST PROCESSOR
SYSTEM BUS
CONFIG REGS (manually assembled)
CGR substrate (automatically generated)

Co-Processor Generator



SB	0	1	2
α	1	1	0
β	0	0	0
γ	x	x	1

Co-Processor Characterization

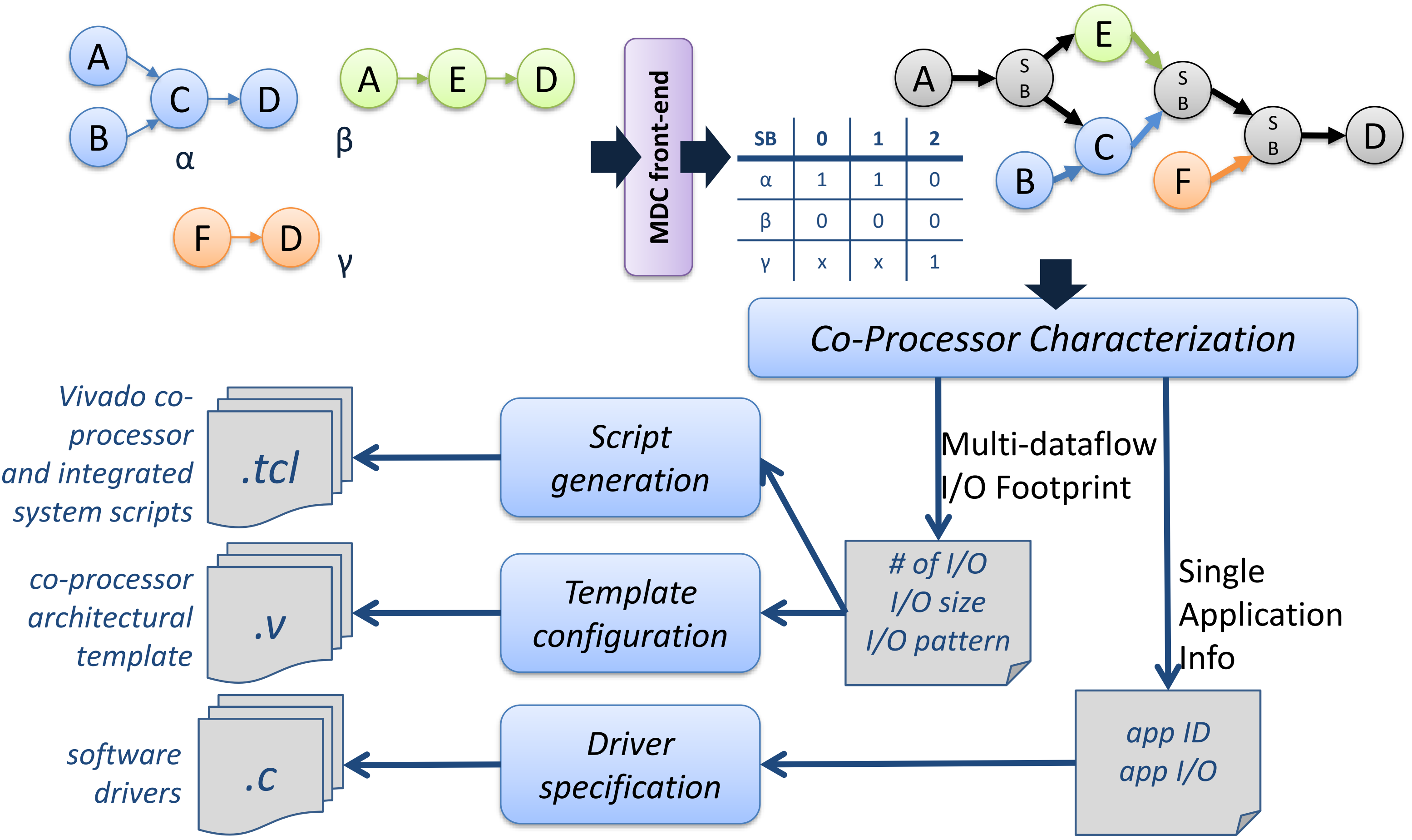
Multi-dataflow I/O Footprint

# of I/O
I/O size
I/O pattern

Single Application Info

app ID
app I/O

Co-Processor Generator



SB	0	1	2
α	1	1	0
β	0	0	0
γ	x	x	1

Co-Processor Characterization

Multi-dataflow I/O Footprint

Single Application Info

# of I/O
I/O size
I/O pattern

app ID
app I/O

Script generation

Template configuration

Driver specification

.tcl

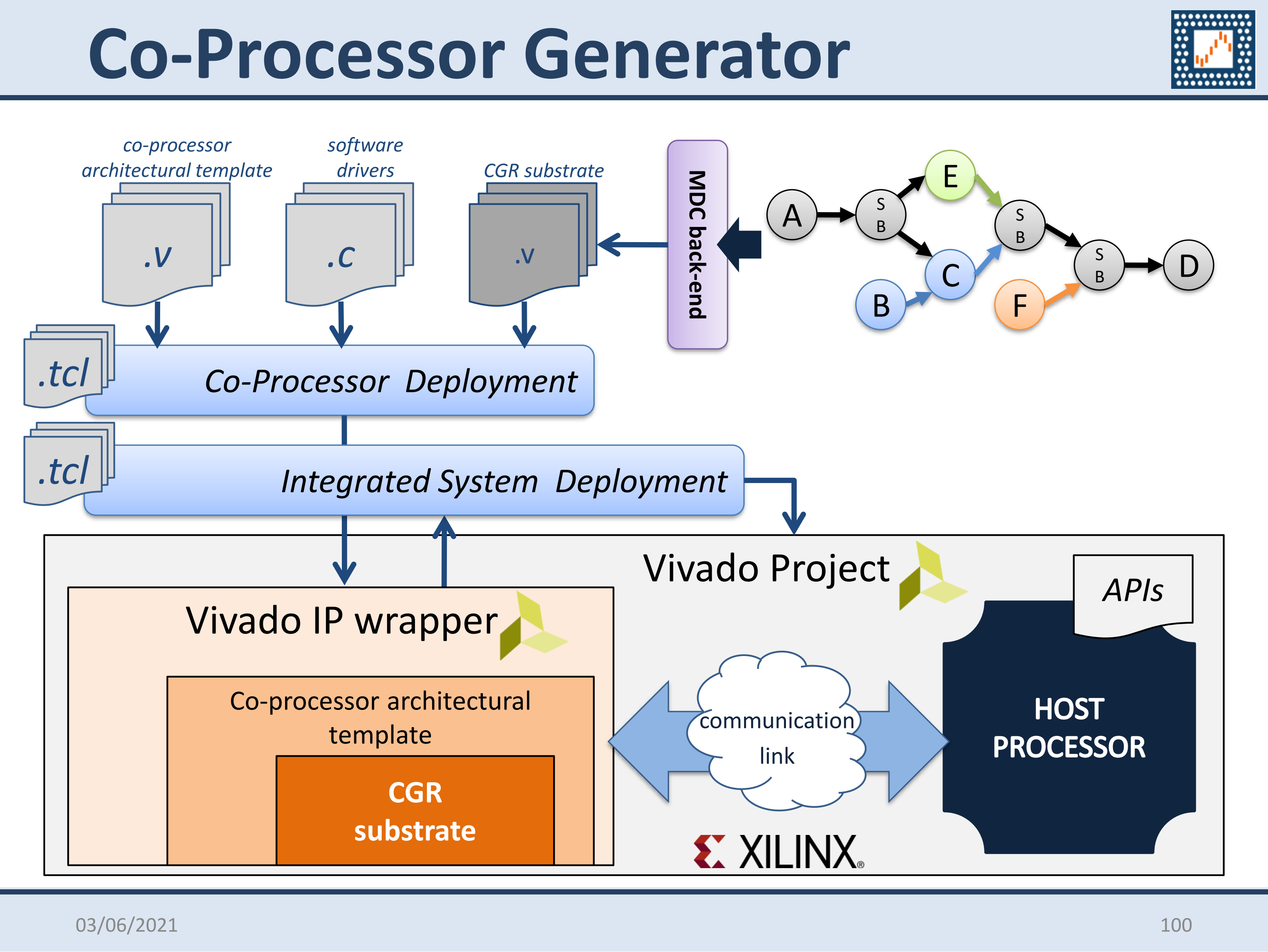
.v

.c

Vivado co-processor and integrated system scripts

co-processor architectural template

software drivers



Co-Processor Generator

03/06/2021

100

CPS&IoT'2021
2nd Summer School on Cyber Physical
+ Systems and Internet of Things

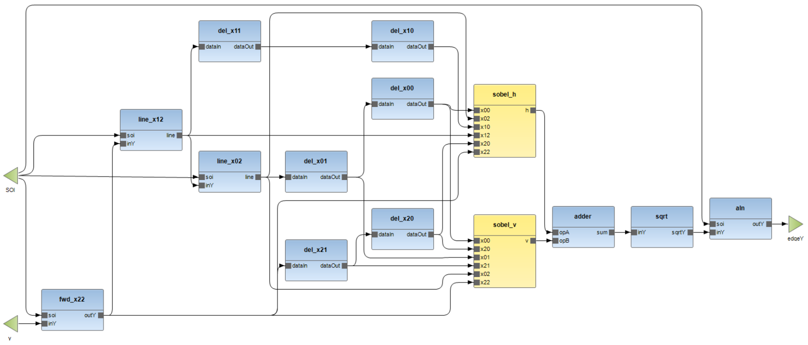
Tutorial

Step 2: Baseline MDC Datapath Merging

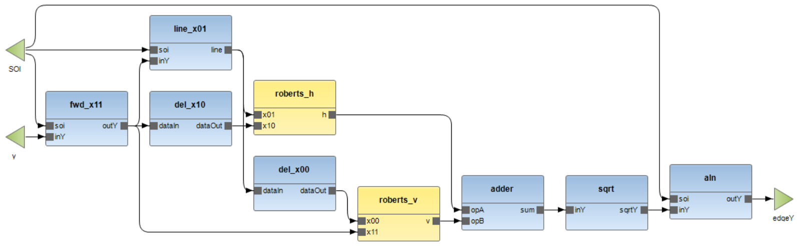
uniss
UNIVERSITÀ DEGLI STUDI DI SASSARI

MDC Datapath Merging

Sobel dataflow



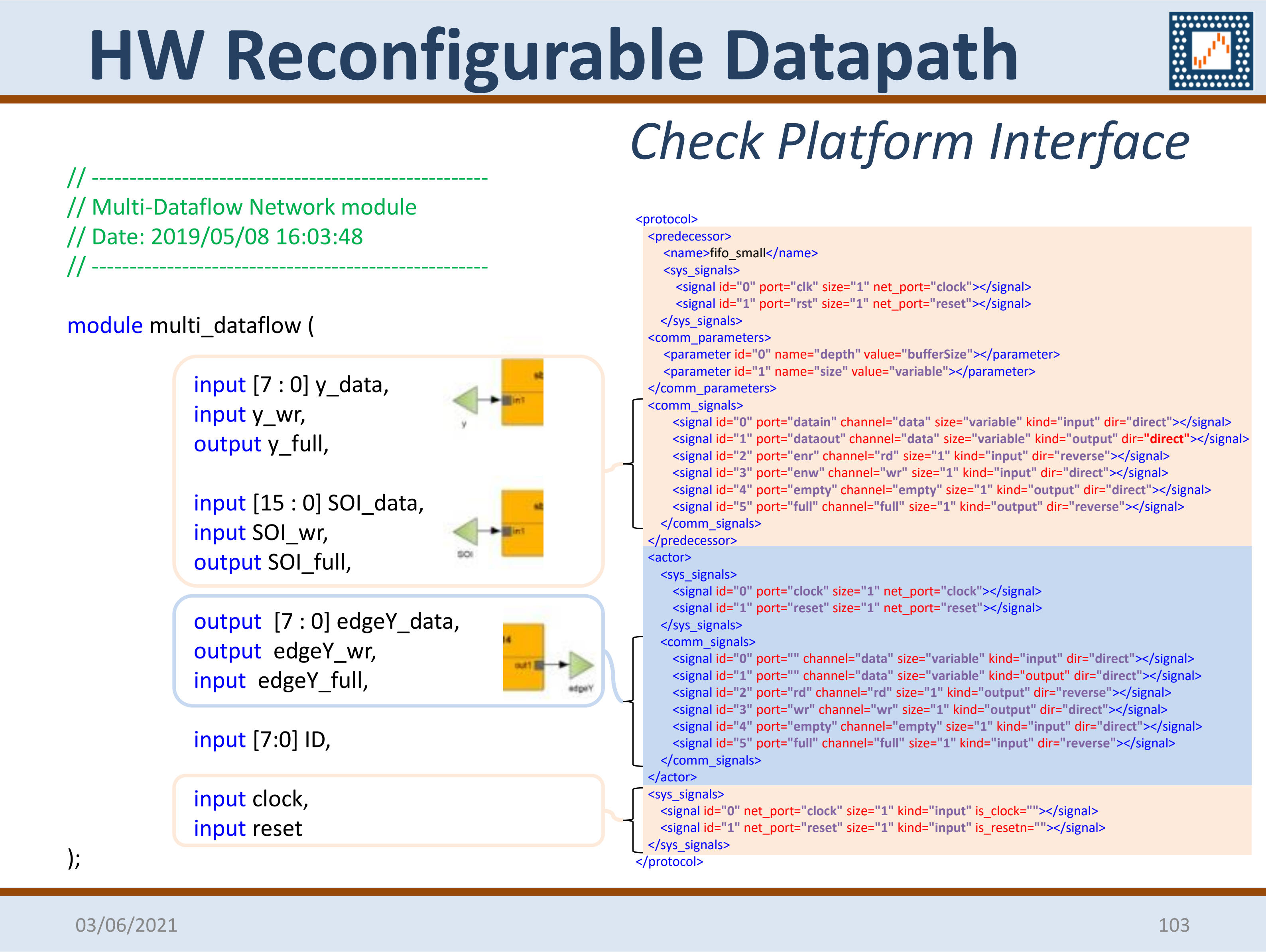
Roberts dataflow



Merging Expectations

actor	Sobel	Roberts	NS	S
Forward2x2	0	1	1	0
Forward3x3	1	0	1	0
Delay	6	2	4	2
LineBuffer	2	1	1	1
LeftShifter	4	0	4	0
Subtractor	6	2	4	2
Adder3x1	2	0	2	0
Multiplier	2	2	0	2
Adder2x1	1	1	0	1
Sqrt	1	1	0	1
Align2x2	0	1	1	0
Align3x3	1	0	1	0
Total	26	11	19	9

NS = Non Shareable, **S** = Shareable


y
in1
SOI
in1
out1
edgeY

HW Reconfigurable Datapath

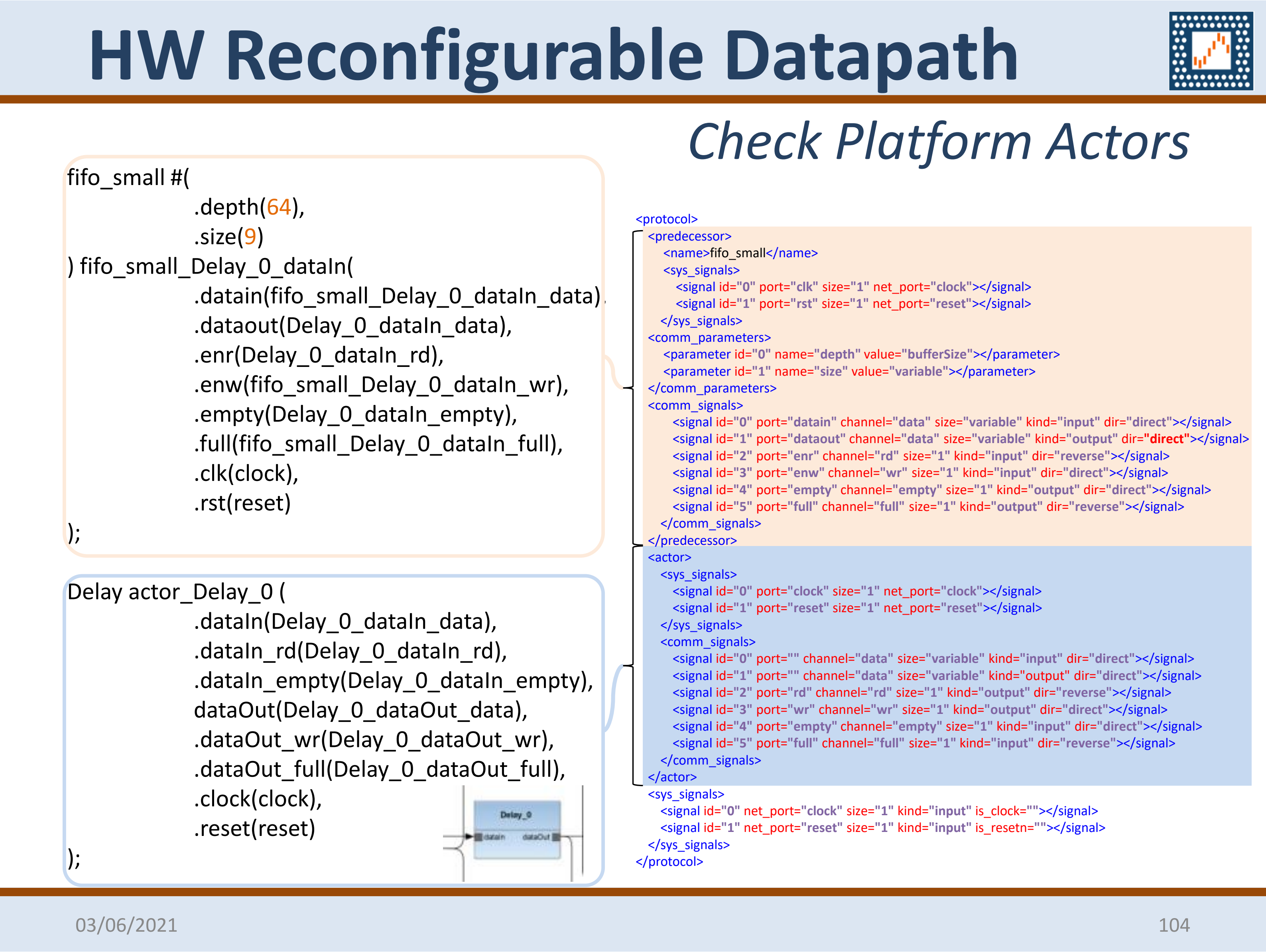
Check Platform Interface

```
// ------------------------------------------------------
// Multi-Dataflow Network module
// Date: 2019/05/08 16:03:48
// ------------------------------------------------------

module multi_dataflow (

        input [7 : 0] y_data,
        input y_wr,
        output y_full,

        input [15 : 0] SOI_data,
        input SOI_wr,
        output SOI_full,

        output  [7 : 0] edgeY_data,
        output  edgeY_wr,
        input  edgeY_full,

        input [7:0] ID,

        input clock,
        input reset
);
```

```
<protocol>
  <predecessor>
    <name>fifo_small</name>
    <sys_signals>
      <signal id="0" port="clk" size="1" net_port="clock"></signal>
      <signal id="1" port="rst" size="1" net_port="reset"></signal>
    </sys_signals>
  <comm_parameters>
    <parameter id="0" name="depth" value="bufferSize"></parameter>
    <parameter id="1" name="size" value="variable"></parameter>
  </comm_parameters>
  <comm_signals>
      <signal id="0" port="datain" channel="data" size="variable" kind="input" dir="direct"></signal>
      <signal id="1" port="dataout" channel="data" size="variable" kind="output" dir="direct"></signal>
      <signal id="2" port="enr" channel="rd" size="1" kind="input" dir="reverse"></signal>
      <signal id="3" port="enw" channel="wr" size="1" kind="input" dir="direct"></signal>
      <signal id="4" port="empty" channel="empty" size="1" kind="output" dir="direct"></signal>
      <signal id="5" port="full" channel="full" size="1" kind="output" dir="reverse"></signal>
    </comm_signals>
  </predecessor>
  <actor>
    <sys_signals>
      <signal id="0" port="clock" size="1" net_port="clock"></signal>
      <signal id="1" port="reset" size="1" net_port="reset"></signal>
    </sys_signals>
    <comm_signals>
      <signal id="0" port="" channel="data" size="variable" kind="input" dir="direct"></signal>
      <signal id="1" port="" channel="data" size="variable" kind="output" dir="direct"></signal>
      <signal id="2" port="rd" channel="rd" size="1" kind="output" dir="reverse"></signal>
      <signal id="3" port="wr" channel="wr" size="1" kind="output" dir="direct"></signal>
      <signal id="4" port="empty" channel="empty" size="1" kind="input" dir="direct"></signal>
      <signal id="5" port="full" channel="full" size="1" kind="input" dir="reverse"></signal>
    </comm_signals>
  </actor>
  <sys_signals>
    <signal id="0" net_port="clock" size="1" kind="input" is_clock=""></signal>
    <signal id="1" net_port="reset" size="1" kind="input" is_resetn=""></signal>
  </sys_signals>
</protocol>
```

03/06/2021

103



HW Reconfigurable Datapath

Check Platform Actors

```
fifo_small #(
            .depth(64),
            .size(9)
) fifo_small_Delay_0_dataIn(
            .datain(fifo_small_Delay_0_dataIn_data),
            .dataout(Delay_0_dataIn_data),
            .enr(Delay_0_dataIn_rd),
            .enw(fifo_small_Delay_0_dataIn_wr),
            .empty(Delay_0_dataIn_empty),
            .full(fifo_small_Delay_0_dataIn_full),
            .clk(clock),
            .rst(reset)
);
```

```
Delay actor_Delay_0 (
            .dataIn(Delay_0_dataIn_data),
            .dataIn_rd(Delay_0_dataIn_rd),
            .dataIn_empty(Delay_0_dataIn_empty),
            dataOut(Delay_0_dataOut_data),
            .dataOut_wr(Delay_0_dataOut_wr),
            .dataOut_full(Delay_0_dataOut_full),
            .clock(clock),
            .reset(reset)
);
```

```
<protocol>
  <predecessor>
     <name>fifo_small</name>
     <sys_signals>
        <signal id="0" port="clk" size="1" net_port="clock"></signal>
        <signal id="1" port="rst" size="1" net_port="reset"></signal>
    </sys_signals>
  <comm_parameters>
     <parameter id="0" name="depth" value="bufferSize"></parameter>
     <parameter id="1" name="size" value="variable"></parameter>
  </comm_parameters>
  <comm_signals>
       <signal id="0" port="datain" channel="data" size="variable" kind="input" dir="direct"></signal>
       <signal id="1" port="dataout" channel="data" size="variable" kind="output" dir="direct"></signal>
       <signal id="2" port="enr" channel="rd" size="1" kind="input" dir="reverse"></signal>
       <signal id="3" port="enw" channel="wr" size="1" kind="input" dir="direct"></signal>
       <signal id="4" port="empty" channel="empty" size="1" kind="output" dir="direct"></signal>
       <signal id="5" port="full" channel="full" size="1" kind="output" dir="reverse"></signal>
    </comm_signals>
  </predecessor>
  <actor>
    <sys_signals>
       <signal id="0" port="clock" size="1" net_port="clock"></signal>
       <signal id="1" port="reset" size="1" net_port="reset"></signal>
    </sys_signals>
    <comm_signals>
       <signal id="0" port="" channel="data" size="variable" kind="input" dir="direct"></signal>
       <signal id="1" port="" channel="data" size="variable" kind="output" dir="direct"></signal>
       <signal id="2" port="rd" channel="rd" size="1" kind="output" dir="reverse"></signal>
       <signal id="3" port="wr" channel="wr" size="1" kind="output" dir="direct"></signal>
       <signal id="4" port="empty" channel="empty" size="1" kind="input" dir="direct"></signal>
       <signal id="5" port="full" channel="full" size="1" kind="input" dir="reverse"></signal>
    </comm_signals>
  </actor>
  <sys_signals>
    <signal id="0" net_port="clock" size="1" kind="input" is_clock=""></signal>
    <signal id="1" net_port="reset" size="1" kind="input" is_resetn=""></signal>
  </sys_signals>
</protocol>
```

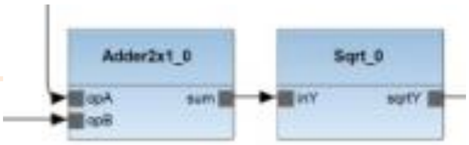
03/06/2021

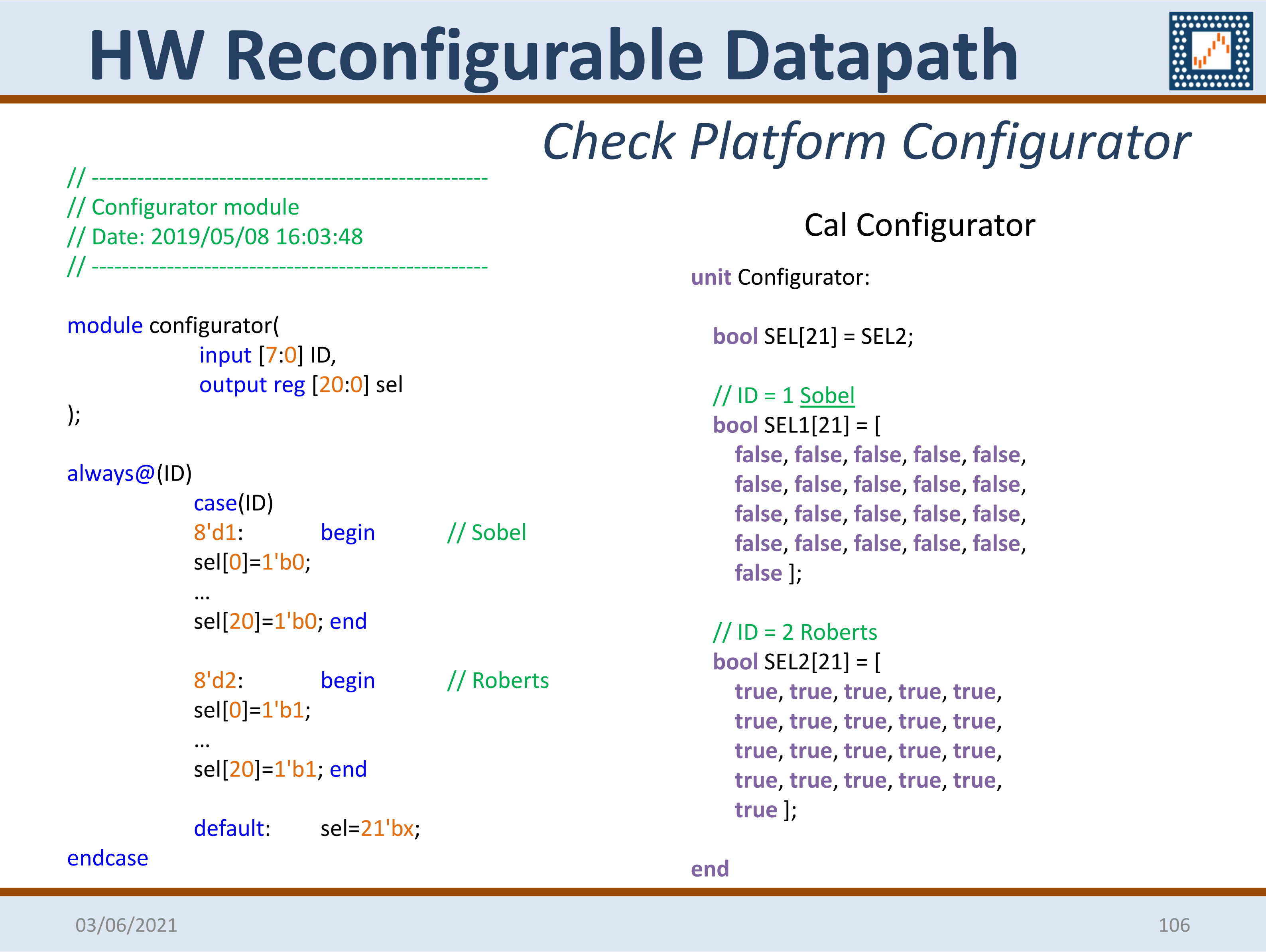
104

HW Reconfigurable Datapath

Check Platform Connections

```
assign fifo_small_Adder2x1_0_opA_data = Multiplier_0_prod_data;
assign fifo_small_Adder2x1_0_opA_wr = Multiplier_0_prod_wr;
assign Multiplier_0_prod_full = fifo_small_Adder2x1_0_opA_full;

assign fifo_small_Adder2x1_0_opB_data = Multiplier_1_prod_data;
assign fifo_small_Adder2x1_0_opB_wr = Multiplier_1_prod_wr;
assign Multiplier_1_prod_full = fifo_small_Adder2x1_0_opB_full;

assign fifo_small_Sqrt_0_inY_data = Adder2x1_0_sum_data;
assign fifo_small_Sqrt_0_inY_wr = Adder2x1_0_sum_wr;
assign Adder2x1_0_sum_full = fifo_small_Sqrt_0_inY_full;

assign sbox_0_in1_data = y_data;
assign sbox_0_in1_wr = y_wr;
assign y_full = sbox_0_in1_full;

assign fifo_small_Forward2x2_0_inY_data = sbox_0_out2_data;
assign fifo_small_Forward2x2_0_inY_wr = sbox_0_out2_wr;
assign sbox_0_out2_full = fifo_small_Forward2x2_0_inY_full;
```





HW Reconfigurable Datapath

Check Platform Configurator

```
// ---------------------------------------------------
// Configurator module
// Date: 2019/05/08 16:03:48
// ---------------------------------------------------

module configurator(
                input [7:0] ID,
                output reg [20:0] sel
);

always@(ID)
               case(ID)
               8'd1:          begin          // Sobel
               sel[0]=1'b0;
               …
               sel[20]=1'b0; end

               8'd2:          begin          // Roberts
               sel[0]=1'b1;
               …
               sel[20]=1'b1; end

               default:       sel=21'bx;
endcase
```

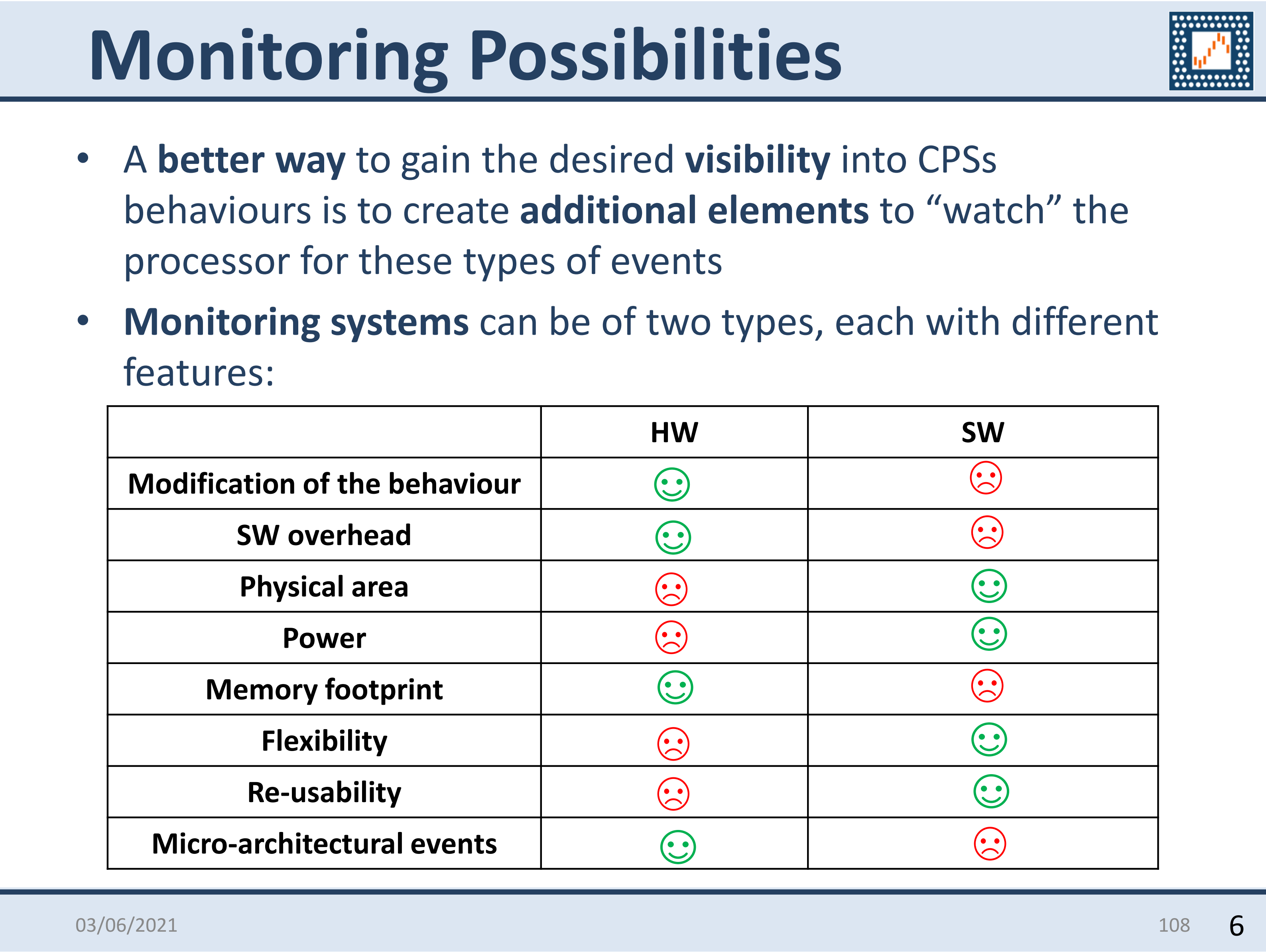
Cal Configurator

```
unit Configurator:

  bool SEL[21] = SEL2;

  // ID = 1 Sobel
  bool SEL1[21] = [
    false, false, false, false, false,
    false, false, false, false, false,
    false, false, false, false, false,
    false, false, false, false, false,
    false ];

  // ID = 2 Roberts
  bool SEL2[21] = [
    true, true, true, true, true,
    true, true, true, true, true,
    true, true, true, true, true,
    true, true, true, true, true,
    true ];

end
```

03/06/2021 106

CPS&IoT'2021
2nd Summer School on Cyber Physical +
Systems and Internet of Things

Step 3: Monitoring

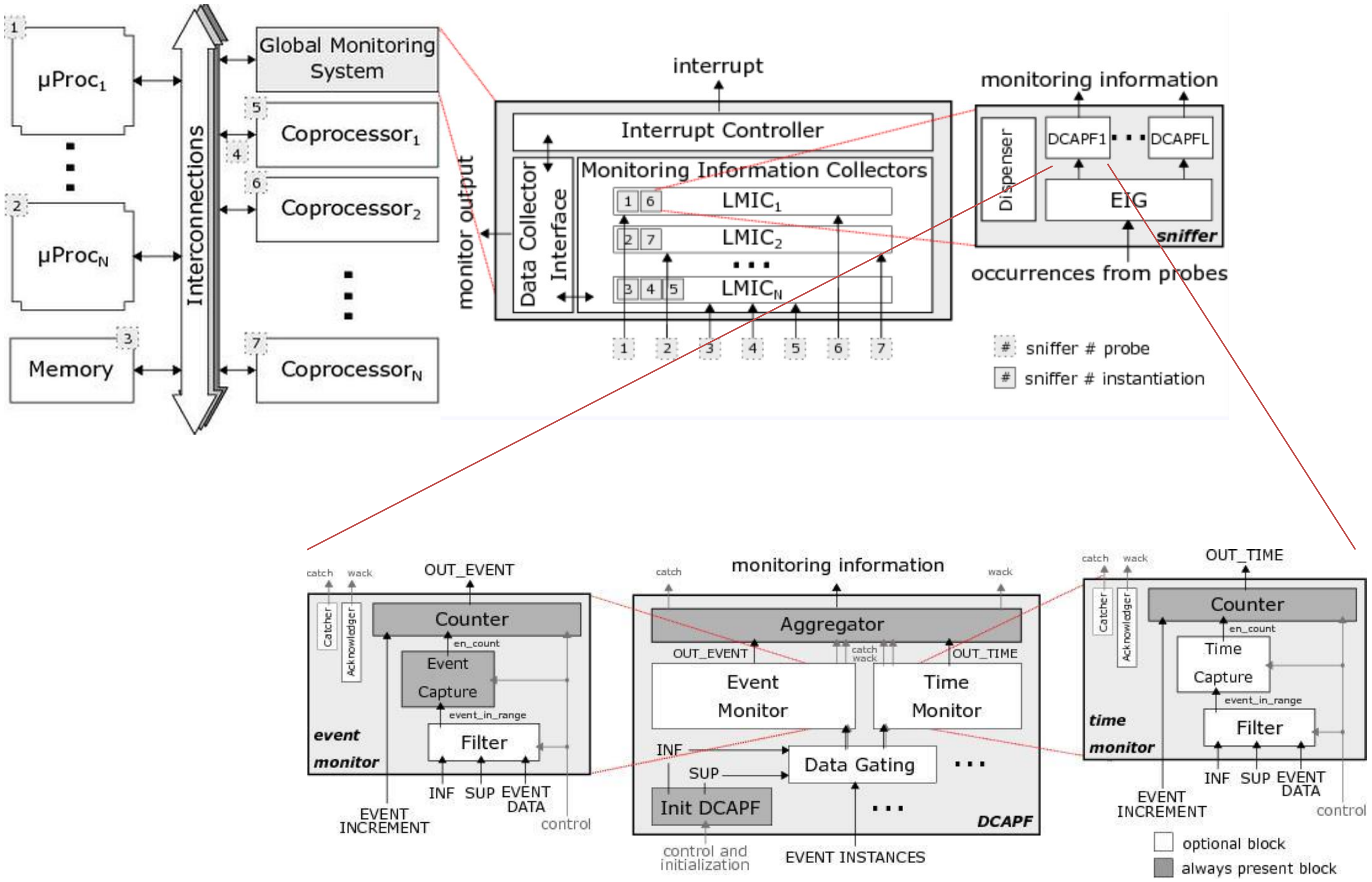


Monitoring Possibilities

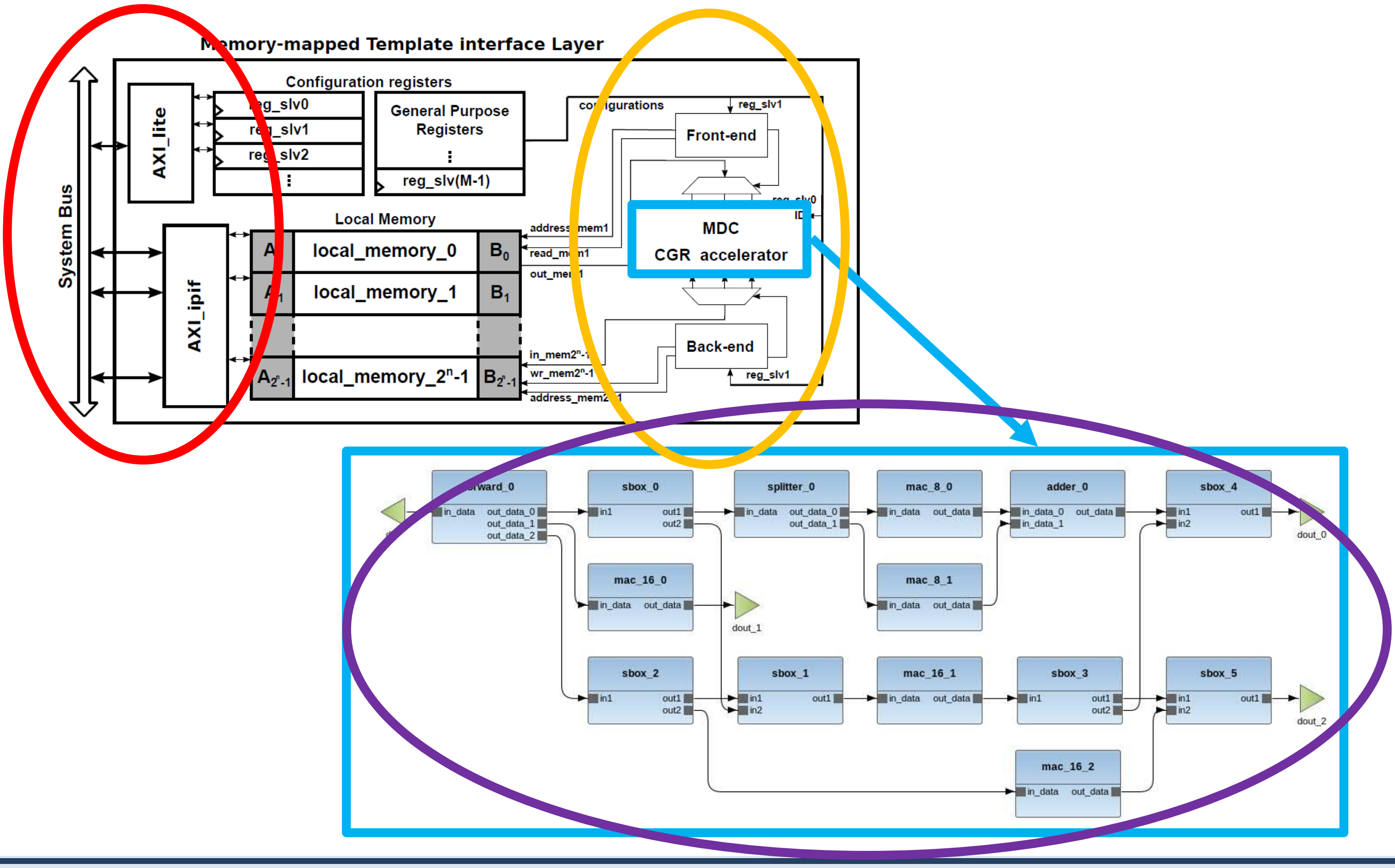
- A **better way** to gain the desired **visibility** into CPSs behaviours is to create **additional elements** to “watch” the processor for these types of events
- **Monitoring systems** can be of two types, each with different features:

	HW	SW
Modification of the behaviour	☺	☹
SW overhead	☺	☹
Physical area	☹	☺
Power	☹	☺
Memory footprint	☺	☹
Flexibility	☹	☺
Re-usability	☹	☺
Micro-architectural events	☺	☹

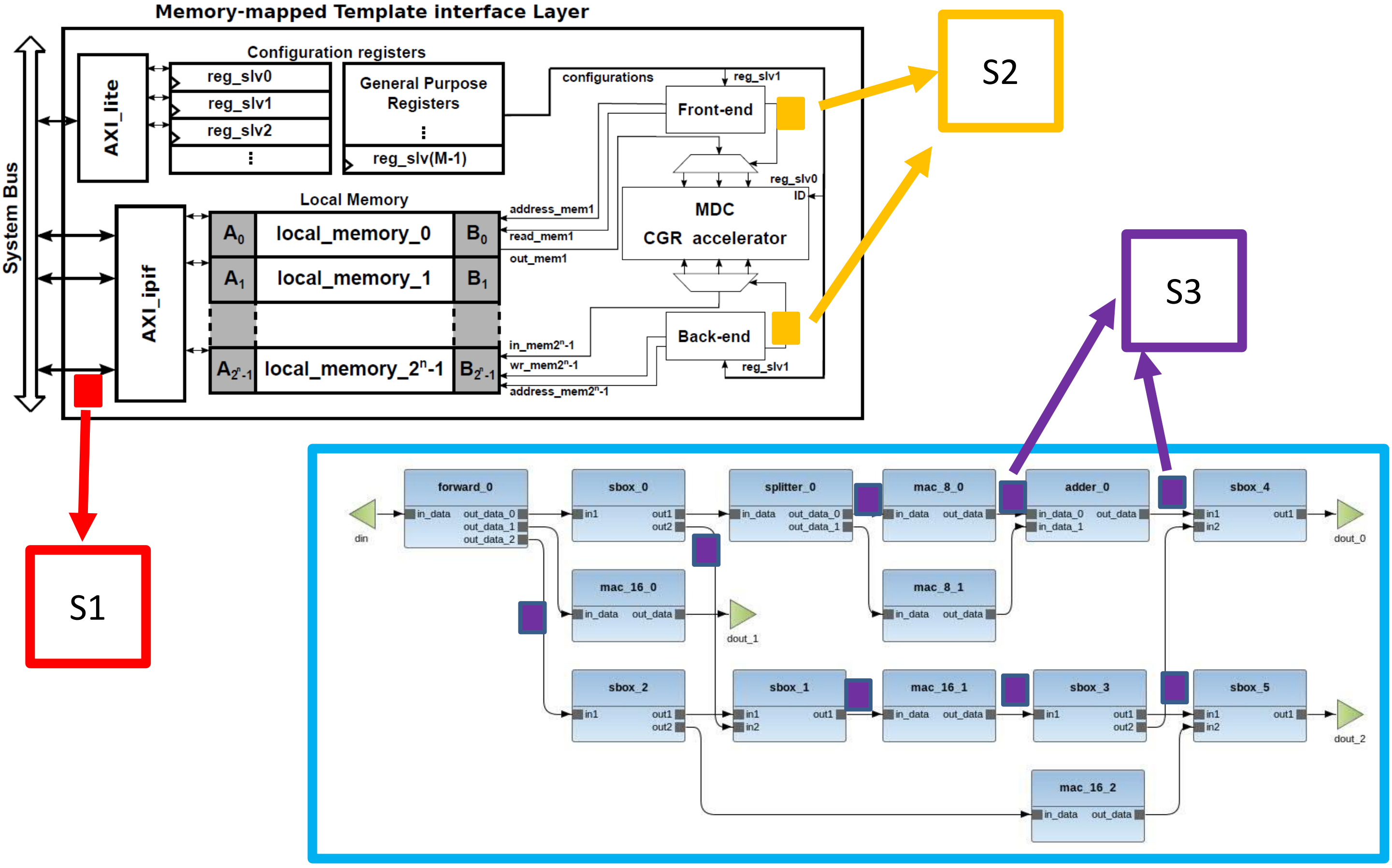
Composition of a monitor



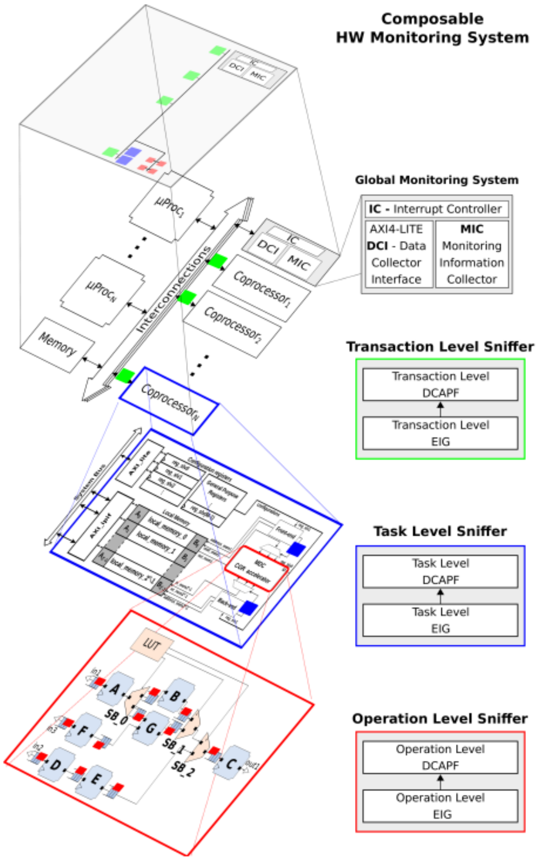
MDC-accelerator monitoring



Sniffers for MDC accelerators

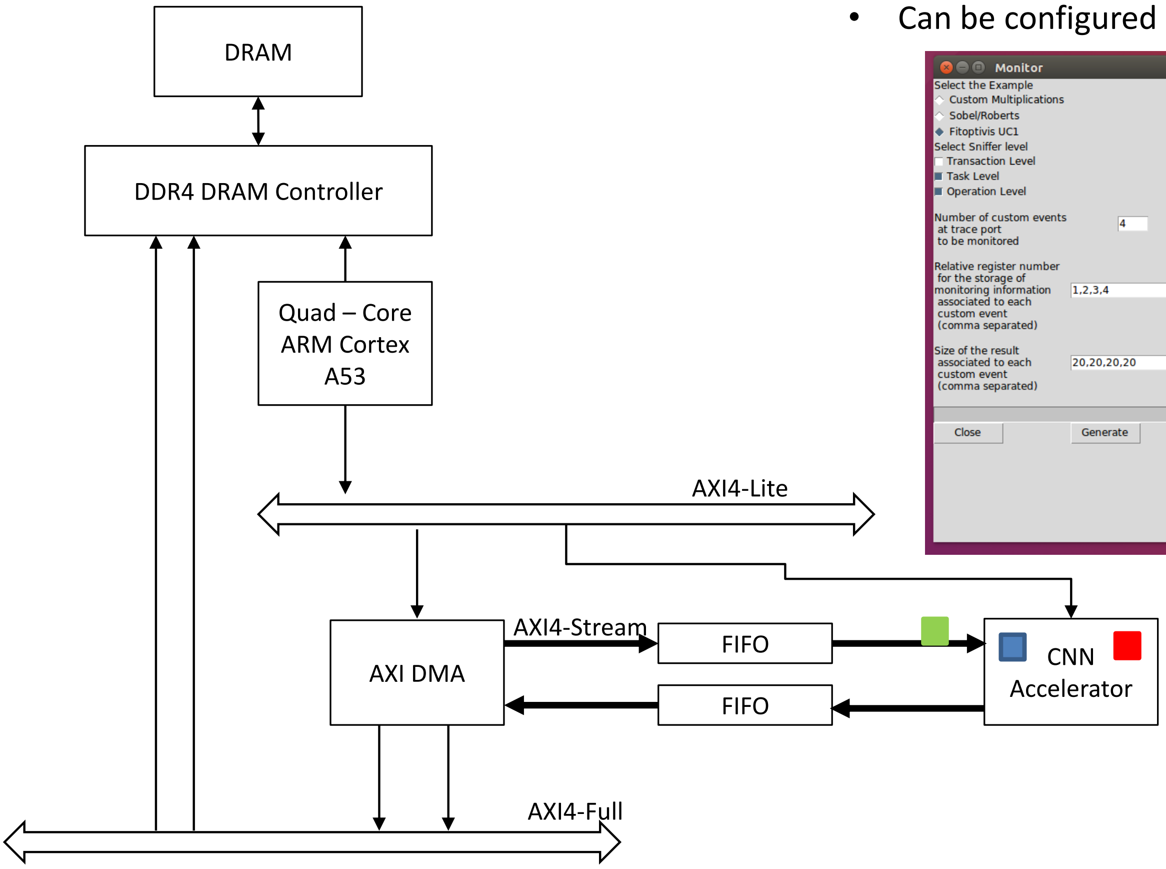


Monitored infrastructure

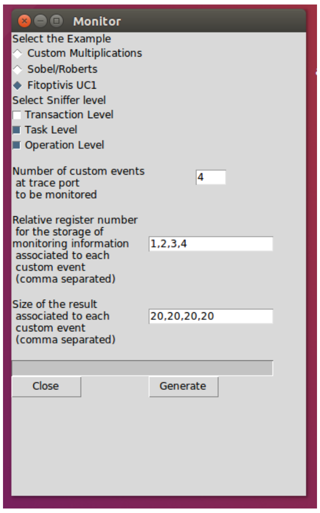


- Monitor of a Sobel/Roberts filter coprocessor developed using MDC
- Collect the following metrics:
  - Number of bytes written "toward" the coprocessor
  - Execution time to perform the computation with the coprocessor
  - Verification of happening of specific internal user-defined transitions

Monitoring Accelerators



- Can be configured through:



Select the Example
○ Custom Multiplications
○ Sobel/Roberts
● Fitoptivis UC1
Select Sniffer level
□ Transaction Level
■ Task Level
■ Operation Level

Number of custom events at trace port to be monitored: 4

Relative register number for the storage of monitoring information associated to each custom event (comma separated): 1,2,3,4

Size of the result associated to each custom event (comma separated): 20,20,20,20

CPS&IoT'2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

Dataflow-Based Toolchain for Adaptive Hardware Accelerators Deployment and Monitoring

Daniel Madronal[1], Francesco Ratto[2], Giacomo Valente[3]

[1]University of Sassari, Intelligent system DEsign and Application (IDEA) Group

[2]University of Cagliari, Diee – Microelectronics and Bioengineering (EOLAB) Group

[3]University of L'Aquila, Disim – Embedded Systems Group

CPS&IoT'2021
2nd Summer School on Cyber Physical + Systems and Internet of Things

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 826610. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Spain, Austria, Belgium, Czech Republic, France, Italy, Latvia, Netherlands.

COMP4DRONES

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

This work is part of the FitOptiVis project [1] funded by the ECSEL Joint Undertaking under grant number H2020-ECSEL-2017-2-783162.

FIT PTI VIS

[1] "The FitOptiVis ECSEL project: highly efficient distributed embedded image/video processing in cyber-physical systems", ACM Int'l Conf. on Computing Frontiers, 2019, pp. 333-338, https://doi.org/10.1145/3310273.3323437

uniss
UNIVERSITÀ DEGLI STUDI DI SASSARI

5G Connectivity: the Key to Success for European Industry?

Hui Cao
Head of Policy and Strategy of Huawei's EU office

Abstract – **The presentation will demonstrate how 5G connectivity will help deploying technologies like Artificial Intelligence in different sectors of the economy (agriculture, education, healthcare) and how will help industries working together with EU Policy makers to achieve successful European Digital Transformation. Huawei is a leading global provider of information and communications technology (ICT) infrastructure and smart devices. It is committed to bringing digital to every person, home and organization for a fully connected, intelligent world. Huawei has approximately 197,000 employees and for more than 30 years, it has worked closely with their carrier customers to build over 1,500 networks in more than 170 countries and regions, serving more than three billion people around the world. At Huawei, innovation focuses on customer needs. It invests heavily in basic research, concentrating on technological breakthroughs that drive the world forward.**

About the author

***Dr Hui Cao** has broad experience in the telecommunications industry ranging from the operator to academic research and the vendor. He has a deep knowledge of market trends, industry challenges, network deployment and technical developments. As Head at Huawei's EU Public Affairs and Communication Office based in Communication Office Brussels. Dr Cao is responsible for regulatory issues on connectivity and innovative ICT technologies.*

Prior to this position, he was the Network CTO in Huawei Western Europe region with a focus on the latest technologies exploring cost-effective solutions and practices in building experience-oriented and future-proof broadband networks with Simplicity,

Automation and Intelligence. He also worked with China Telecom on broadband network management and development. Dr Cao obtained his doctoral degree in Electronic Engineering from Oxford Brookes University in the UK.

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Model-Driven Design of CPSoSs

Application to drone-based services

Eugenio Villar
University of Cantabria

CPS&IoT

CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

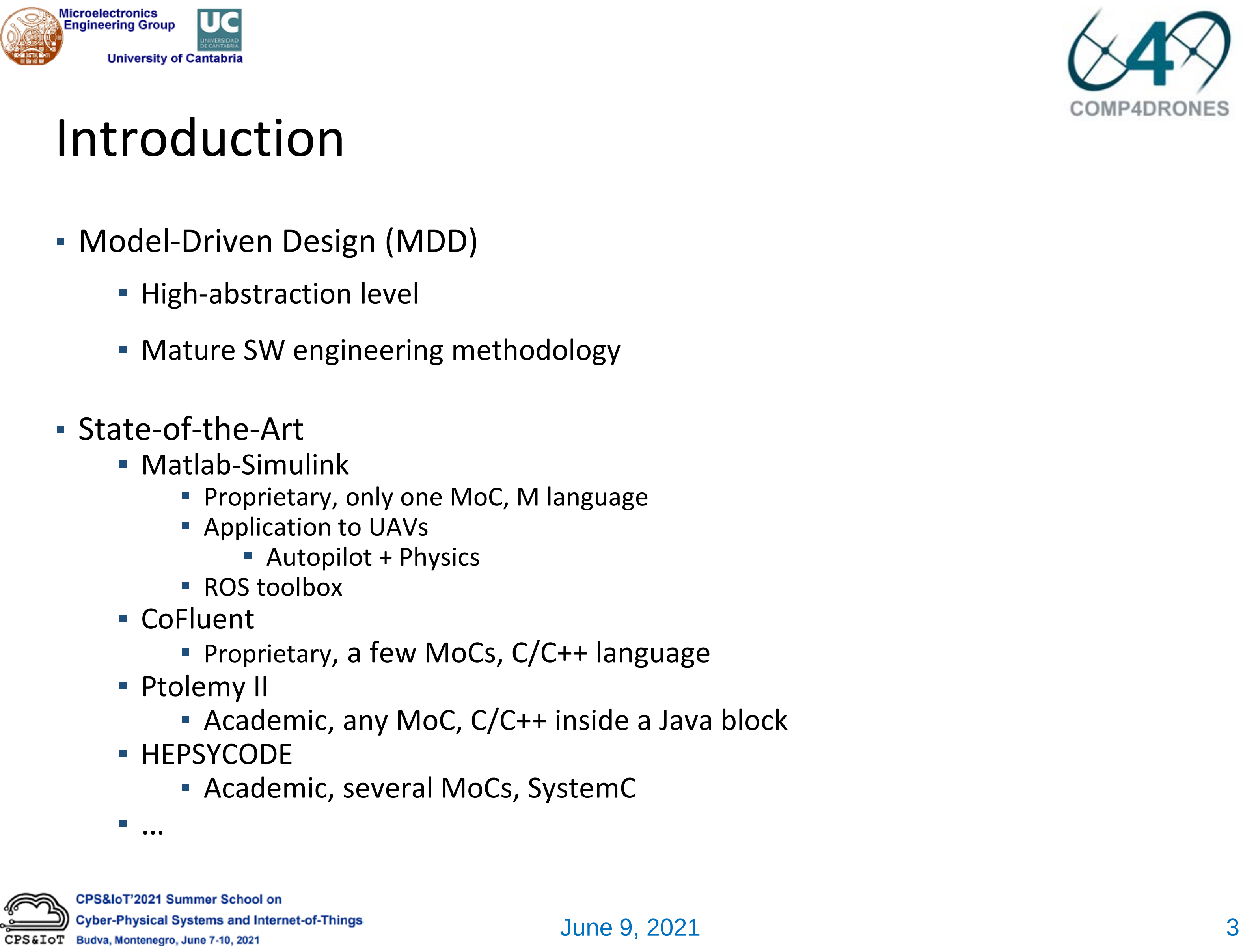
Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Agenda

- Introduction
- Model-Driven Design of CPSoS
- Design Verification and Performance Analysis
- Experimental Results
- Conclusions

- Slides can be found at:
  - https://www.slideshare.net/EugenioVillar/



Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Introduction

- Model-Driven Design (MDD)
  - High-abstraction level
  - Mature SW engineering methodology
- State-of-the-Art
  - Matlab-Simulink
    - Proprietary, only one MoC, M language
    - Application to UAVs
      - Autopilot + Physics
    - ROS toolbox
  - CoFluent
    - Proprietary, a few MoCs, C/C++ language
  - Ptolemy II
    - Academic, any MoC, C/C++ inside a Java block
  - HEPSYCODE
    - Academic, several MoCs, SystemC
  - …

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things Budva, Montenegro, June 7-10, 2021

June 9, 2021

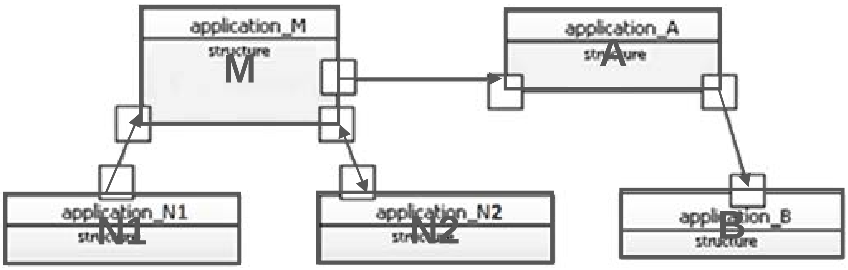
3

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Introduction

- UML
  - Standard, any (user-defined) MoC, any language
  - Natural way to capture system architecture



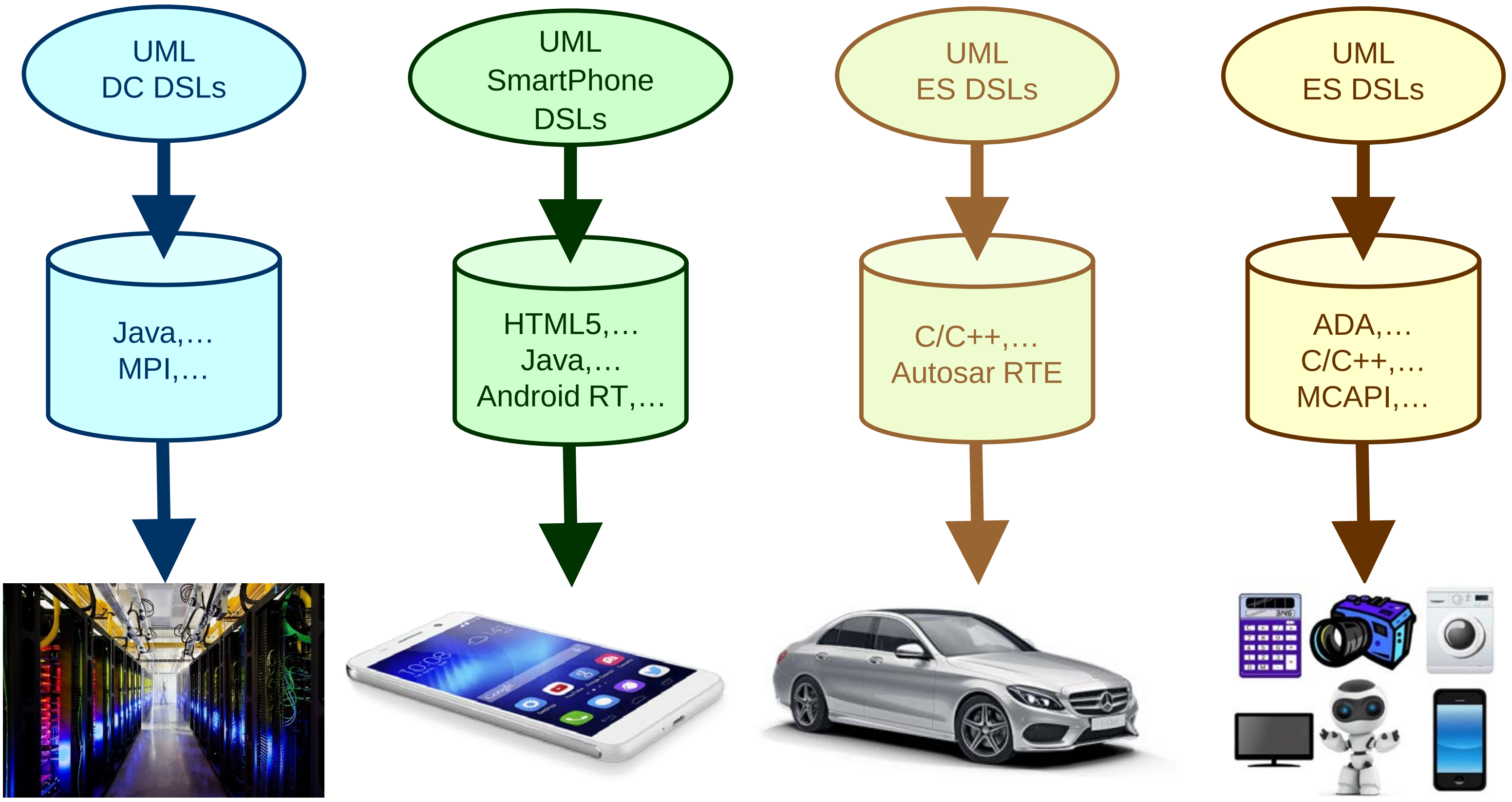
- Semantic lacks
- Domain-specific profiles
- MetaMorph
  - OpenSource, any (user-defined) MoC, language agnostic

Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Introduction



UML
DC DSLs

Java,…
MPI,…

UML
SmartPhone
DSLs

HTML5,…
Java,…
Android RT,…

UML
ES DSLs

C/C++,…
Autosar RTE

UML
ES DSLs

ADA,…
C/C++,…
MCAPI,…

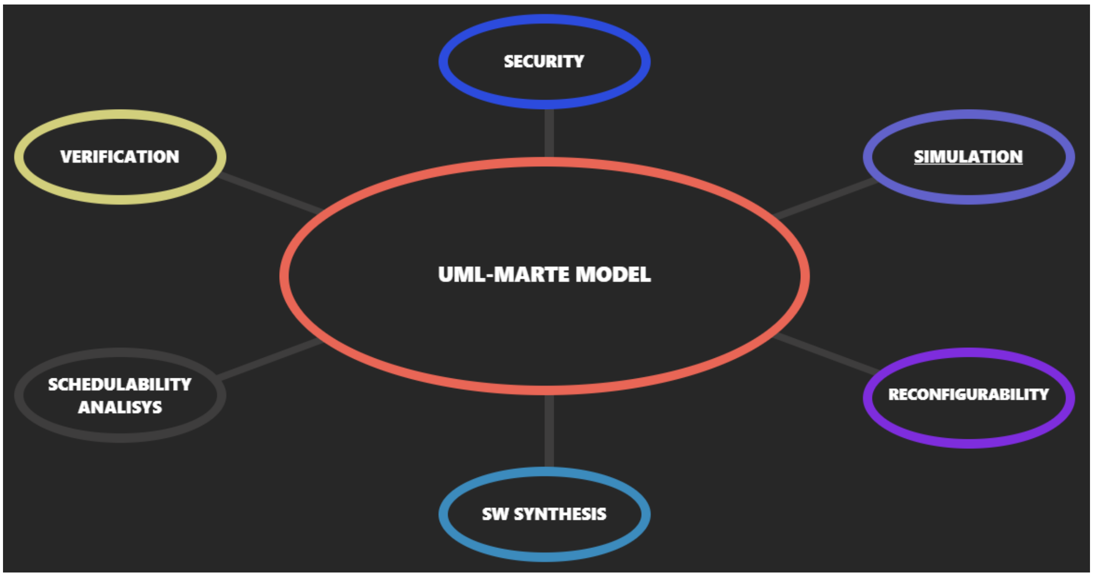
Microelectronics Engineering Group

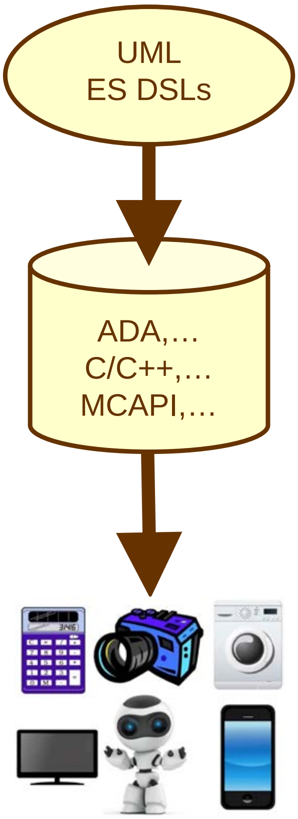
University of Cantabria

COMP4DRONES

Introduction

- S3D: Single-Source System Design Framework



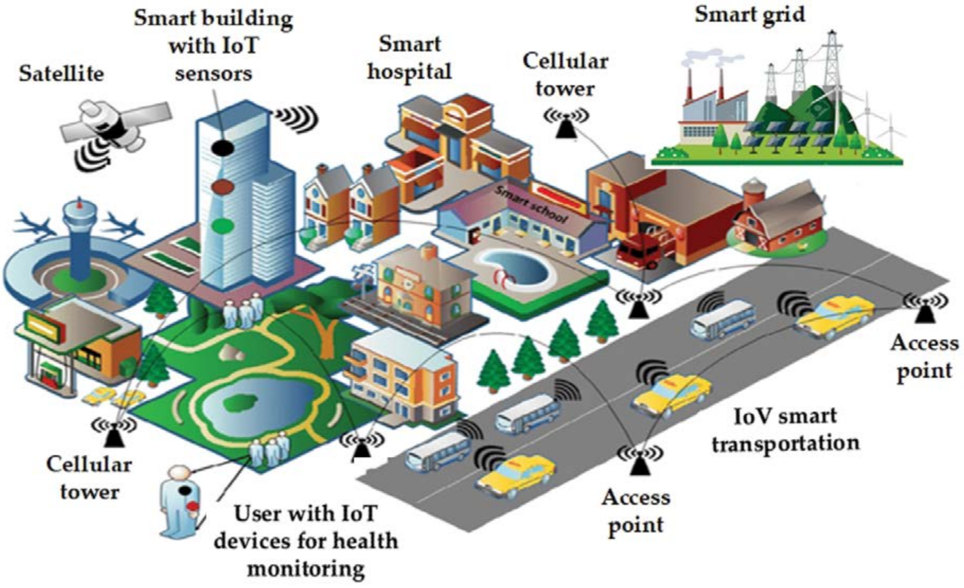


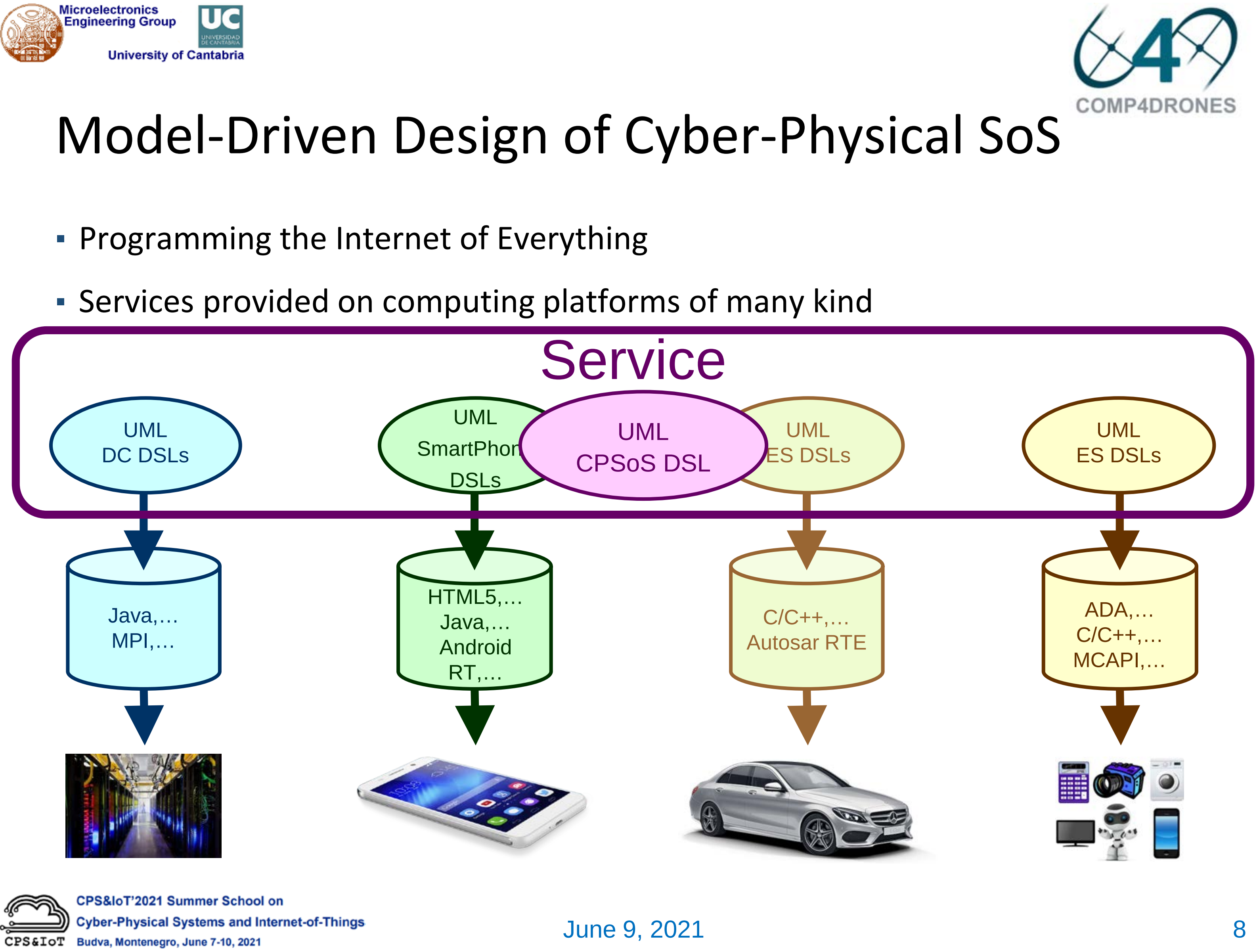
Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Programming the Internet of Everything
  - In close interaction with the physical world
- Services provided on computing platforms of many kind





Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Programming the Internet of Everything
- Services provided on computing platforms of many kind

Service

UML DC DSLs → Java,… MPI,…

UML SmartPhon DSLs → HTML5,… Java,… Android RT,…

UML CPSoS DSL

UML ES DSLs → C/C++,… Autosar RTE

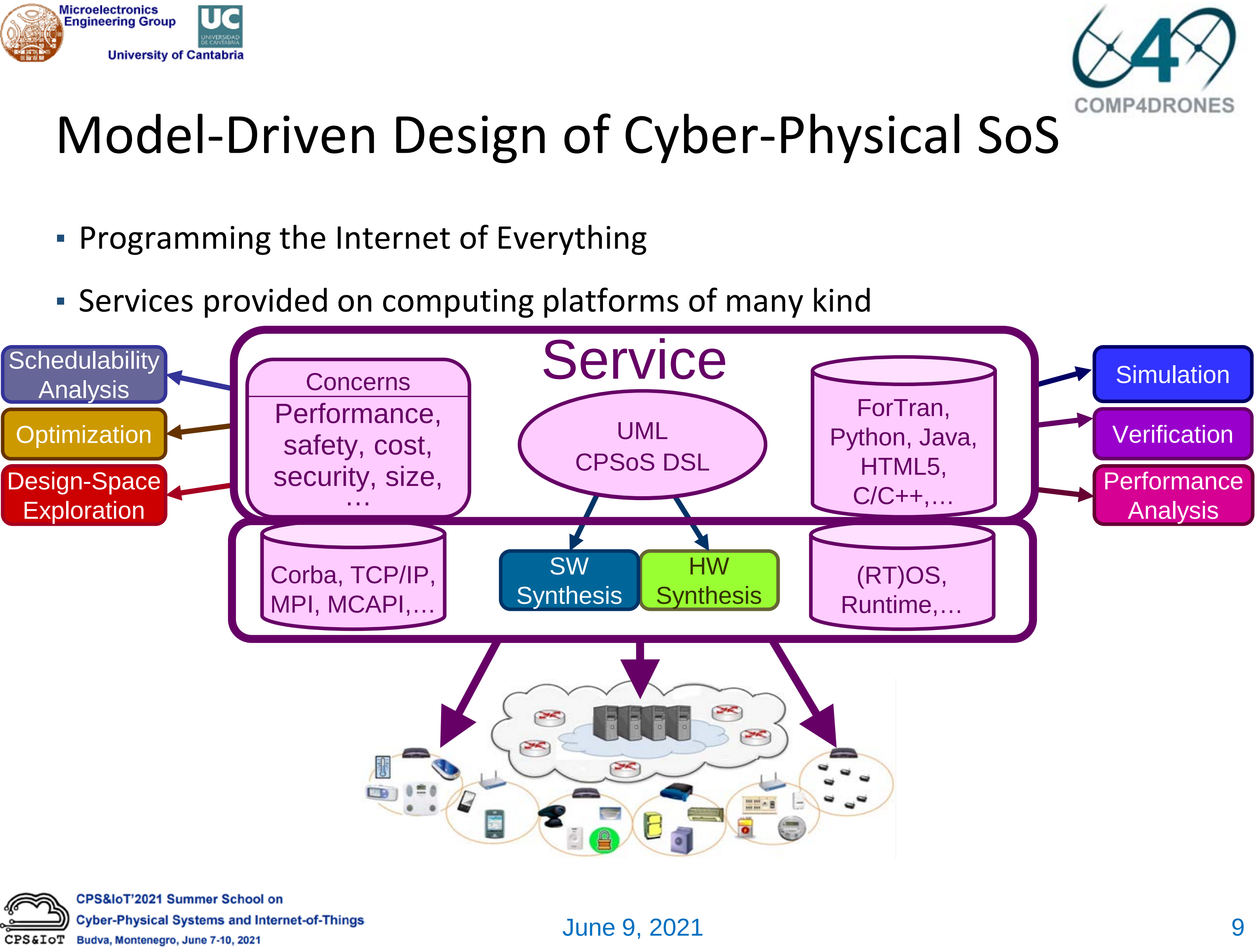
UML ES DSLs → ADA,… C/C++,… MCAPI,…

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things Budva, Montenegro, June 7-10, 2021

CPS&IoT

June 9, 2021

8



Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Programming the Internet of Everything
- Services provided on computing platforms of many kind

Schedulability Analysis

Optimization

Design-Space Exploration

Service

Concerns

Performance, safety, cost, security, size, …

UML CPSoS DSL

ForTran, Python, Java, HTML5, C/C++,…

Simulation

Verification

Performance Analysis

Corba, TCP/IP, MPI, MCAPI,…

SW Synthesis

HW Synthesis

(RT)OS, Runtime,…

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things

Budva, Montenegro, June 7-10, 2021

CPS&IoT

June 9, 2021

9

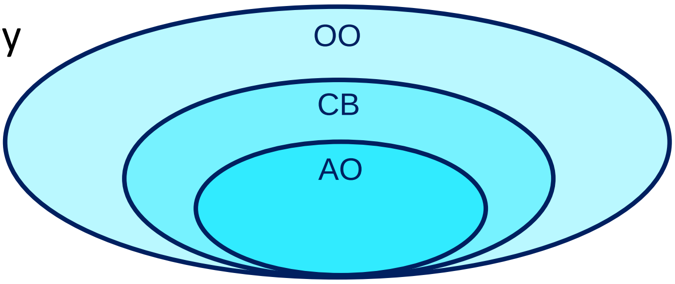
Microelectronics Engineering Group

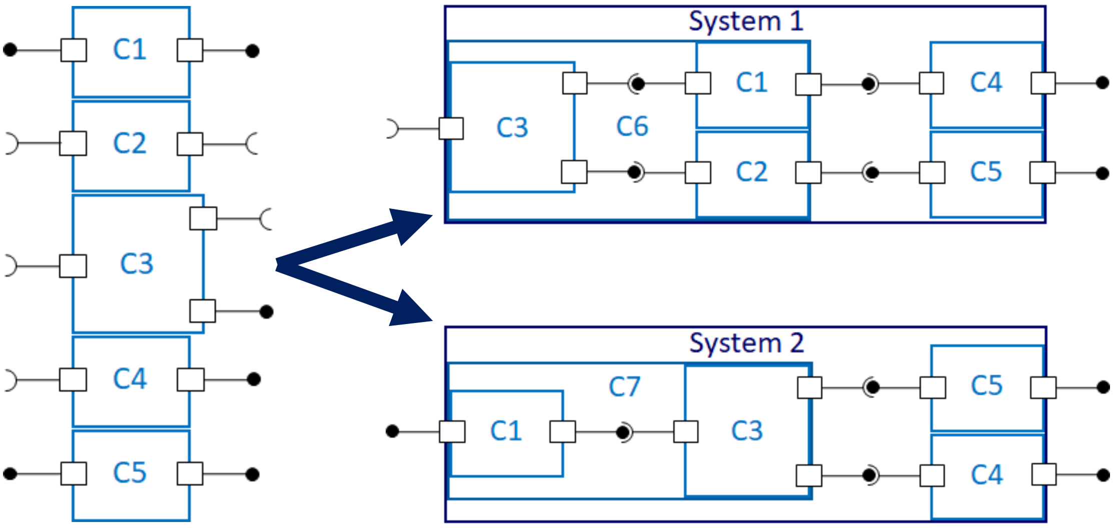
University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- UML/MARTE System Modeling Methodology
- Platform-Independent
  - Flexible
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation



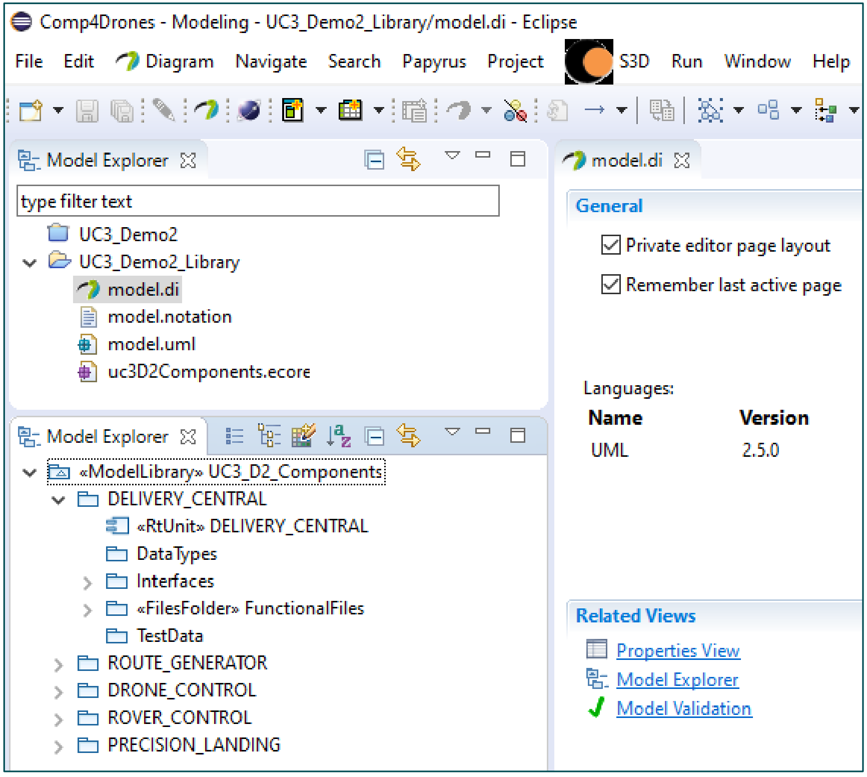


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- UML/MARTE System Modeling Methodology
- Platform-Independent
  - Flexible
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation
- Reusable
  - Library-based
  - Interface Inheritance



☑ Private editor page layout

☑ Remember last active page

Languages:

Name	Version
UML	2.5.0

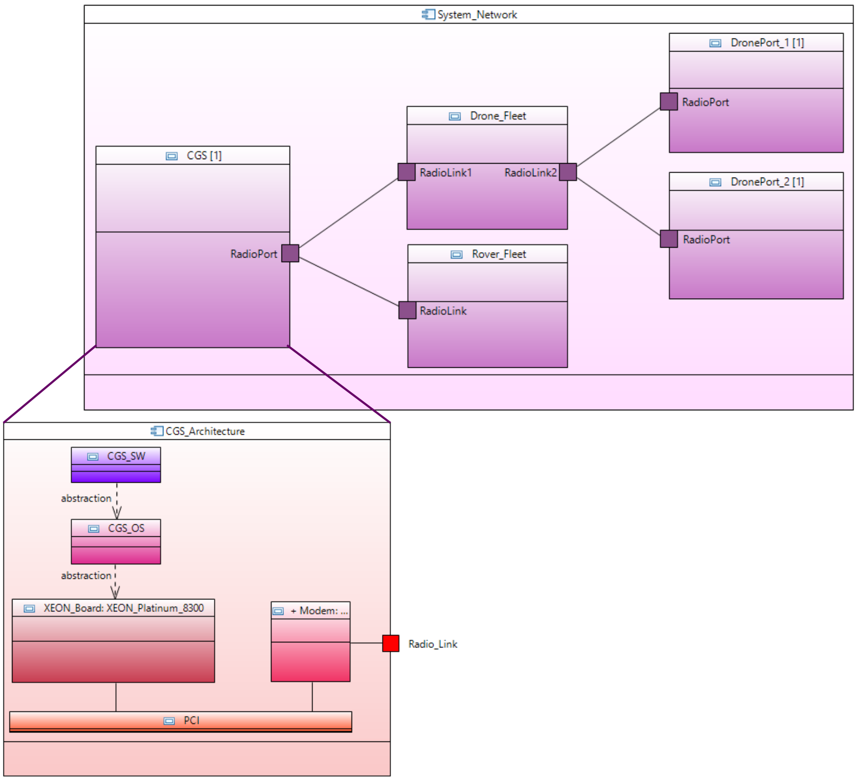
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- UML/MARTE System Modeling Methodology
- Platform-Independent
  - Flexible
- Component-Based
  - Supporting
    - Object-Orientation
    - Actor-Orientation
- Reusable
  - Library-based
  - Interface Inheritance
- Scalable
  - Hierarchical
    - Functionality
    - Execution Platform



CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

12

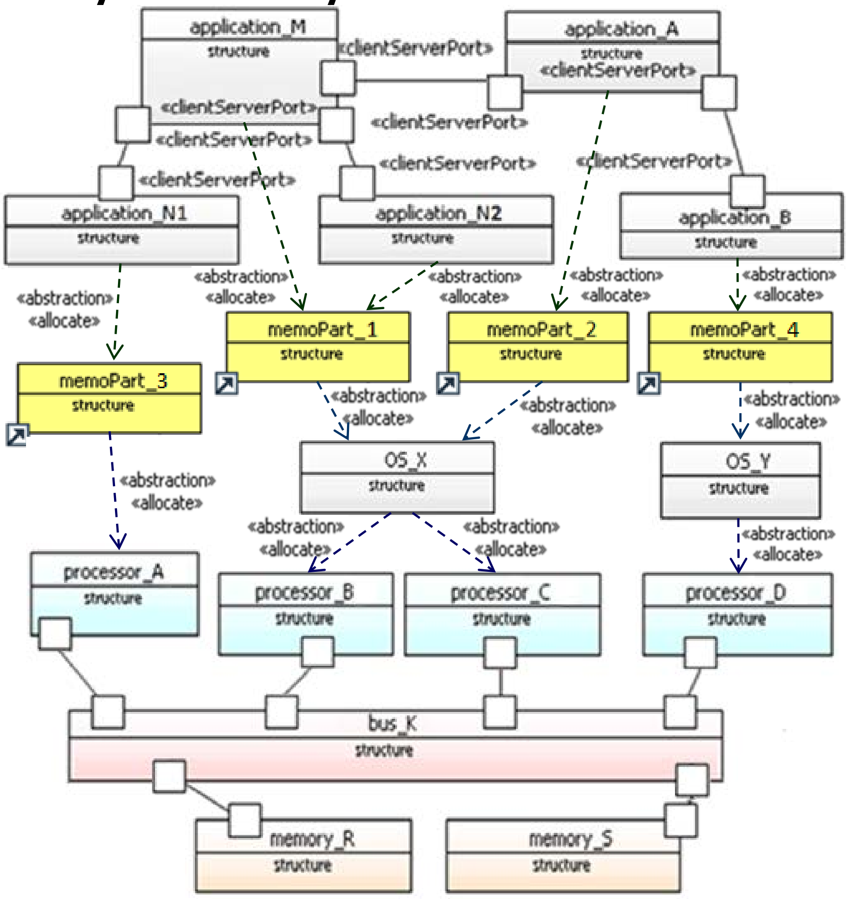
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Architectural (Functional) Design
- Code Reuse and/or Development
  - Platform Independent
- Architectural Mapping
- HW/SW Execution Platform



CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
CPS&IoT Budva, Montenegro, June 7-10, 2021

June 9, 2021

13

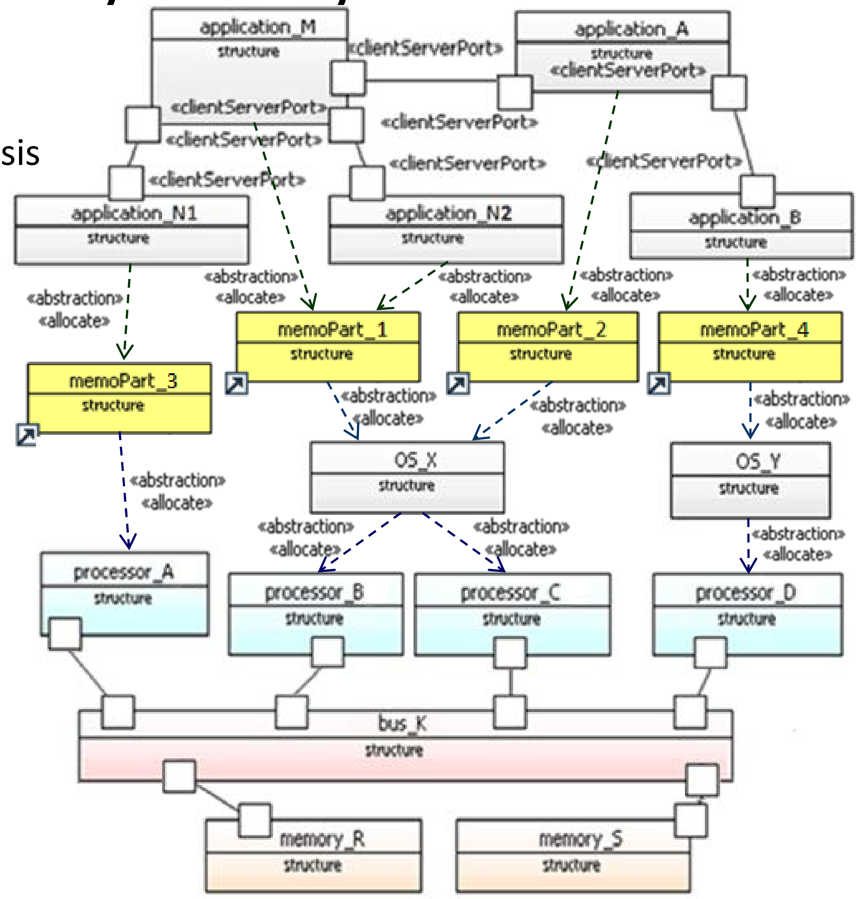
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

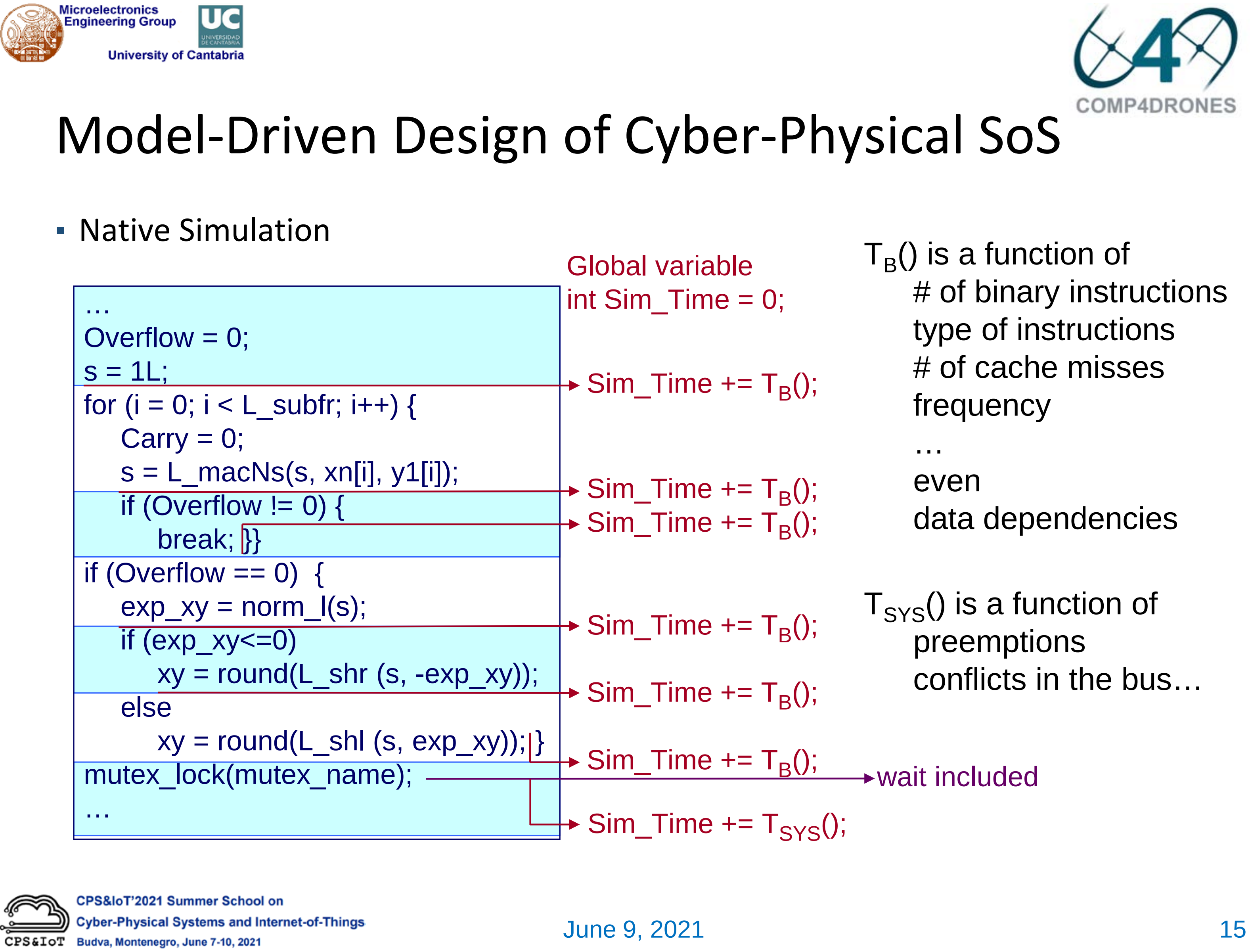
- Problem Statement
  - Fast Simulation & Performance Analysis
  - Before full SW Development
  - Along the design process
  - Multi-Level Simulation
- Native Simulation
  - Host-Compiled



CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things Budva, Montenegro, June 7-10, 2021

June 9, 2021

14



Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Native Simulation

Global variable
int Sim_Time = 0;

```
…
Overflow = 0;
s = 1L;
for (i = 0; i < L_subfr; i++) {
    Carry = 0;
    s = L_macNs(s, xn[i], y1[i]);
    if (Overflow != 0) {
        break; }}
if (Overflow == 0)  {
    exp_xy = norm_l(s);
    if (exp_xy<=0)
        xy = round(L_shr (s, -exp_xy));
    else
        xy = round(L_shl (s, exp_xy));}
mutex_lock(mutex_name);
…
```

Sim_Time += T_B();

Sim_Time += T_B();

Sim_Time += T_B();

Sim_Time += T_B();

Sim_Time += T_B();

Sim_Time += T_B();

wait included

Sim_Time += T_{SYS}();

T_B() is a function of
# of binary instructions
type of instructions
# of cache misses
frequency
…
even
data dependencies

T_{SYS}() is a function of
preemptions
conflicts in the bus…

CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021 15

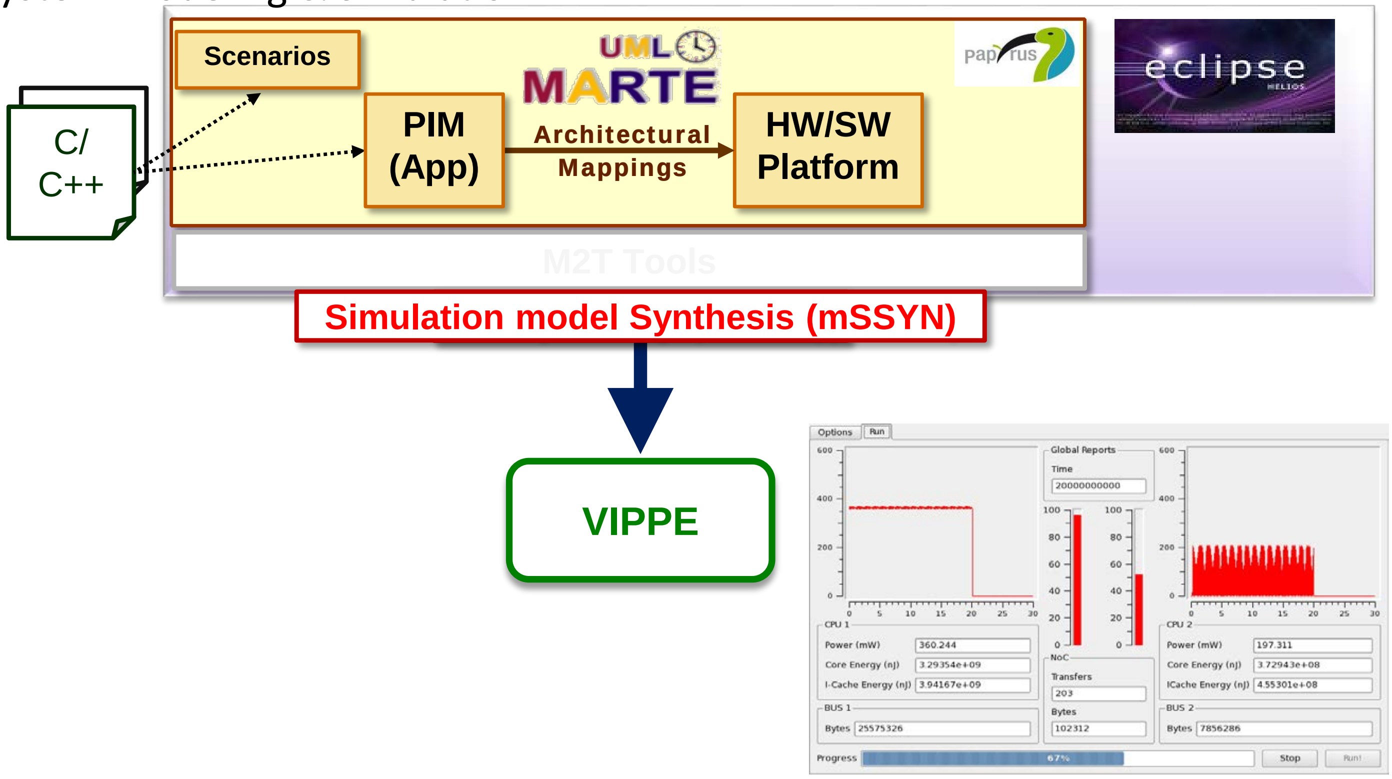
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- System Modeling & Simulation



Global Reports

Time 20000000000

CPU 1

Power (mW) 360.244

Core Energy (nJ) 3.29354e+09

I-Cache Energy (nJ) 3.94167e+09

BUS 1

Bytes 25575326

NoC

Transfers 203

Bytes 102312

CPU 2

Power (mW) 197.311

Core Energy (nJ) 3.72943e+08

ICache Energy (nJ) 4.55301e+08

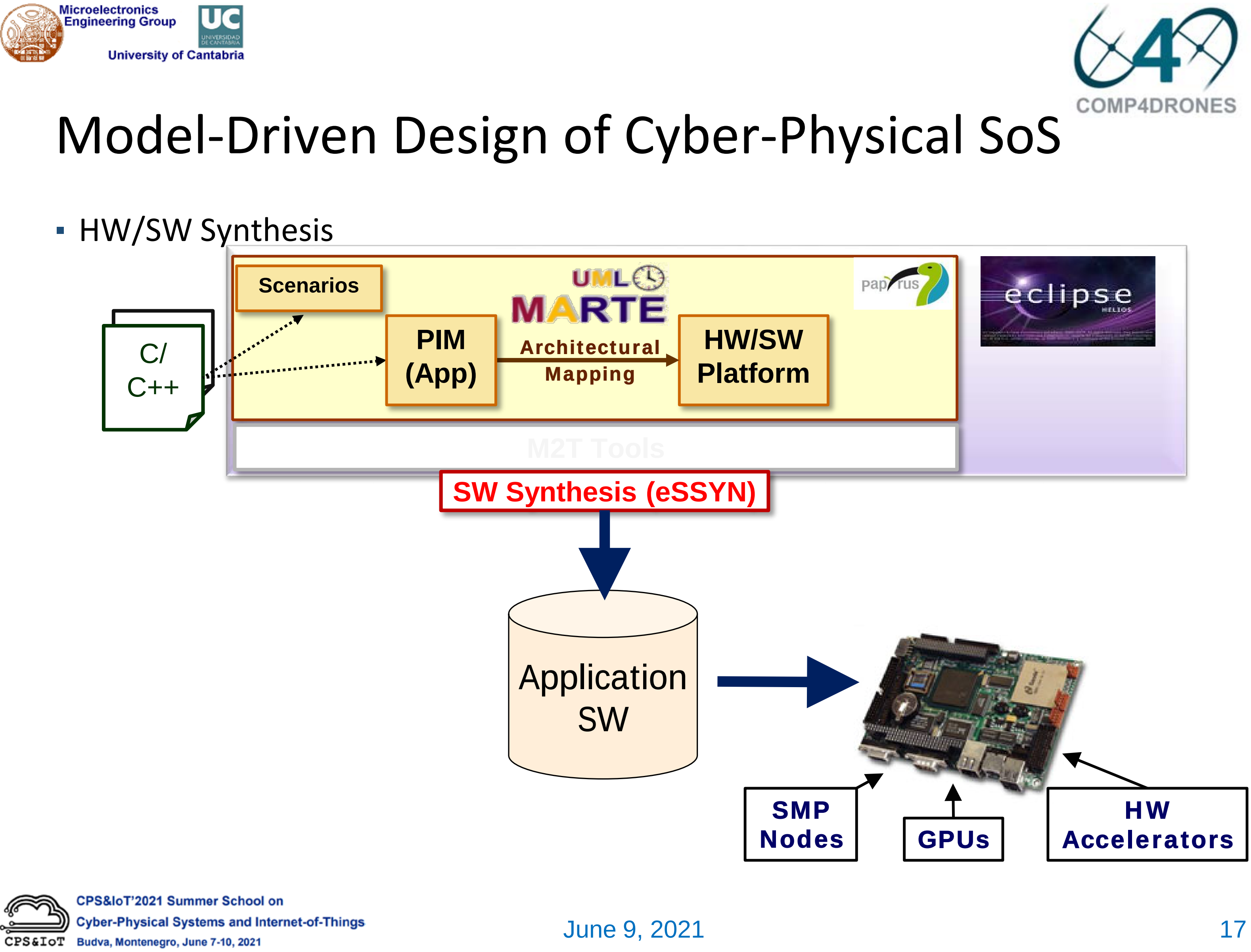
BUS 2

Bytes 7856286

Progress 67%

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021



Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- HW/SW Synthesis

C/ C++

Scenarios

UML MARTE

PIM (App)

Architectural Mapping

HW/SW Platform

papyrus

eclipse

M2T Tools

SW Synthesis (eSSYN)

Application SW

SMP Nodes

GPUs

HW Accelerators

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

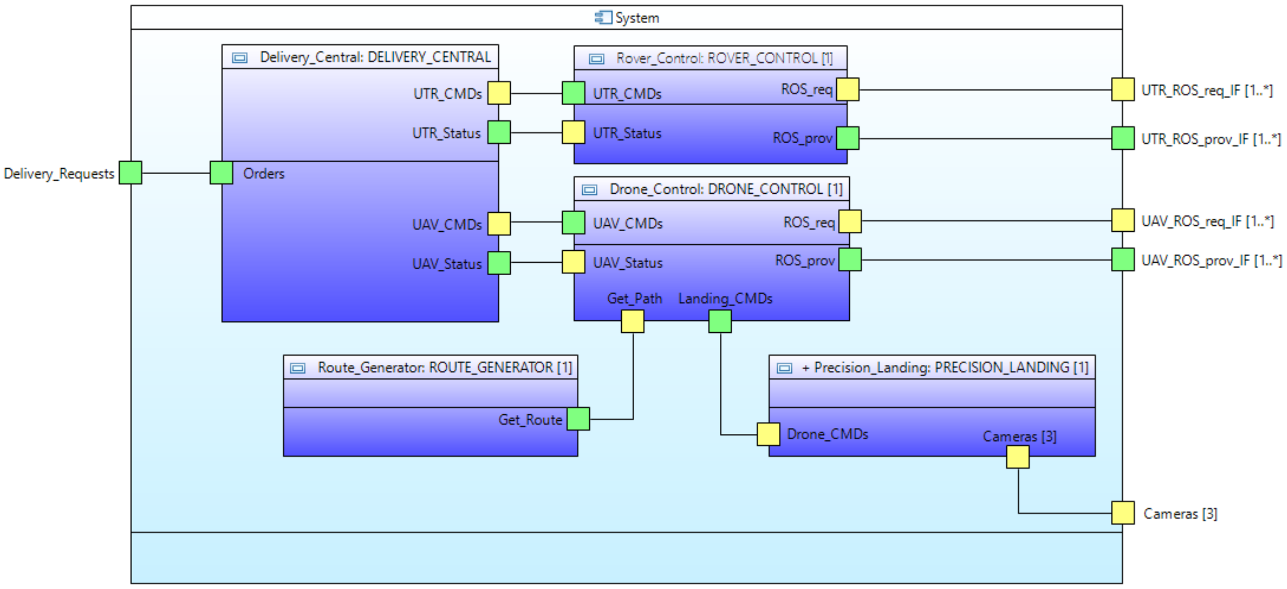
17

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Model-Driven Design of Cyber-Physical SoS

- Use case: A Delivery Service using rovers and drones
  - ROS is not an Operating System
    - ROS components
    - ROS infrastructure



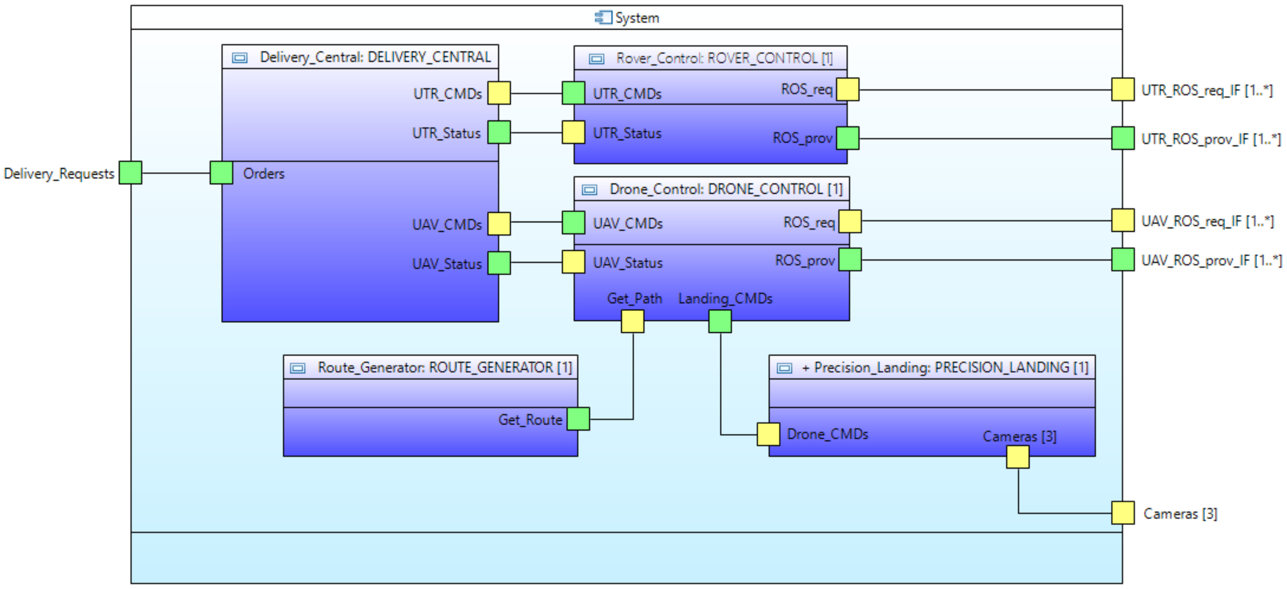
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- CPS: Digital Behavior in a Physical World
  - System Model (Specification)
    - The implementation is as good as similar to the model

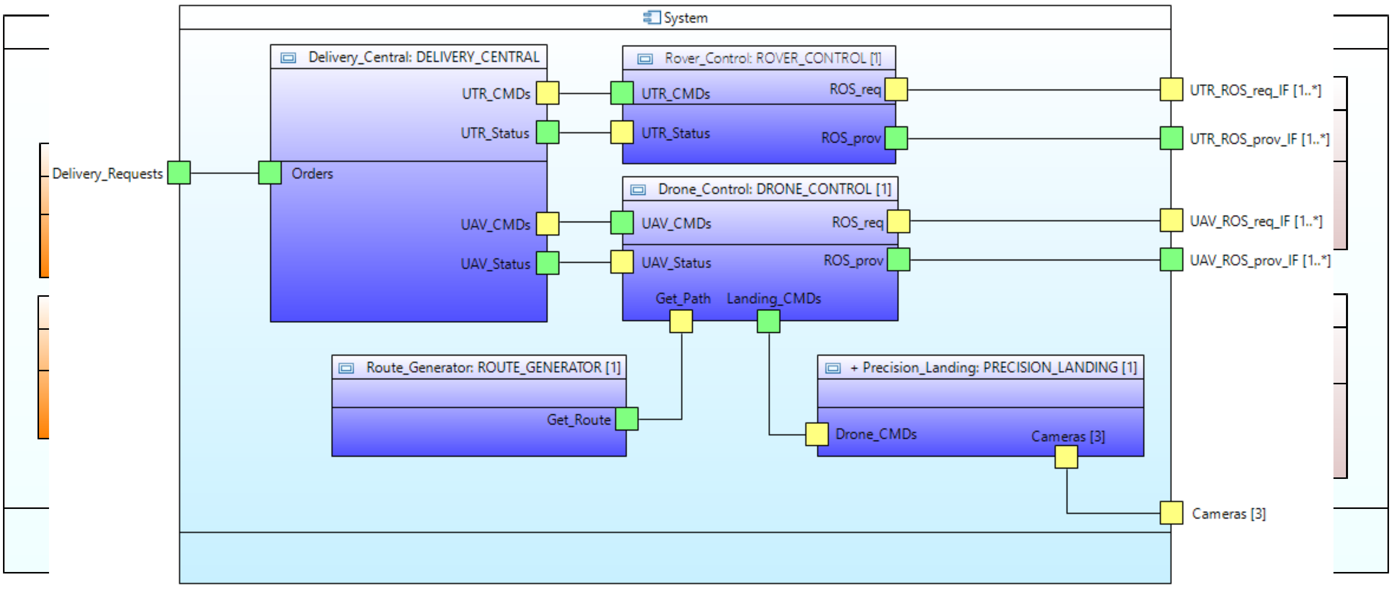


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- CPS: Digital Behavior in a Physical World
  - System Model (Specification)
    - The implementation is as good as similar to the model
  - Environment Model
    - The model is as good as similar to reality

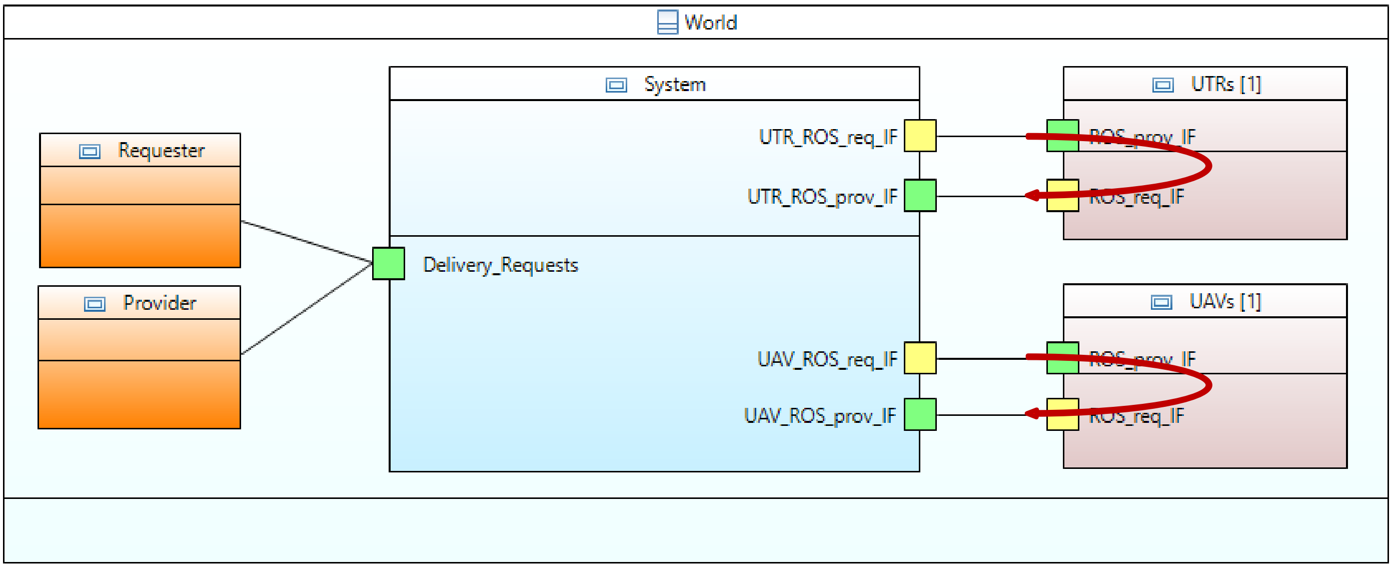


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- CPS: Digital Behavior in a Physical World
  - System Model (Specification)
    - The implementation is as good as similar to the model
  - Environment Model
    - The model is as good as similar to reality
    - Close-loop behavior can be extremely difficult to model

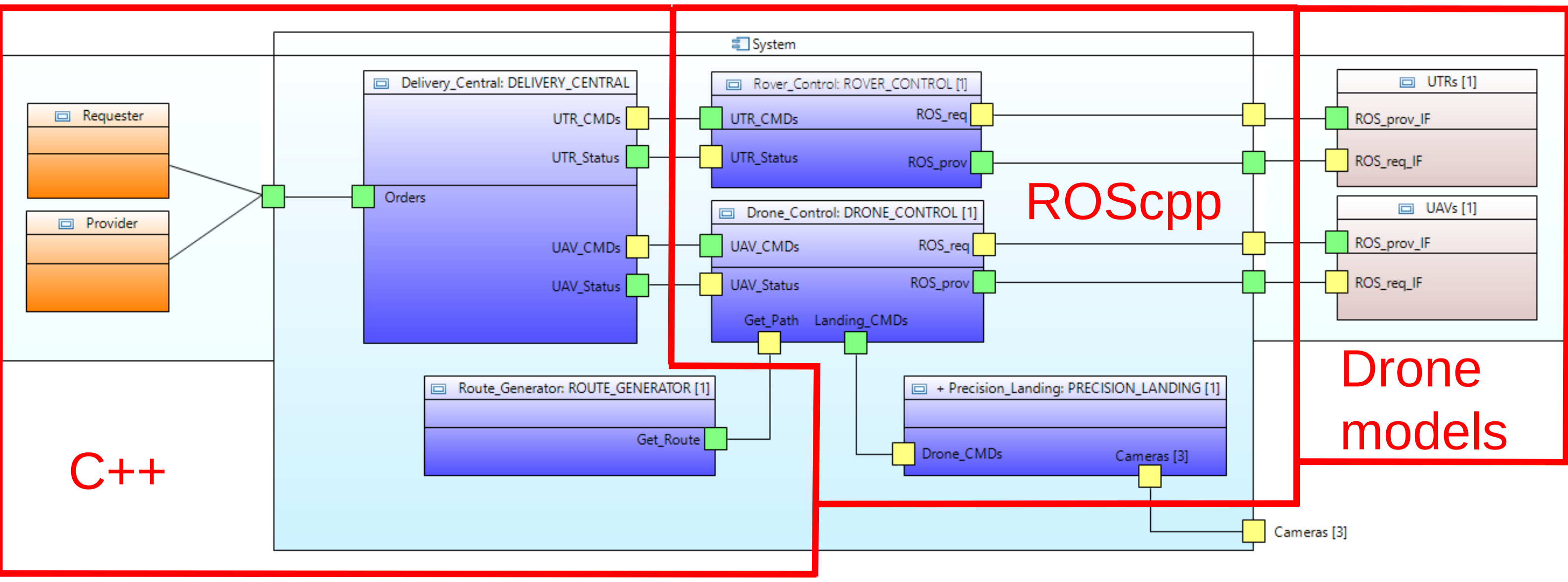


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

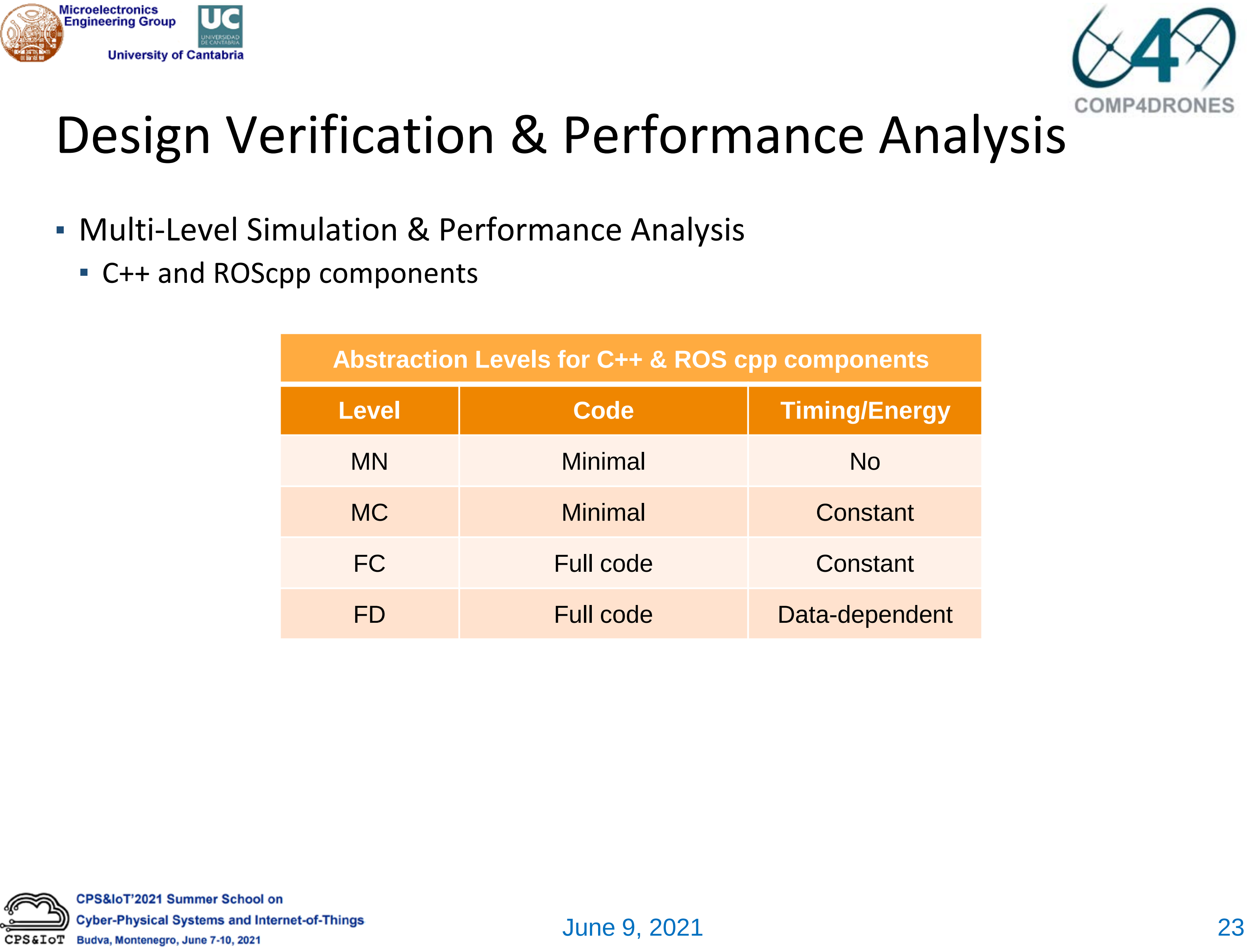
- S3D components in a drone-based service
  - C++ components
  - ROScpp components
  - Drone model



CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

22



Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

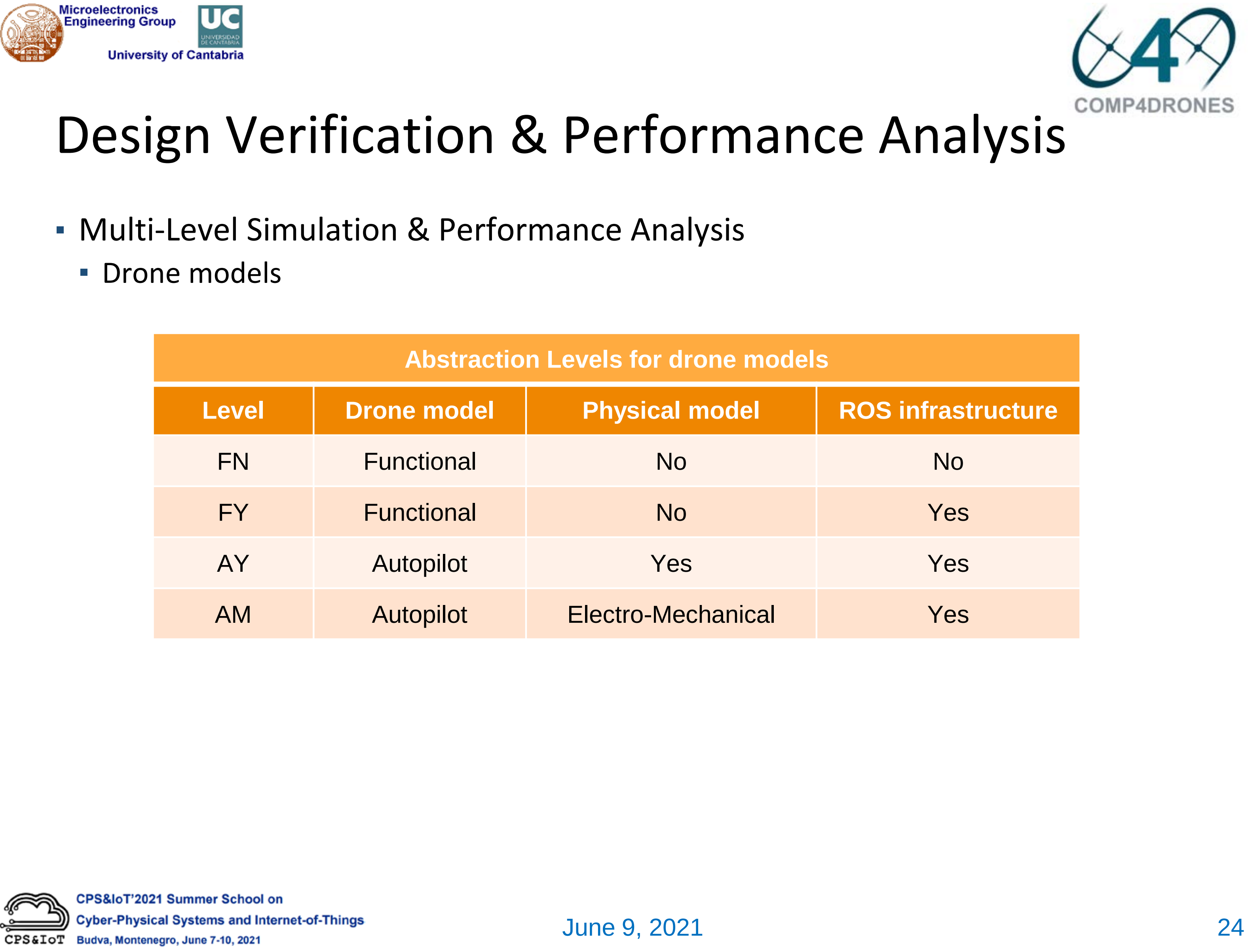
- Multi-Level Simulation & Performance Analysis
  - C++ and ROScpp components

Abstraction Levels for C++ & ROS cpp components		
Level	**Code**	**Timing/Energy**
MN	Minimal	No
MC	Minimal	Constant
FC	Full code	Constant
FD	Full code	Data-dependent

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things Budva, Montenegro, June 7-10, 2021

June 9, 2021

23



Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Drone models

Abstraction Levels for drone models			
Level	**Drone model**	**Physical model**	**ROS infrastructure**
FN	Functional	No	No
FY	Functional	No	Yes
AY	Autopilot	Yes	Yes
AM	Autopilot	Electro-Mechanical	Yes

CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

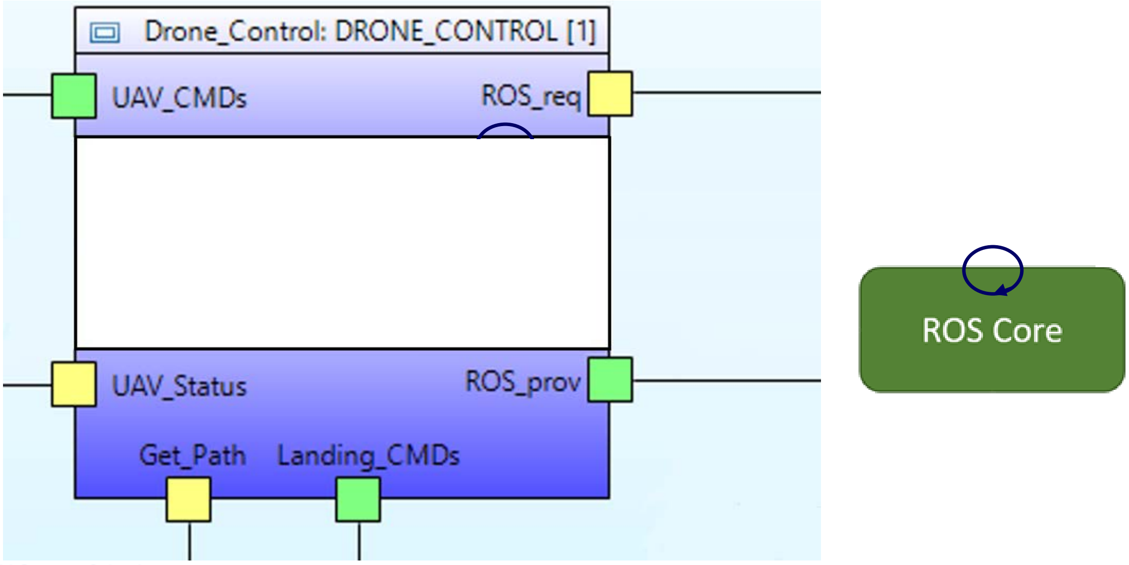
24

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Performance Analysis of ROScpp components
  - Native simulation of C++ code
  - Constant time/energy for ROS method calls
    - Dependent on the CPU
    - Dependent on the number of nodes and subscribers
    - Part to be assigned to the component
    - Part to be assigned to the server executing the ROScore

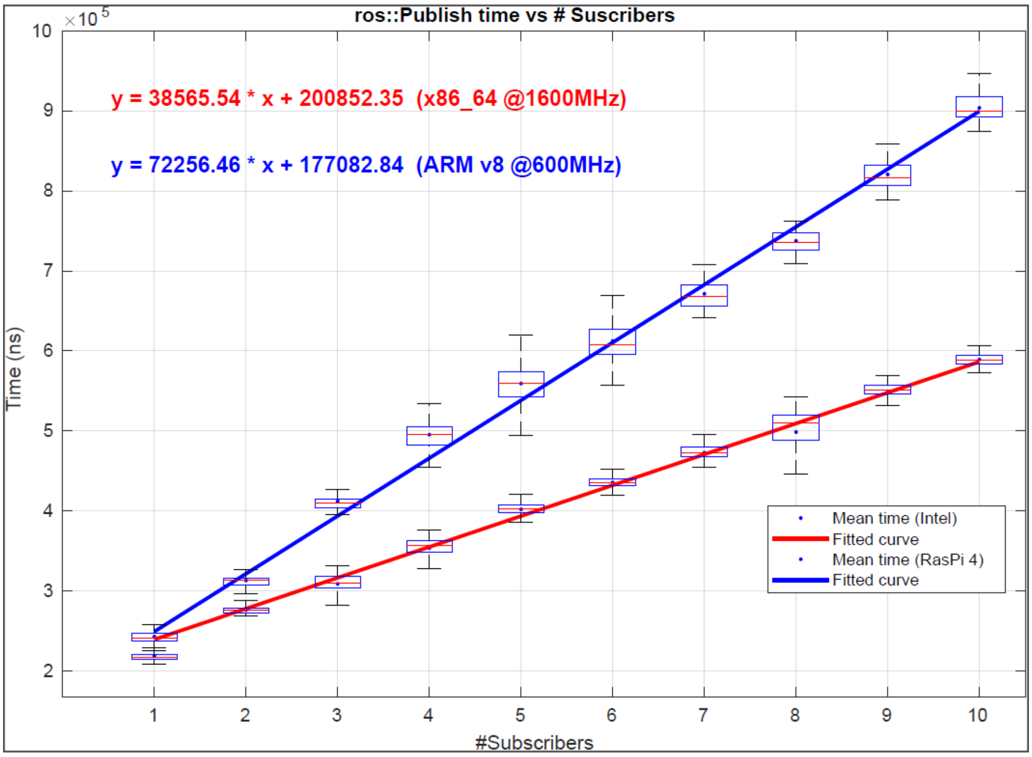


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Performance Analysis of ROScpp components
  - Time/energy for ROS method calls at the component



CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

26

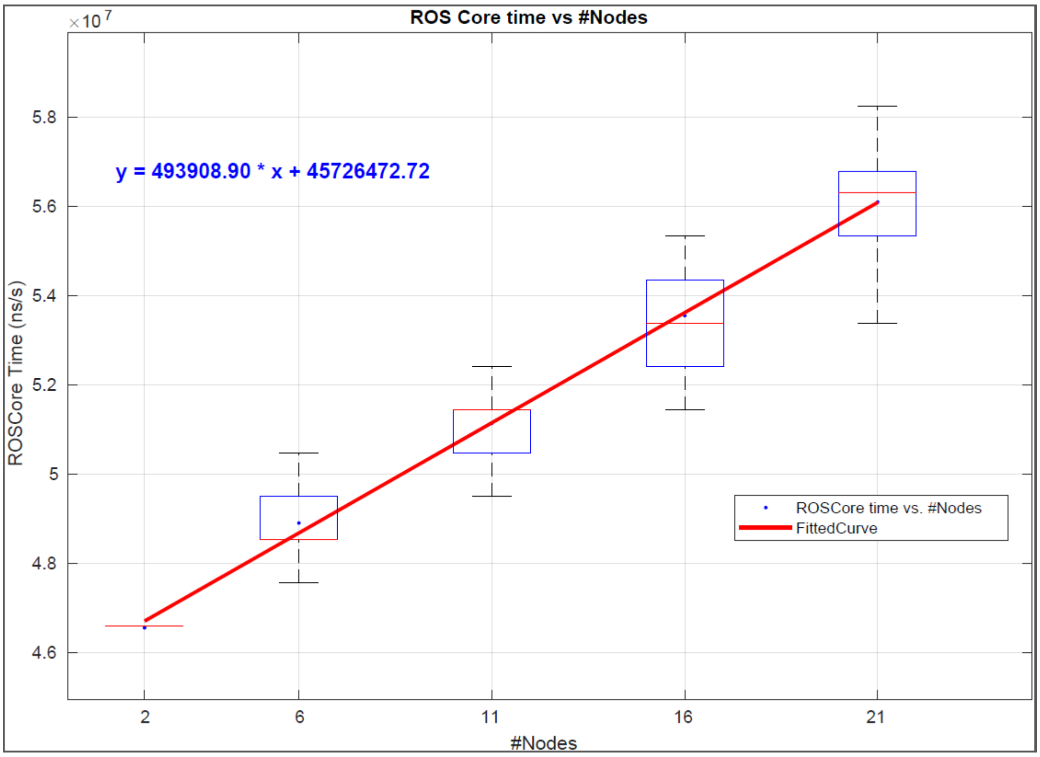
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Performance Analysis of ROScpp components
  - Time/energy for ROS method calls at ROScore

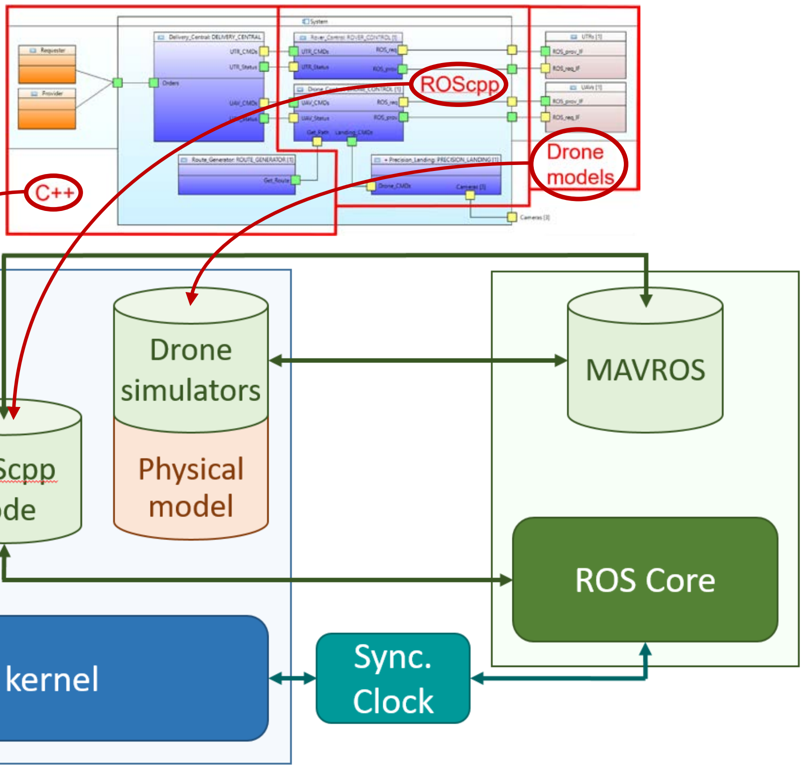


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Simulation Infrastructure
    - General architecture

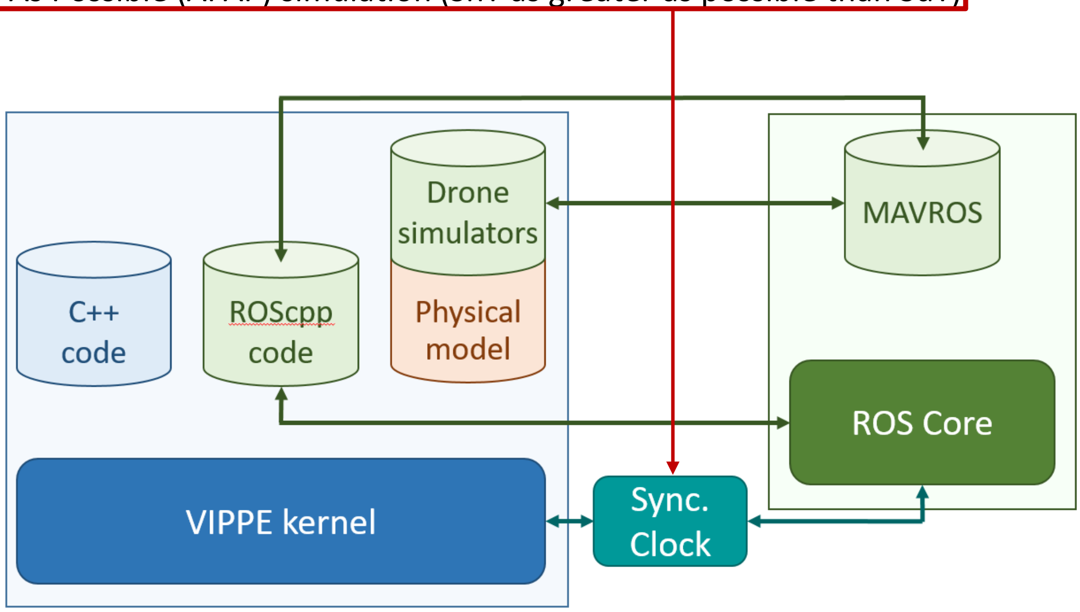


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Simulation Infrastructure
    - General architecture
    - Real-Time (RT) simulation- simulation time = simulated time (SnT = SdT)
    - As Fast As Possible (AFAP) simulation (SnT as greater as possible than SdT)

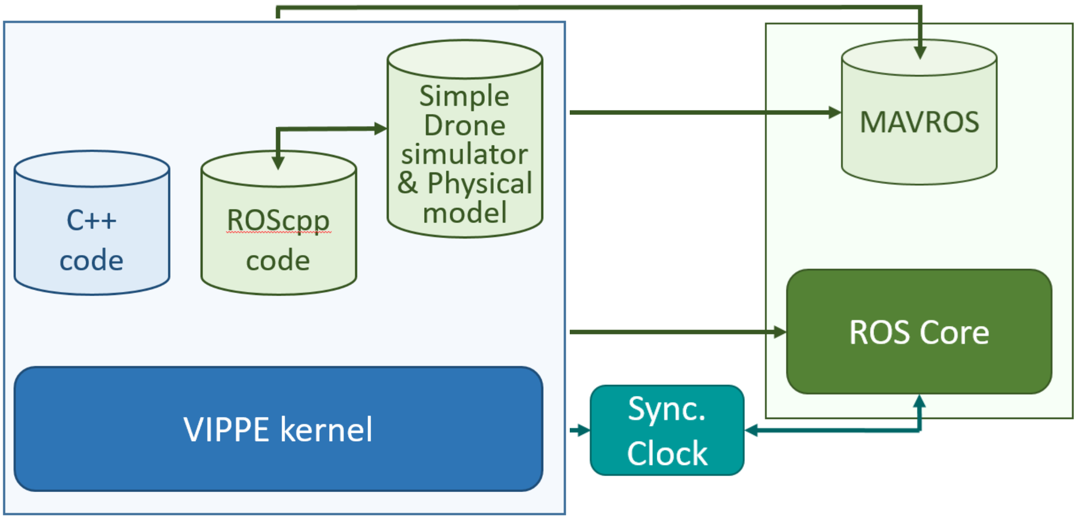


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Simulation Infrastructure
    - Functional drone modeling
    - Without ROS (FN)
    - Any C++ and ROScpp models (MN + MC + FC + FD)



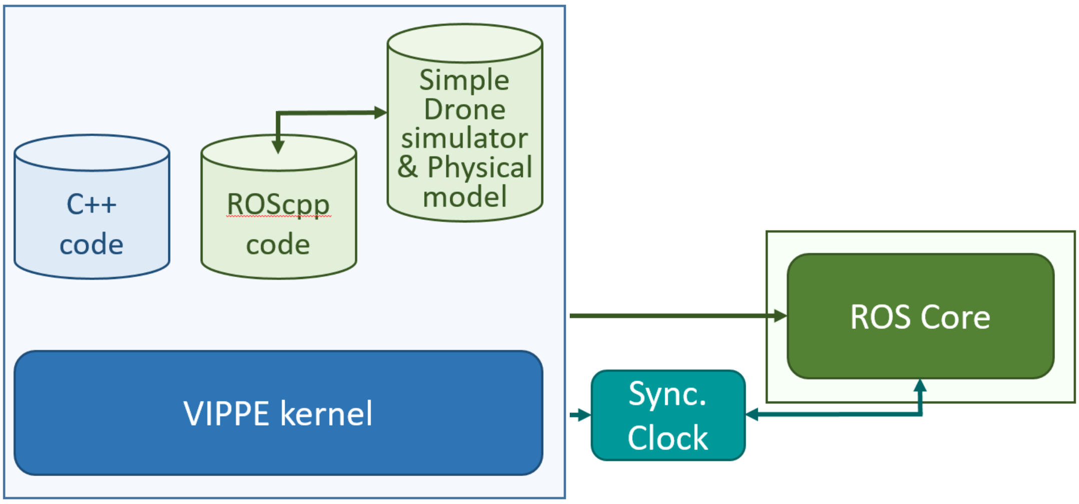
Microelectronics Engineering Group

University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Simulation Infrastructure
    - Functional drone modeling
    - With ROS (FY)
    - Any C++ and ROScpp models (MN + MC + FC + FD)

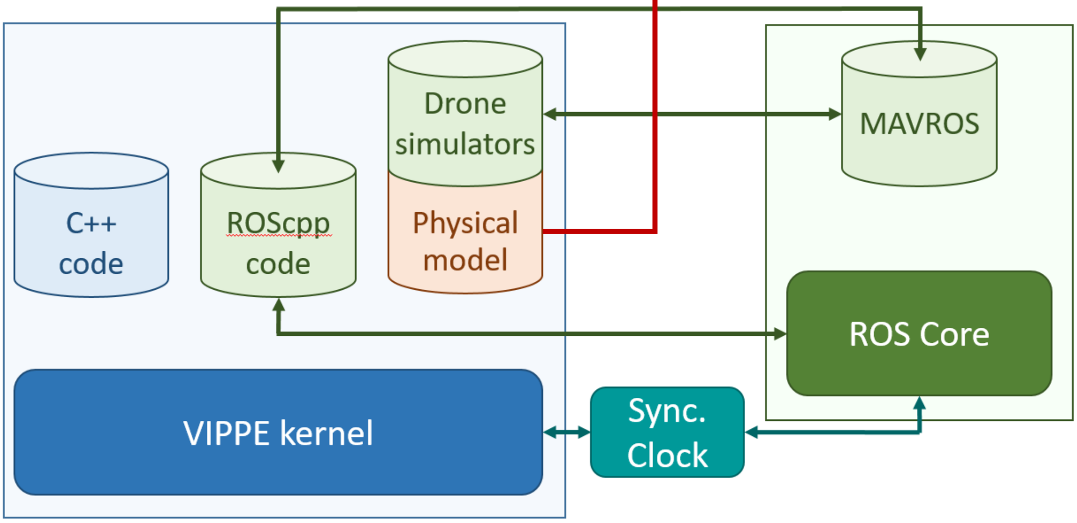


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Design Verification & Performance Analysis

- Multi-Level Simulation & Performance Analysis
  - Simulation Infrastructure
    - Realistic drone modeling (Autopilot + Physics)
    - With ROS (AY + AM)
    - Any C++ and ROScpp models (MN + MC + FC + FD)
    - With or without 3D Graphics

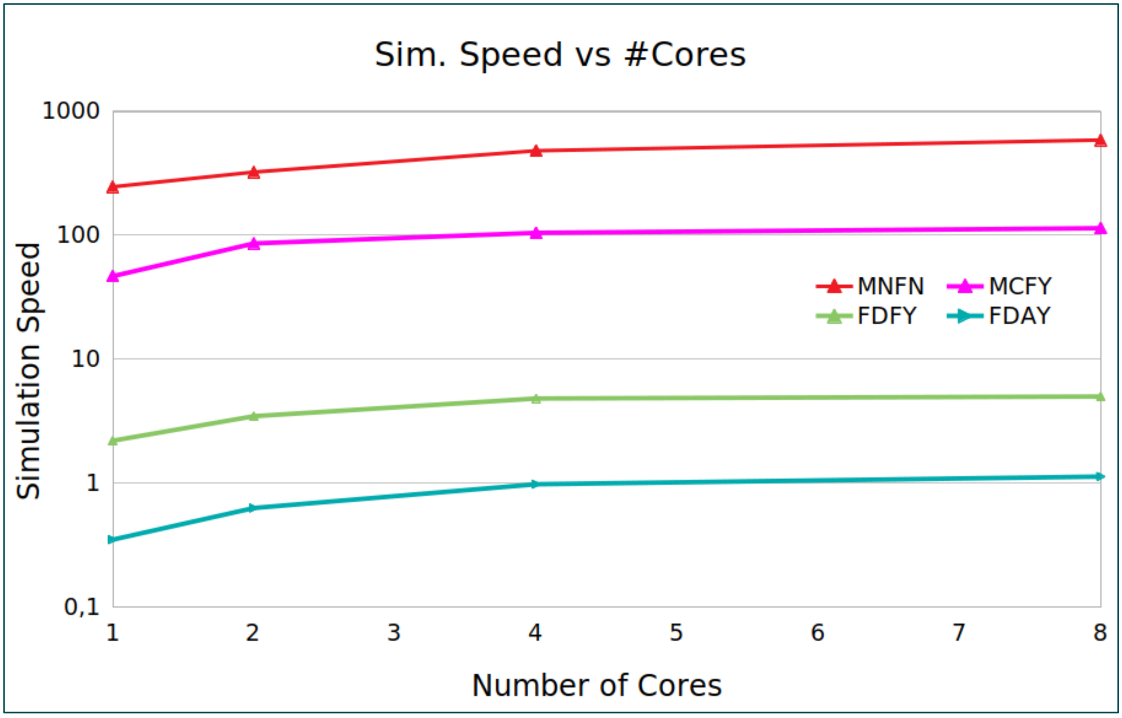


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Simulation Results

- Multi-Level Simulation
  - Impact of an increasing number of host CPUs (8 drones)

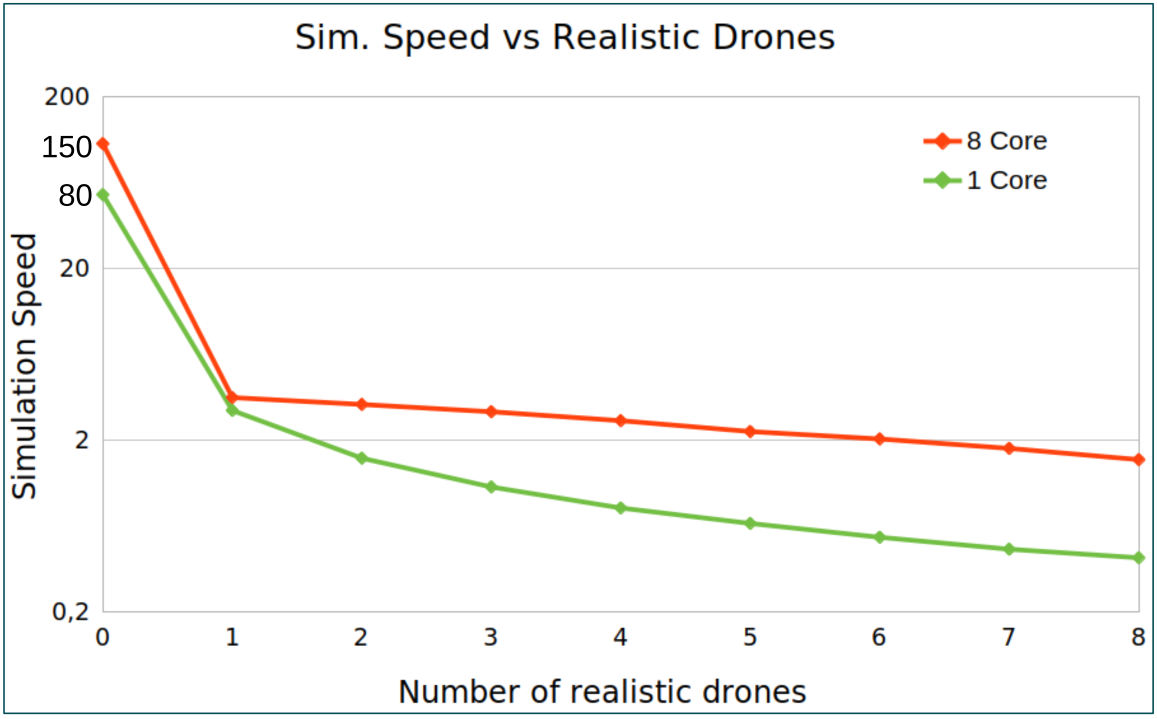


Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Simulation Results

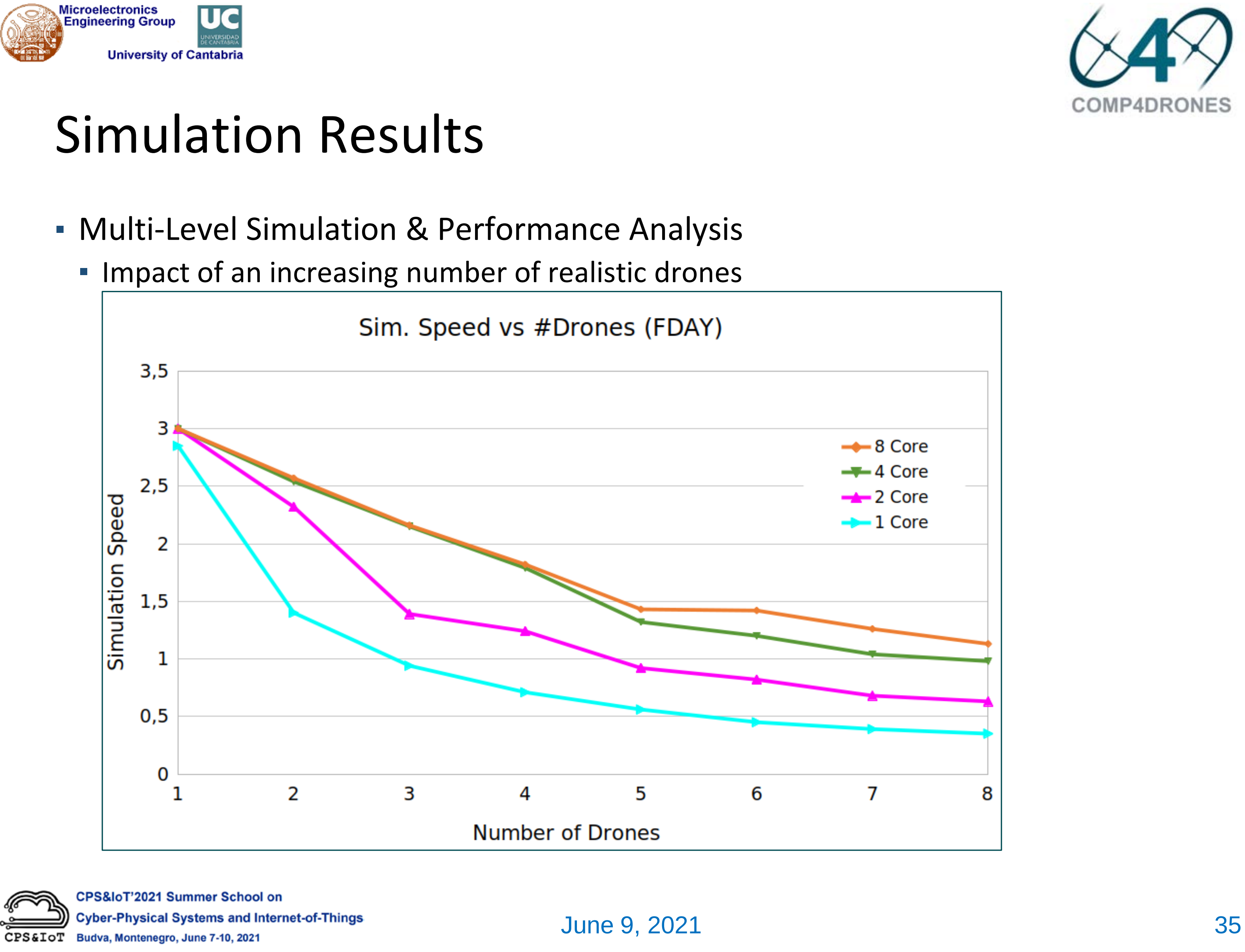
- Multi-Level Simulation
  - Impact of an increasing number or realistic vs functional drones



CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

June 9, 2021

34



Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Simulation Results

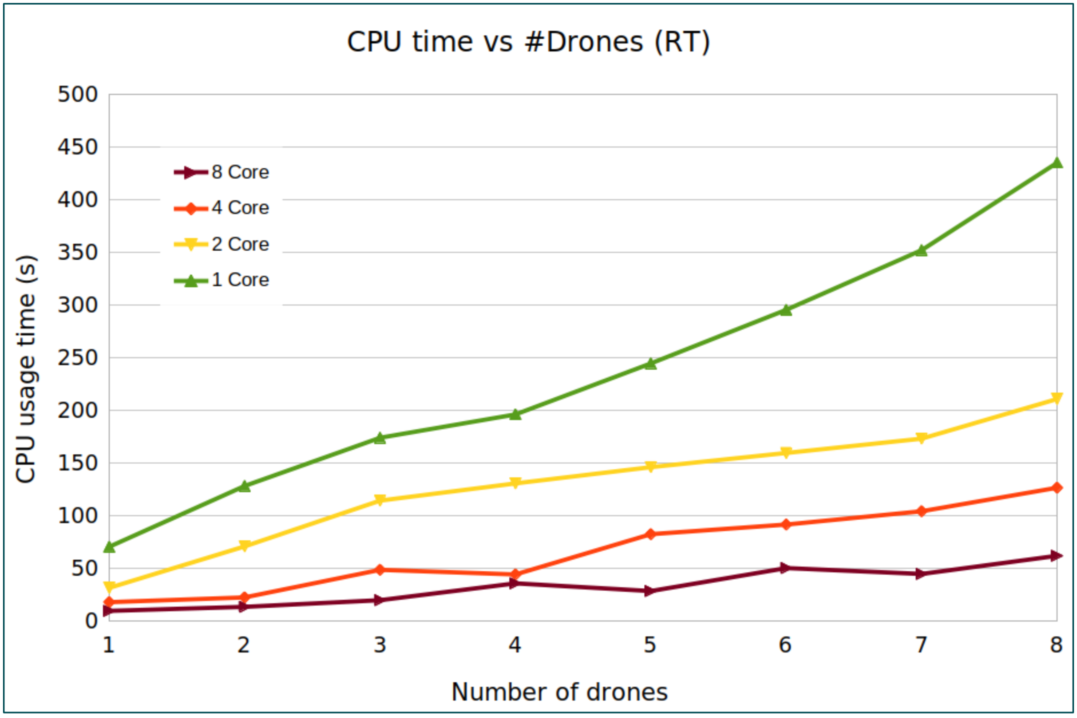
- Multi-Level Simulation & Performance Analysis
  - Impact of an increasing number of realistic drones

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Simulation Results

- Real-Time Simulation in seconds
    - Impact of an increasing number of realistic drones



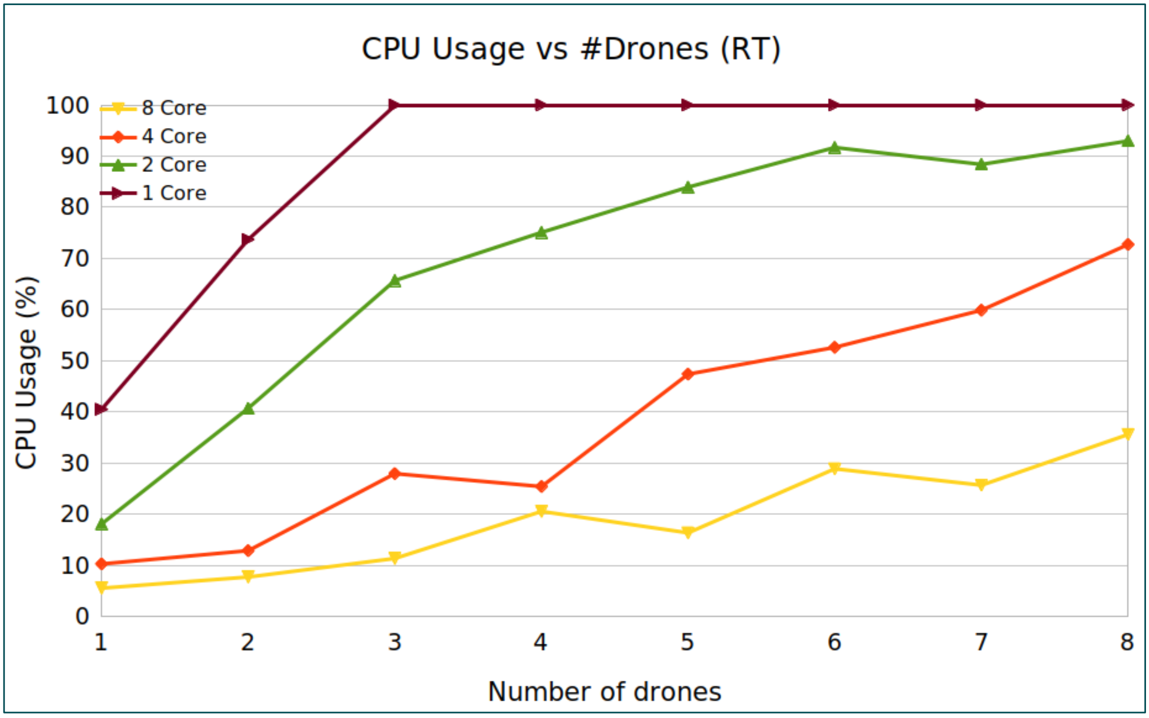
Microelectronics Engineering Group

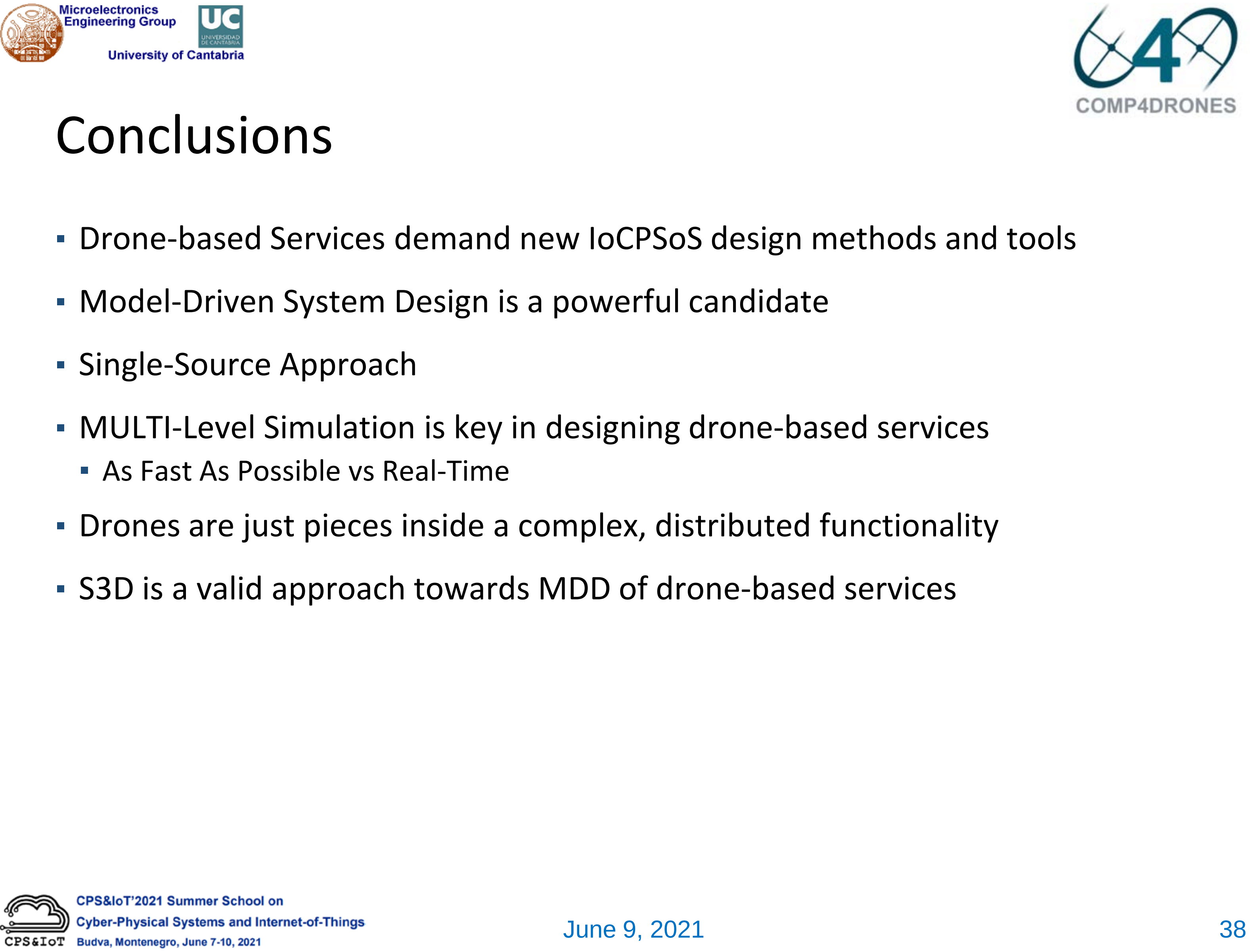
University of Cantabria

COMP4DRONES

Simulation Results

- Real-Time Simulation in % of CPU usage
  - Impact of an increasing number of realistic drones





Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

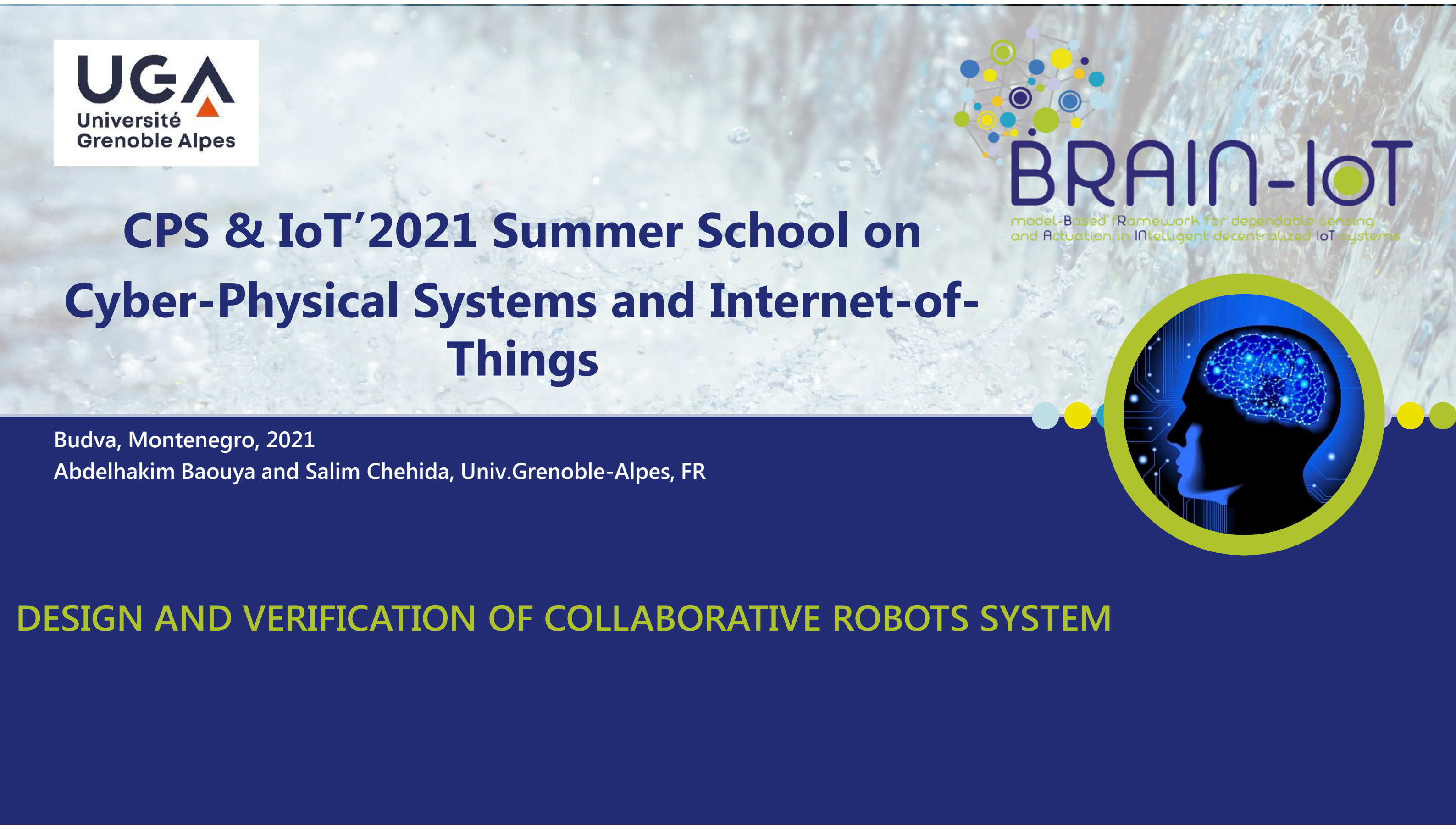
Conclusions

- Drone-based Services demand new IoCPSoS design methods and tools
- Model-Driven System Design is a powerful candidate
- Single-Source Approach
- MULTI-Level Simulation is key in designing drone-based services
  - As Fast As Possible vs Real-Time
- Drones are just pieces inside a complex, distributed functionality
- S3D is a valid approach towards MDD of drone-based services

Microelectronics Engineering Group
University of Cantabria

COMP4DRONES

Any comment/question?



UGA Université Grenoble Alpes

BRAIN-IoT
model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems

CPS & IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things

Budva, Montenegro, 2021
Abdelhakim Baouya and Salim Chehida, Univ.Grenoble-Alpes, FR

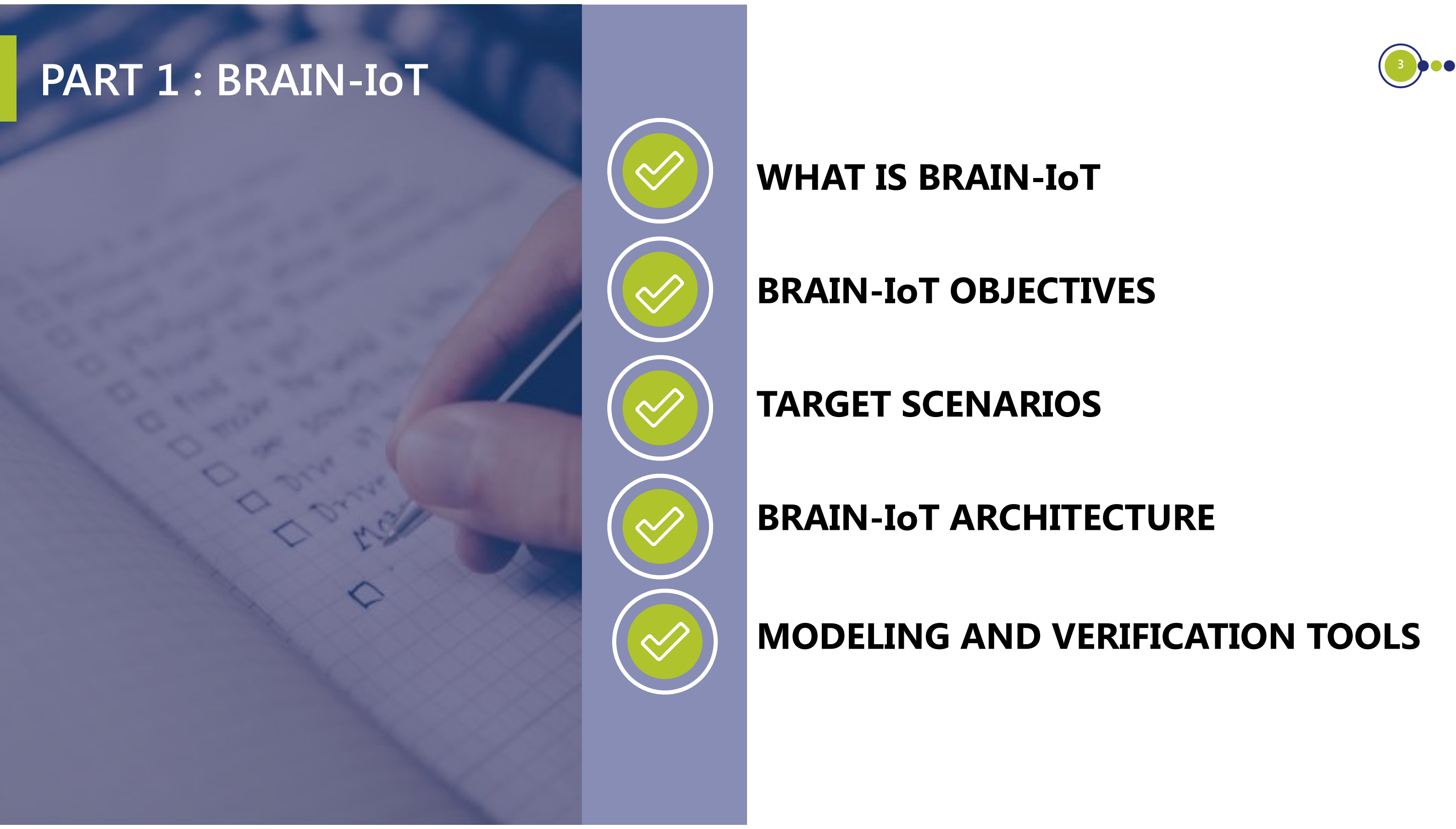
DESIGN AND VERIFICATION OF COLLABORATIVE ROBOTS SYSTEM

CONTENTS

✓ **PART 1 : BRAINT-IoT**

✓ **PART 2 : IoT CONCEPTS AND ARCHITECTURE**

✓ **PART 3 : PROJECTION OVER A REAL CASE STUDY**



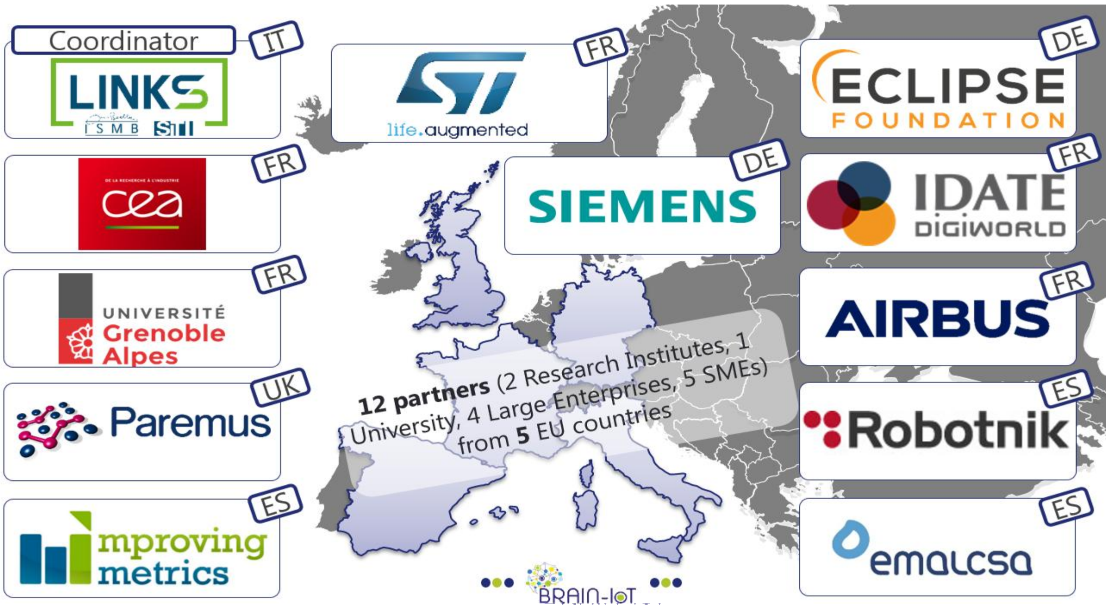
PART 1 : BRAIN-IoT

3

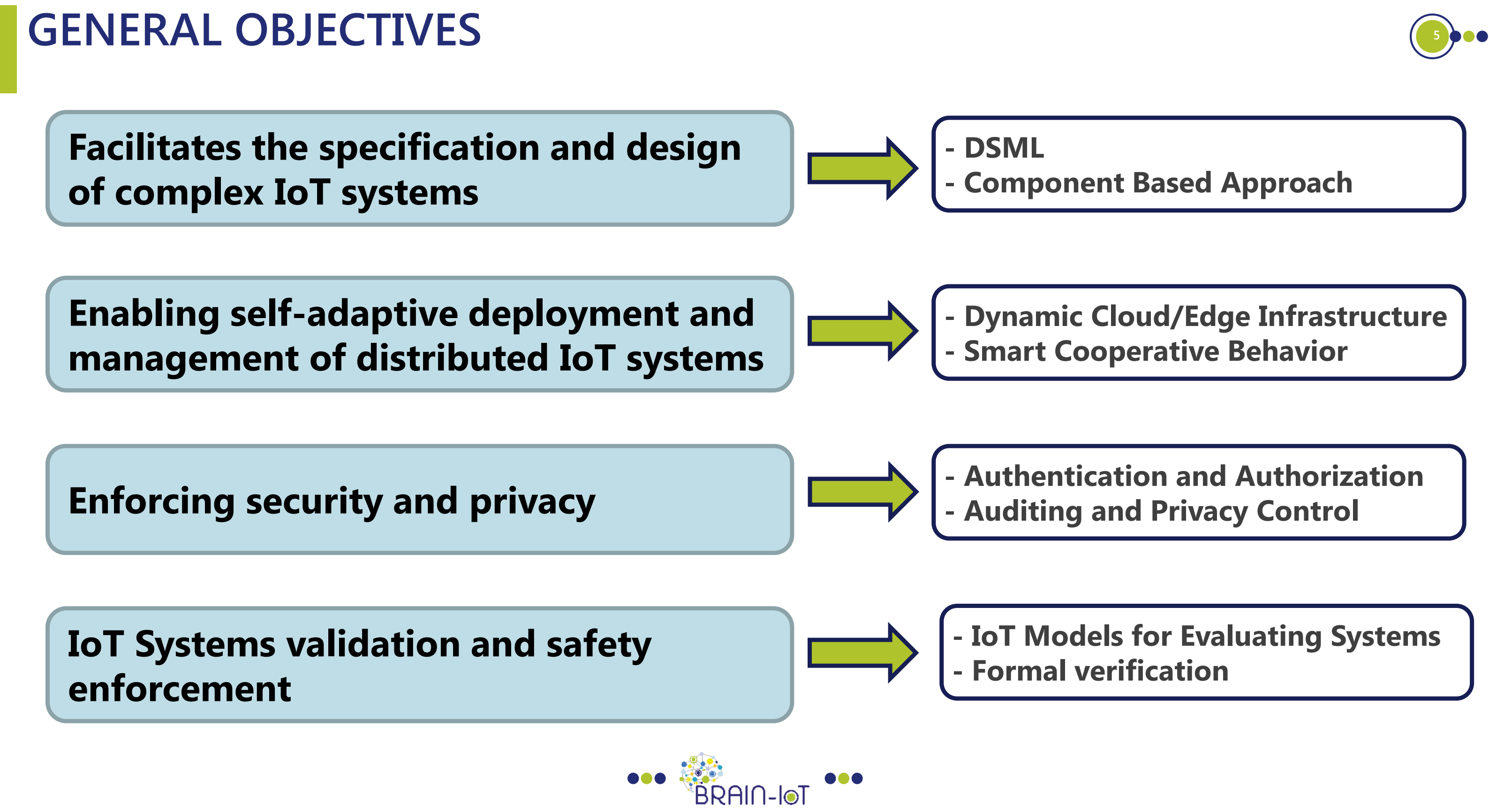
- ✓ WHAT IS BRAIN-IoT
- ✓ BRAIN-IoT OBJECTIVES
- ✓ TARGET SCENARIOS
- ✓ BRAIN-IoT ARCHITECTURE
- ✓ MODELING AND VERIFICATION TOOLS

THE BRAIN-IoT PROJECT

BRAIN-IoT aims at reducing the effort of developing, validating, operating and monitoring IoT-based Systems



12 partners (2 Research Institutes, 1 University, 4 Large Enterprises, 5 SMEs) from **5** EU countries



GENERAL OBJECTIVES

5

Facilitates the specification and design of complex IoT systems →
- DSML
- Component Based Approach

Enabling self-adaptive deployment and management of distributed IoT systems →
- Dynamic Cloud/Edge Infrastructure
- Smart Cooperative Behavior

Enforcing security and privacy →
- Authentication and Authorization
- Auditing and Privacy Control

IoT Systems validation and safety enforcement →
- IoT Models for Evaluating Systems
- Formal verification

BRAIN-IoT

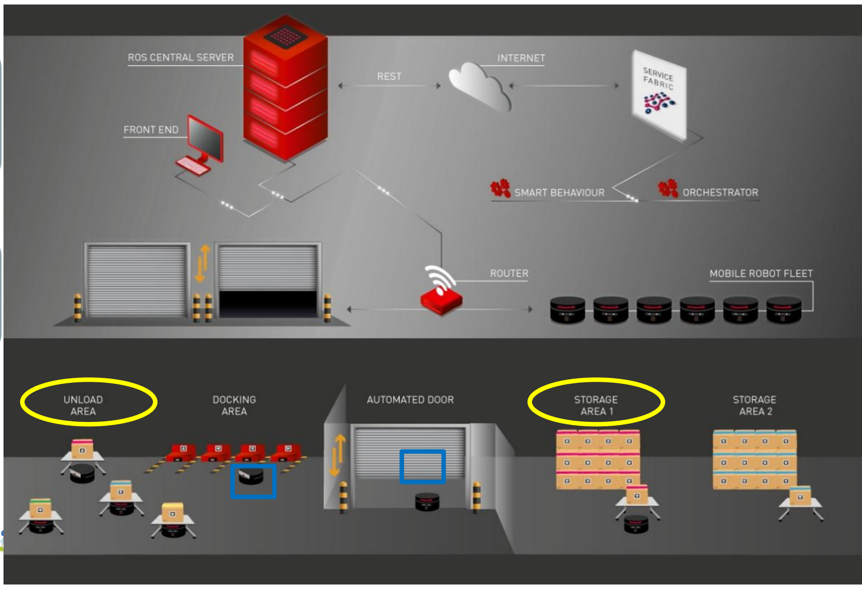
TARGET SCENARIOS (SERVICE ROBOTICS)

Management a fleet of robot that support the movement of different loads, with different challenges and configurations

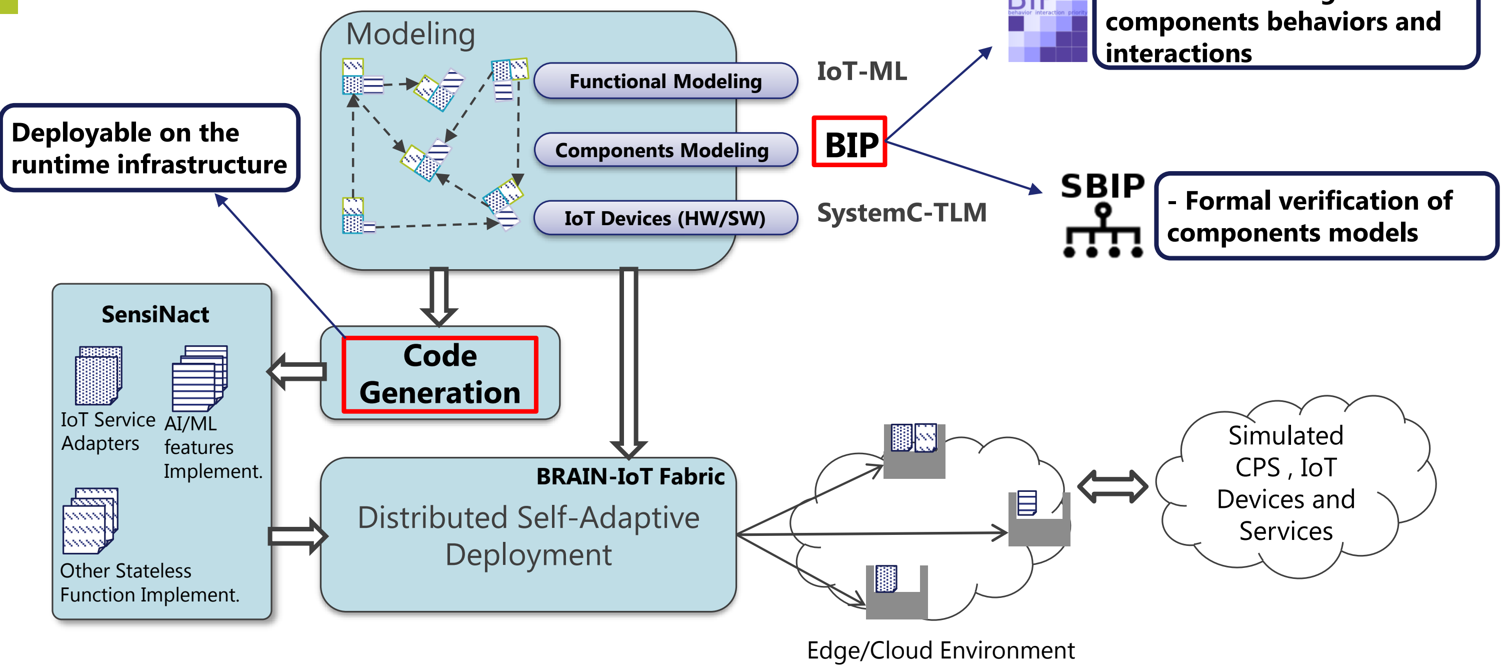
- The robots empty continuously "unload area" where the different loads are brought.

- A specific robot is asked to pick item and place it in a designated storage area

- Door is automatically open in the middle of robot path to storage areas.



BRAIN-IOT CONCEPT AND ARCHITECTURE



Modeling

Functional Modeling

Components Modeling

IoT Devices (HW/SW)

IoT-ML

BIP

SystemC-TLM

- Formal Modeling of IoT components behaviors and interactions

SBIP

- Formal verification of components models

Deployable on the runtime infrastructure

SensiNact

IoT Service Adapters

AI/ML features Implement.

Other Stateless Function Implement.

Code Generation

BRAIN-IoT Fabric

Distributed Self-Adaptive Deployment

Edge/Cloud Environment

Simulated CPS , IoT Devices and Services

BIP LANGUAGE

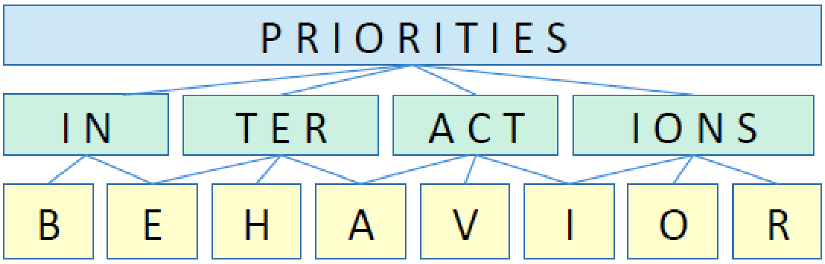
- Highly expressive component-based language
- Separation between architecture and behavior
- Complex system modeling and analysis

Components = layered composition of

– Behavior, atomic functional units (automata + code + timing constraints, stochastic semantic)

– Interactions, cooperation between actions of behavior

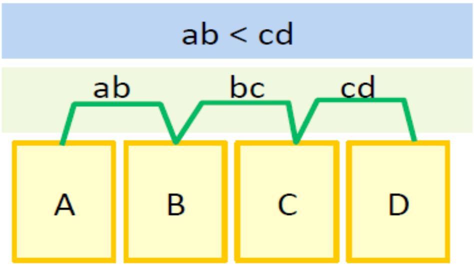
– Priorities, conflict resolution between interactions

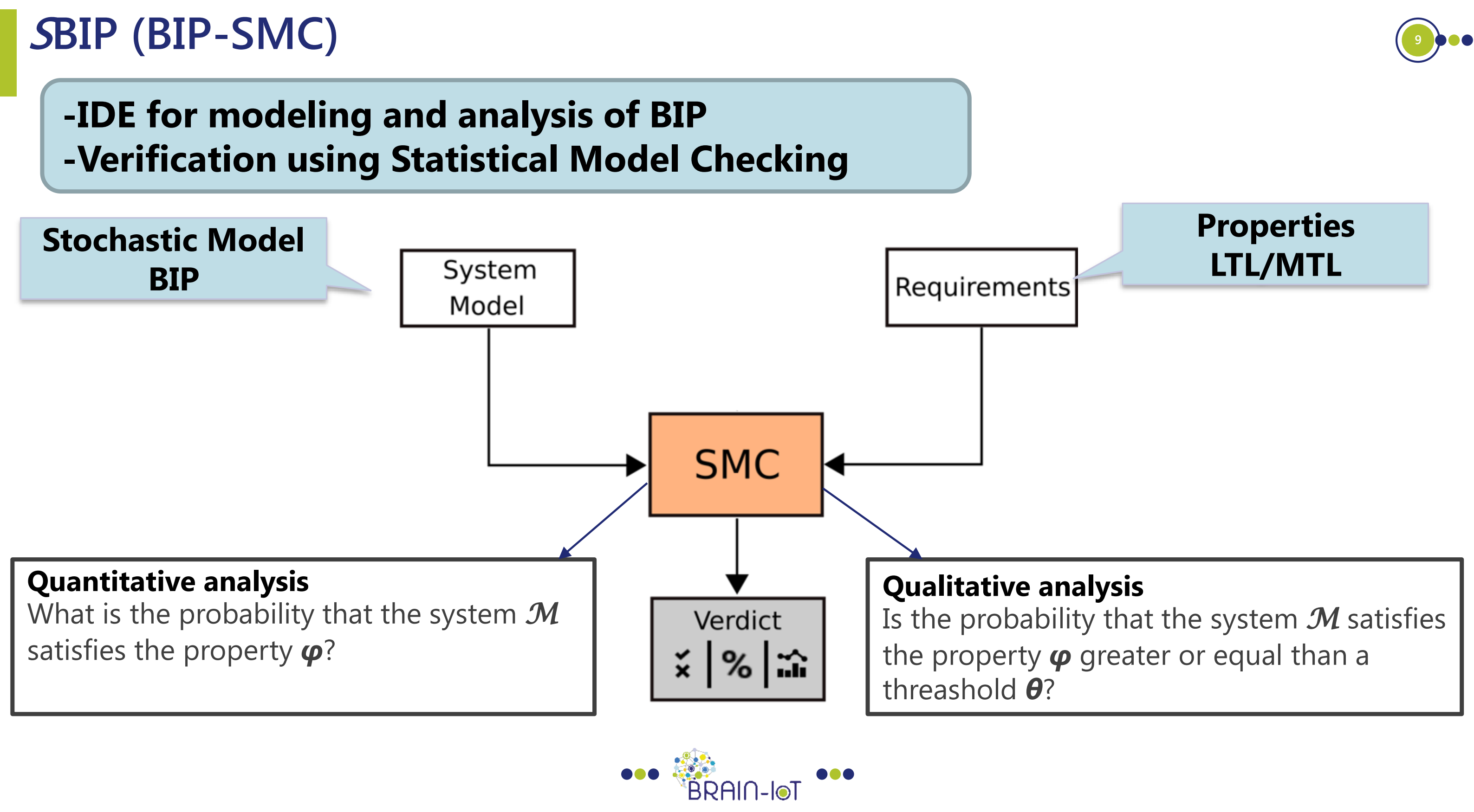


PRIORITIES

IN TER ACT IONS

B E H A V I O R





SBIP (BIP-SMC)

-IDE for modeling and analysis of BIP
-Verification using Statistical Model Checking

Stochastic Model BIP

System Model

Requirements

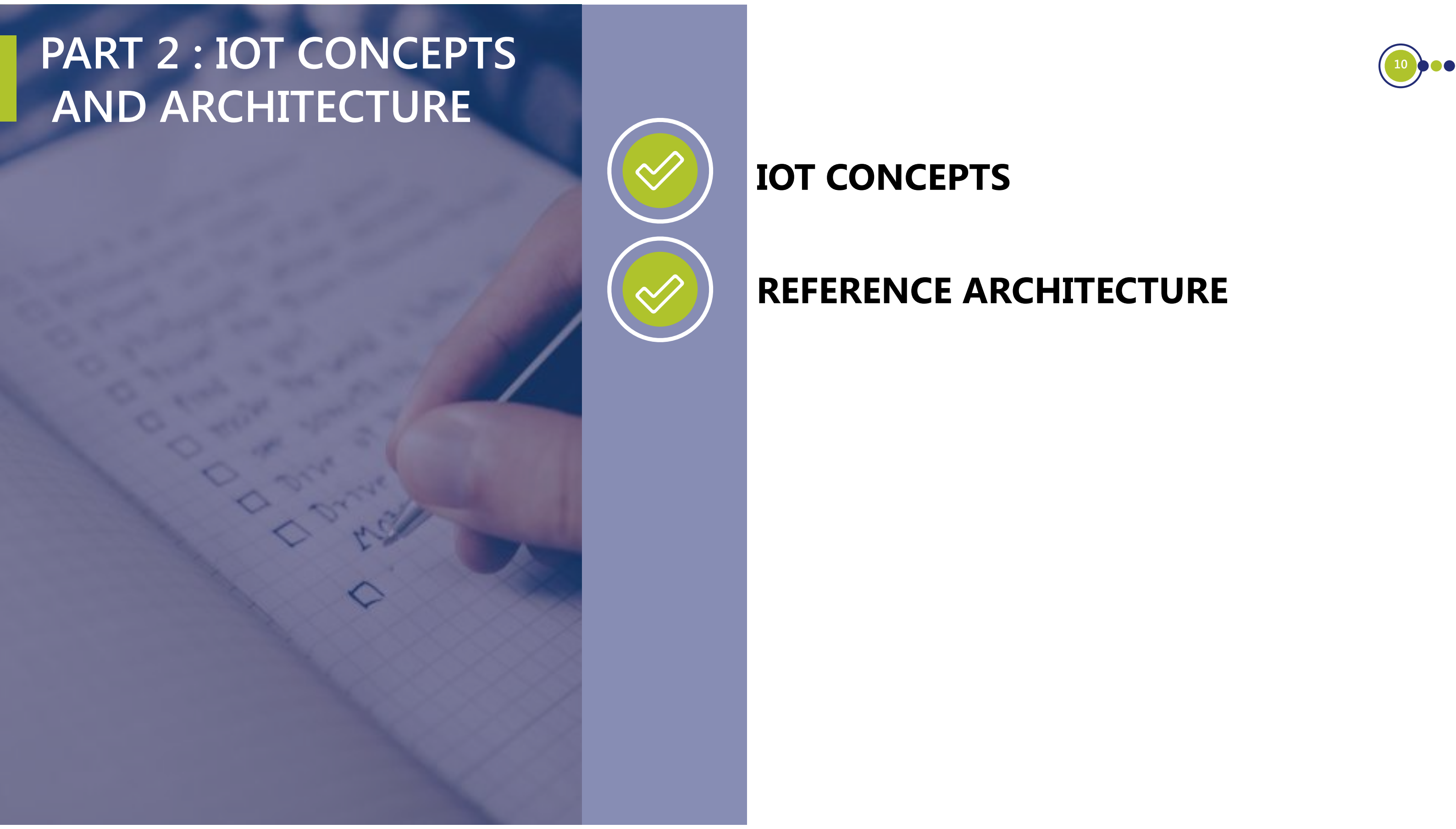
Properties LTL/MTL

SMC

Verdict

Quantitative analysis
What is the probability that the system $\mathcal{M}$ satisfies the property $\boldsymbol{\varphi}$?

Qualitative analysis
Is the probability that the system $\mathcal{M}$ satisfies the property $\boldsymbol{\varphi}$ greater or equal than a threashold $\boldsymbol{\theta}$?

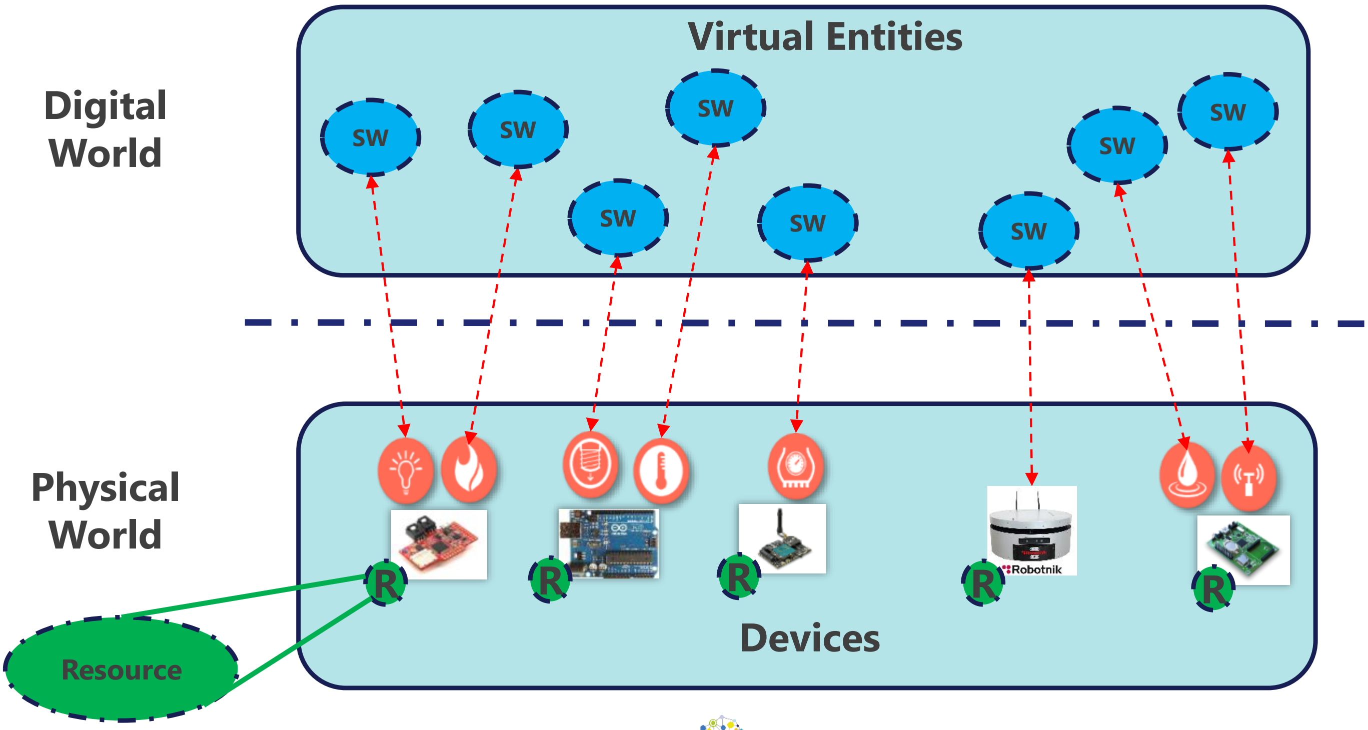


PART 2 : IOT CONCEPTS AND ARCHITECTURE

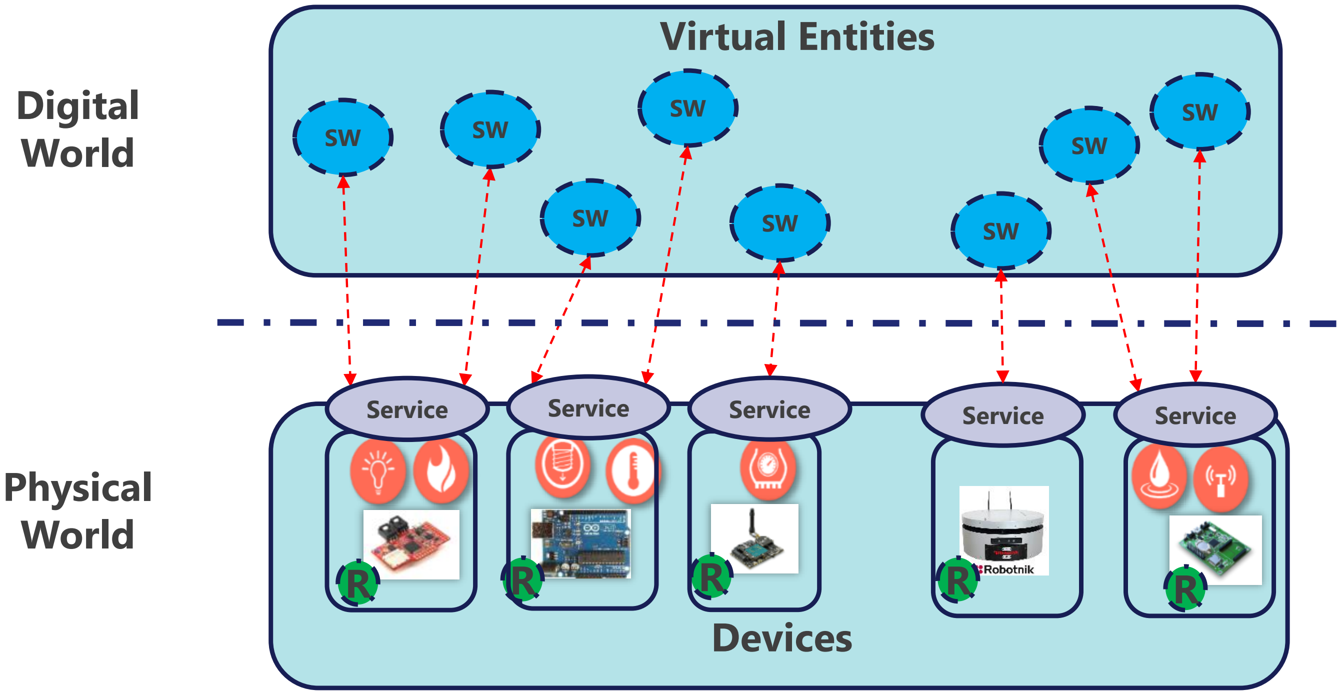
✓ IOT CONCEPTS

✓ REFERENCE ARCHITECTURE

IOT CONCEPTS

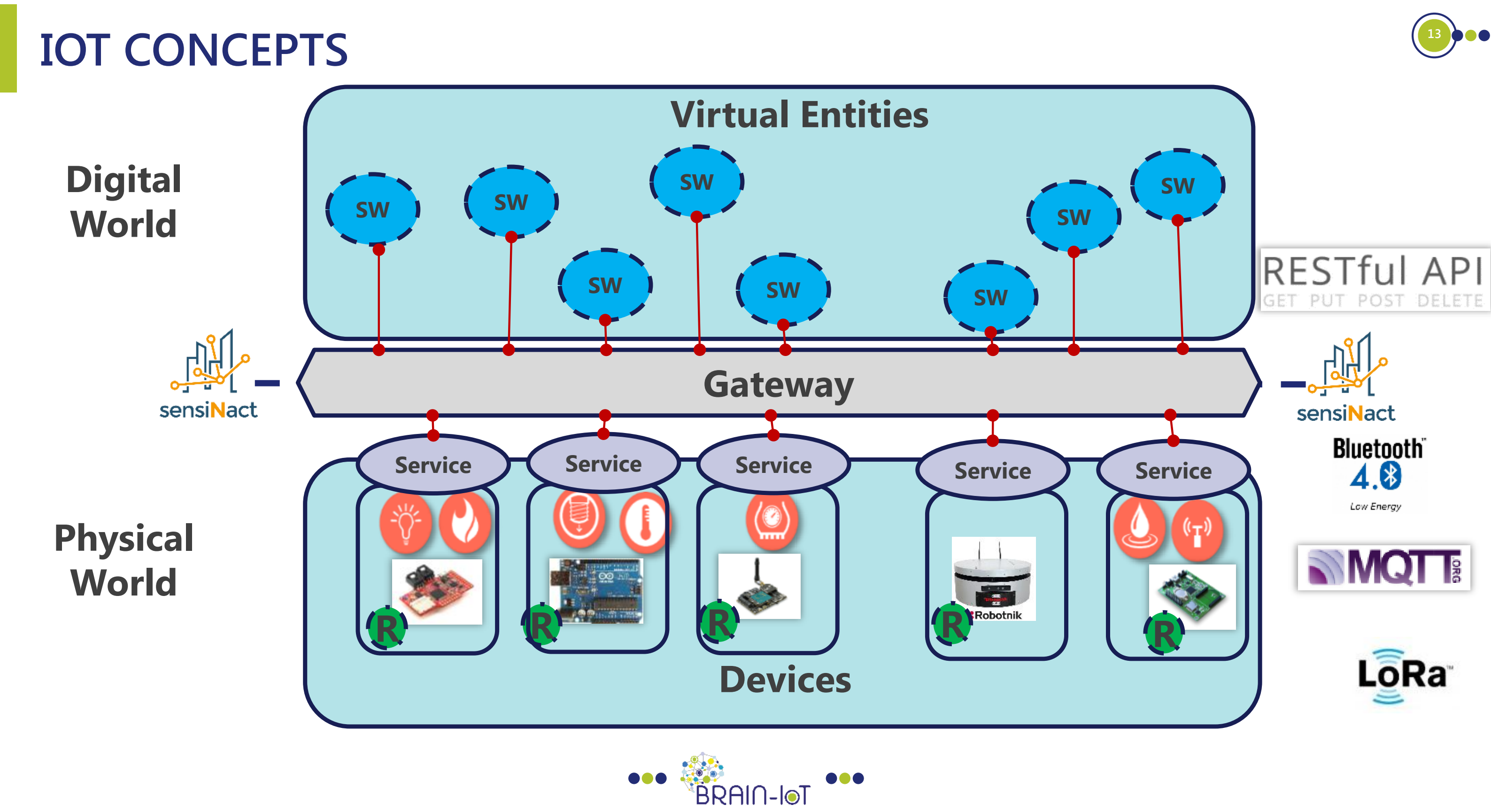


IOT CONCEPTS



BRAIN-IoT

©MECO.net



IOT CONCEPTS

13

Digital World

Virtual Entities

SW SW SW SW SW SW SW SW

RESTful API
GET PUT POST DELETE

sensiNact

Gateway

sensiNact

Service Service Service Service Service

Bluetooth 4.0 Low Energy

MQTT.ORG

LoRa

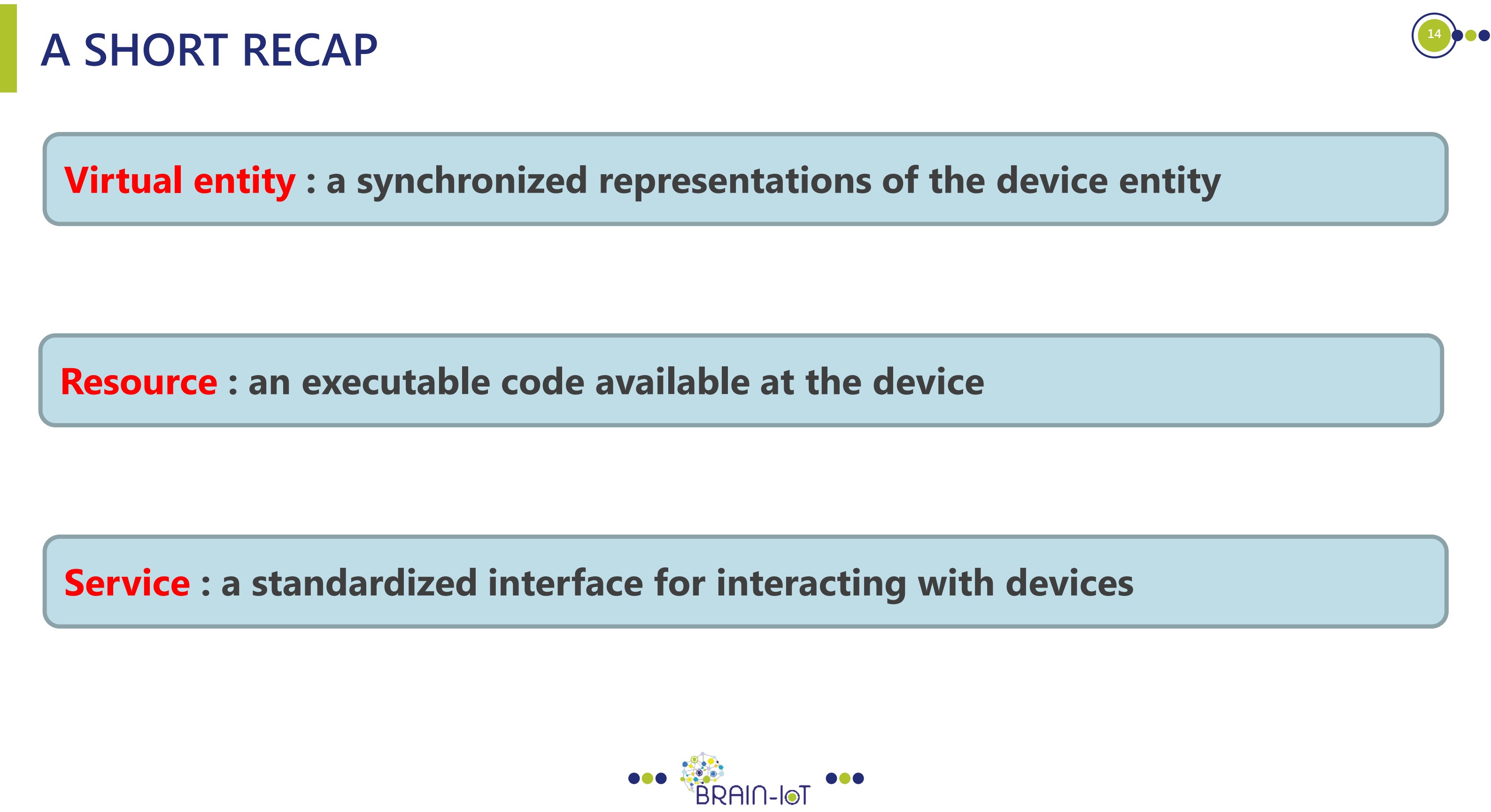
R R R R R

Robotnik

Physical World

Devices

BRAIN-IoT



A SHORT RECAP

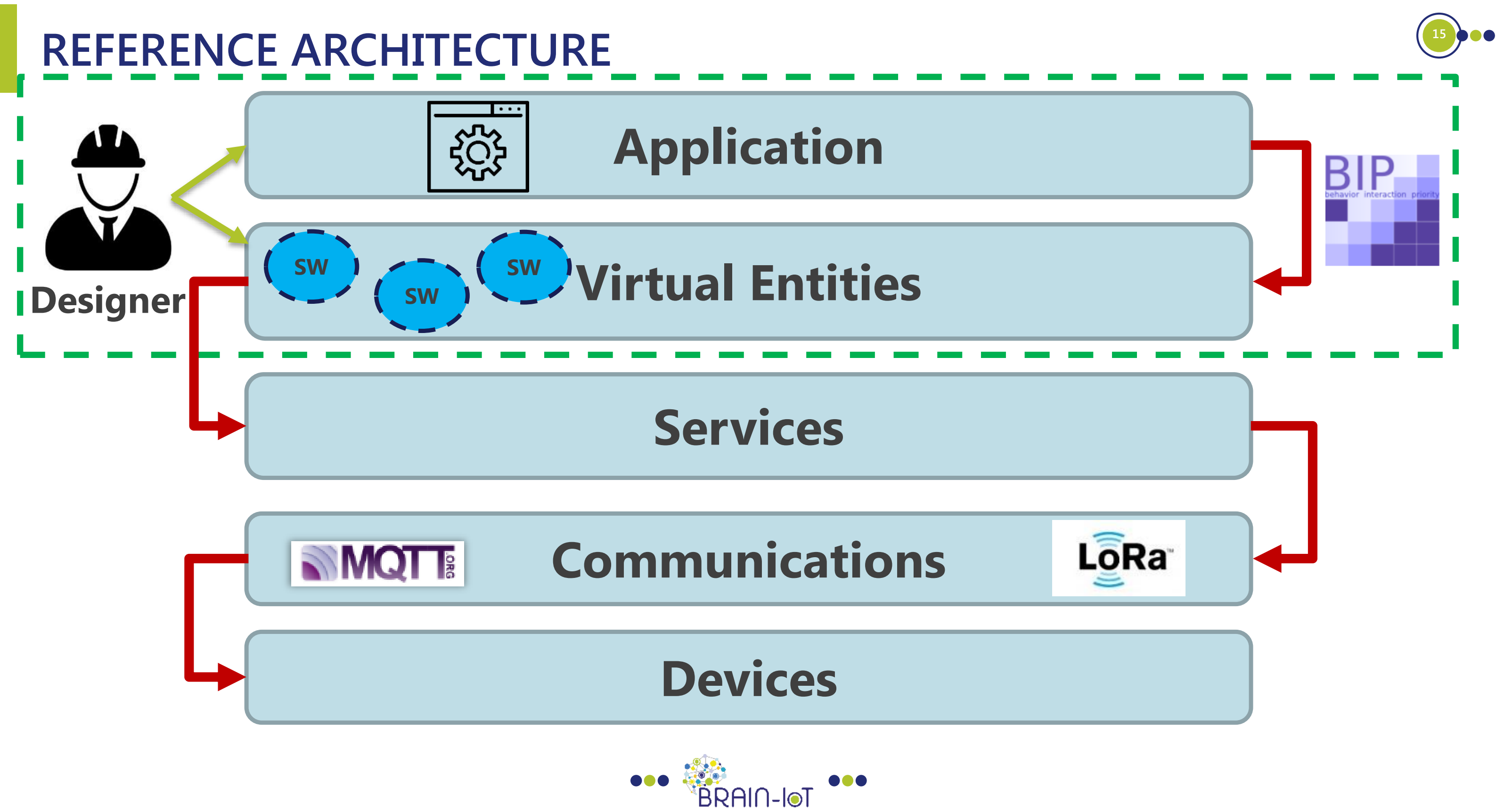
14

Virtual entity : a synchronized representations of the device entity

Resource : an executable code available at the device

Service : a standardized interface for interacting with devices

BRAIN-IoT



REFERENCE ARCHITECTURE

Designer

Application

Virtual Entities

SW

SW

SW

Services

Communications

Devices

A SHORT RECAP

16

Application : user defined software that interacts with virtual entities

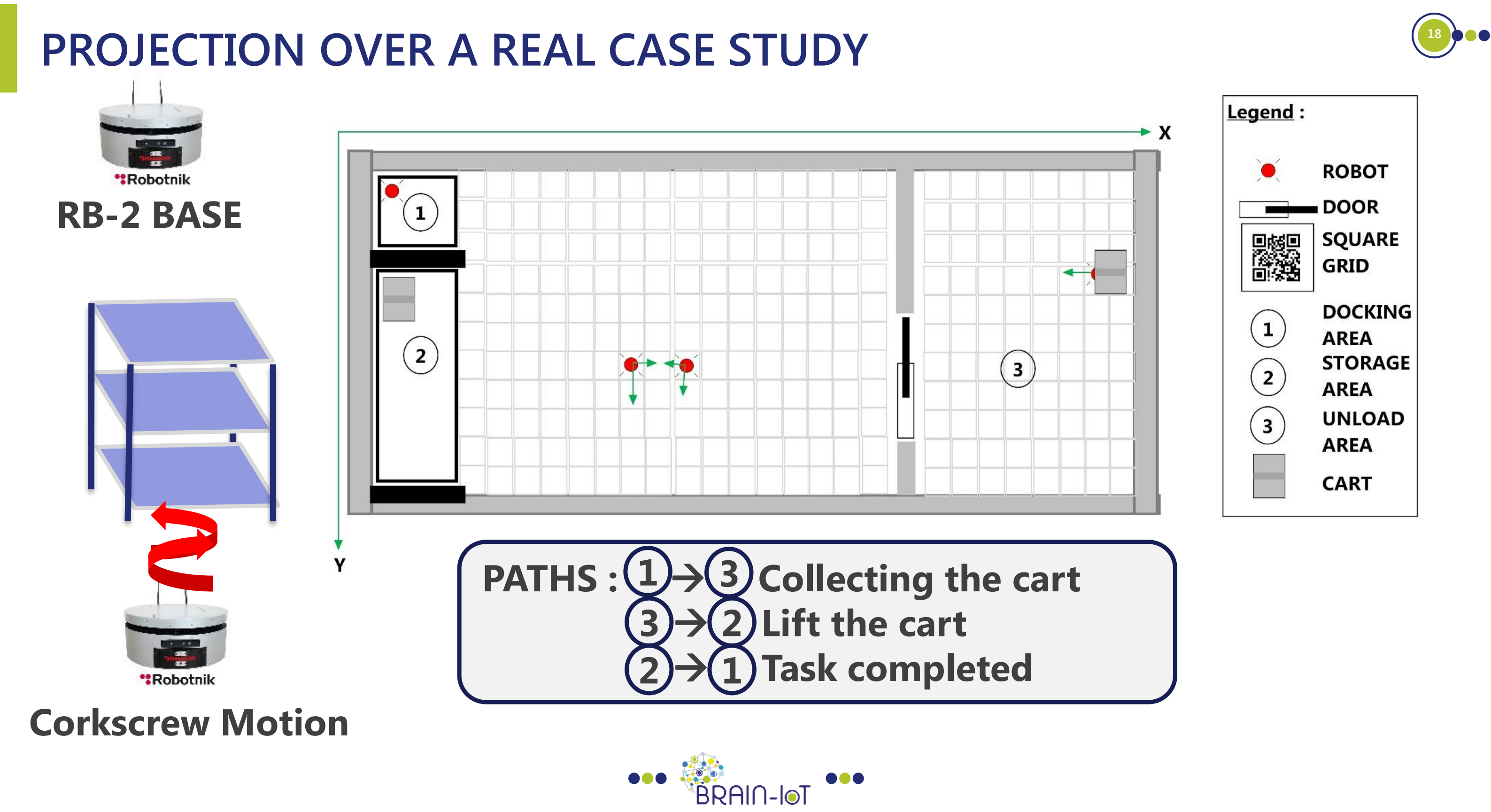
Communications : A set of protocols to interact with physical entities

Devices : a set of sensors and actuators composing the physical entities

BRAIN-IoT

PART 3 : PROJECTION OVER A REAL CASE STUDY

- ✓ **REQUIREMENTS**
- ✓ **CHECKING PROCESS**
- ✓ **BIP MODEL**
- ✓ **VERIFICATION AND SIMULATION**



PROJECTION OVER A REAL CASE STUDY

18

RB-2 BASE

Corkscrew Motion

Legend :

● ROBOT

DOOR

SQUARE GRID

1 DOCKING AREA

2 STORAGE AREA

3 UNLOAD AREA

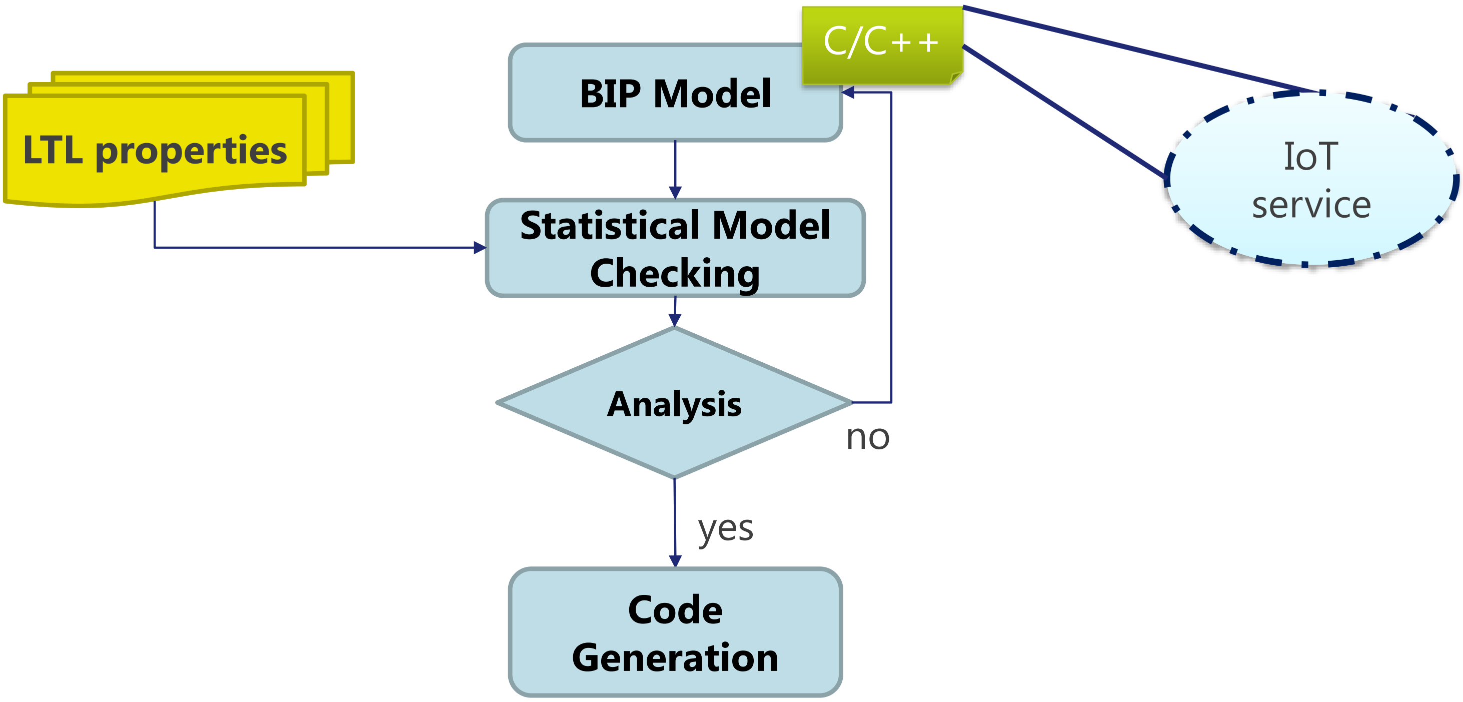
CART

PATHS : 1 → 3 Collecting the cart
3 → 2 Lift the cart
2 → 1 Task completed

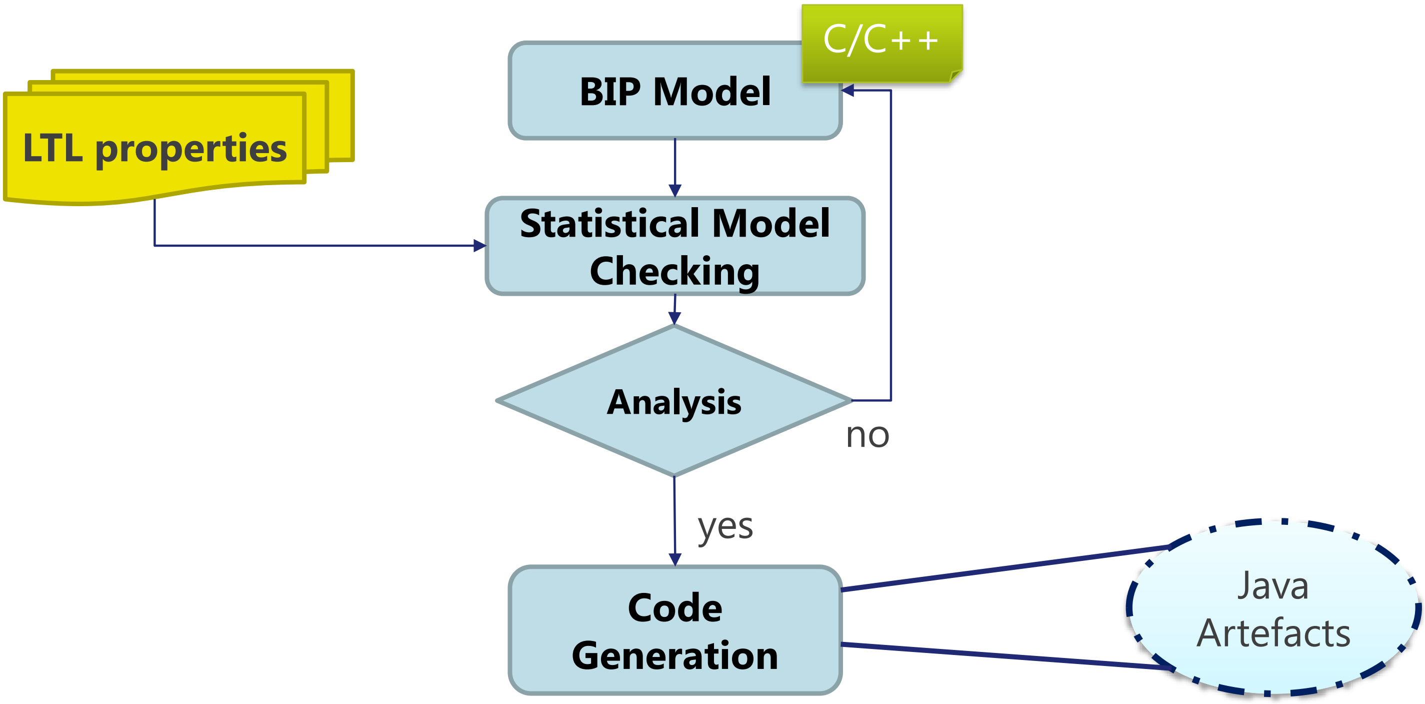
REQUIREMENTS : AN EXAMPLE

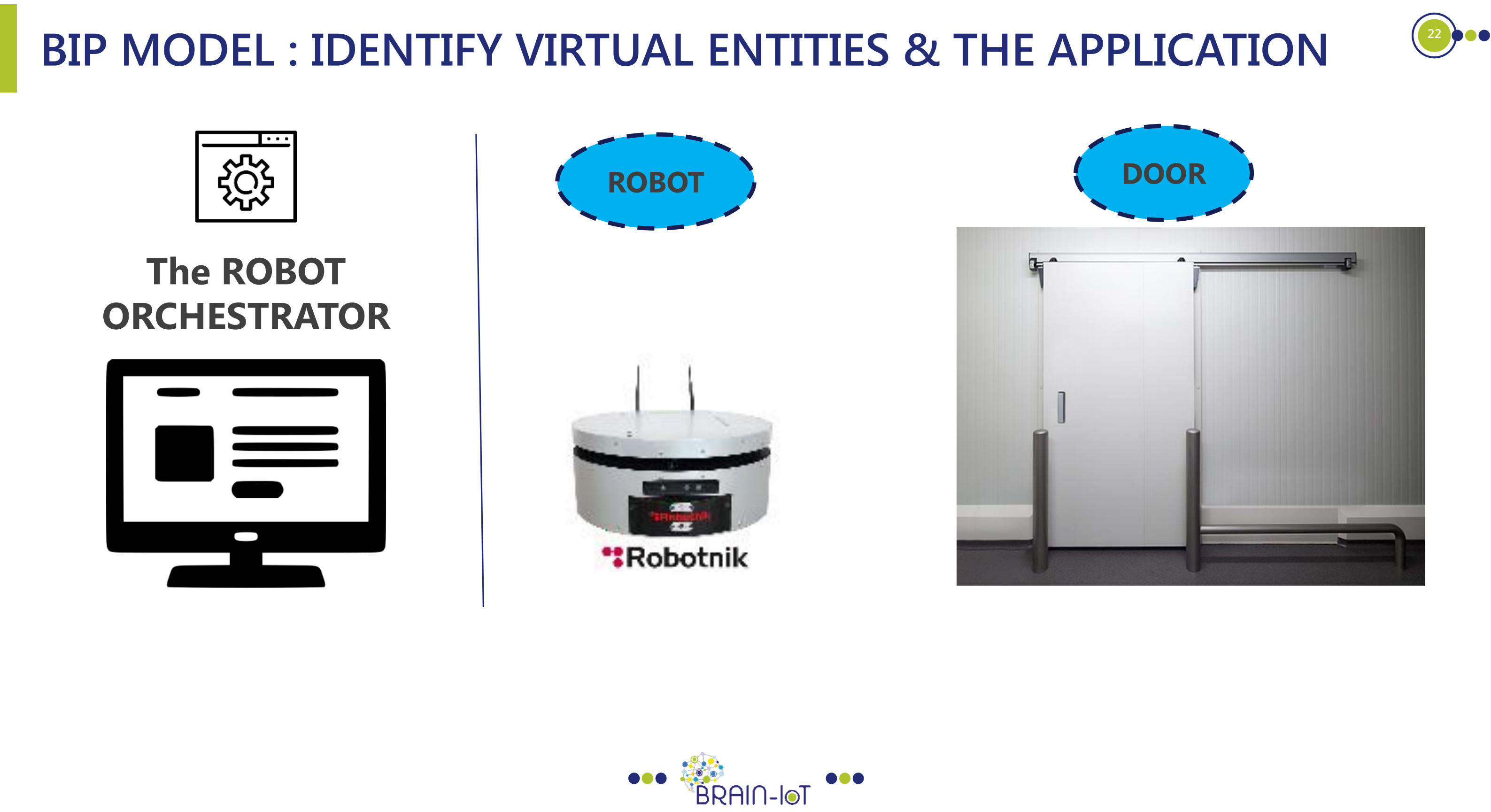
REQ : If a cart is detected with densely filled shelves, then, the robot does a corkscrew motion to lift the cart off the ground and transport the entire unit to the storage area.

HOW TO CHECK IT: NEED A PROCESS



HOW TO CHECK IT: NEED A PROCESS





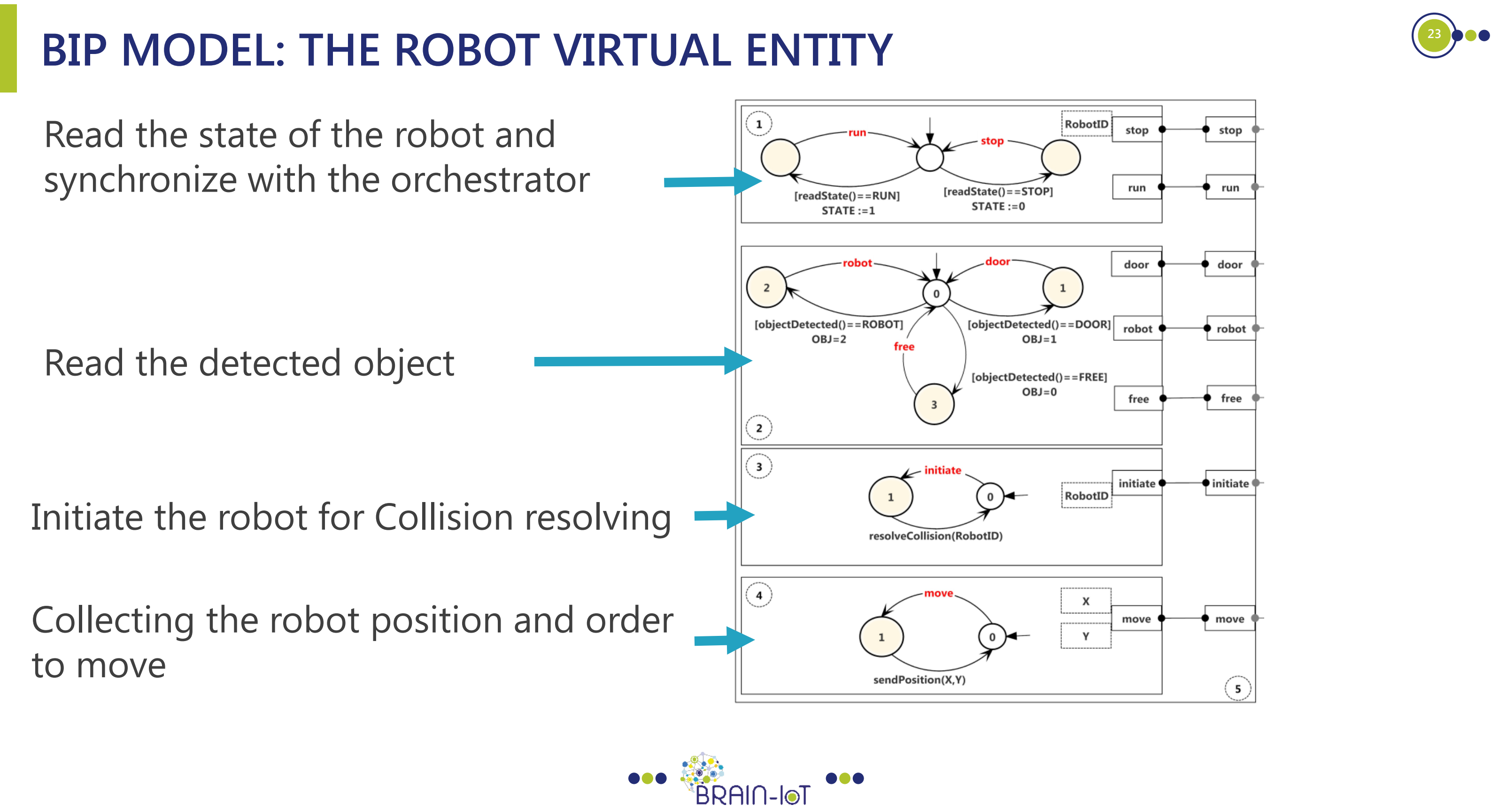
BIP MODEL : IDENTIFY VIRTUAL ENTITIES & THE APPLICATION

22

The ROBOT ORCHESTRATOR

ROBOT

DOOR



BIP MODEL: THE ROBOT VIRTUAL ENTITY

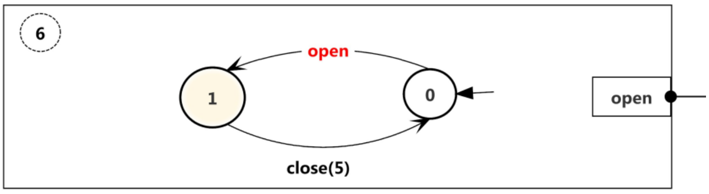
Read the state of the robot and synchronize with the orchestrator

Read the detected object

Initiate the robot for Collision resolving

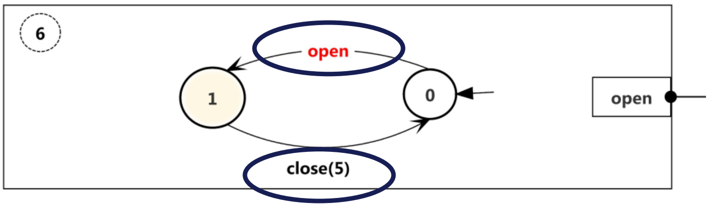
Collecting the robot position and order to move

BIP MODEL: THE DOOR VIRTUAL ENTITY



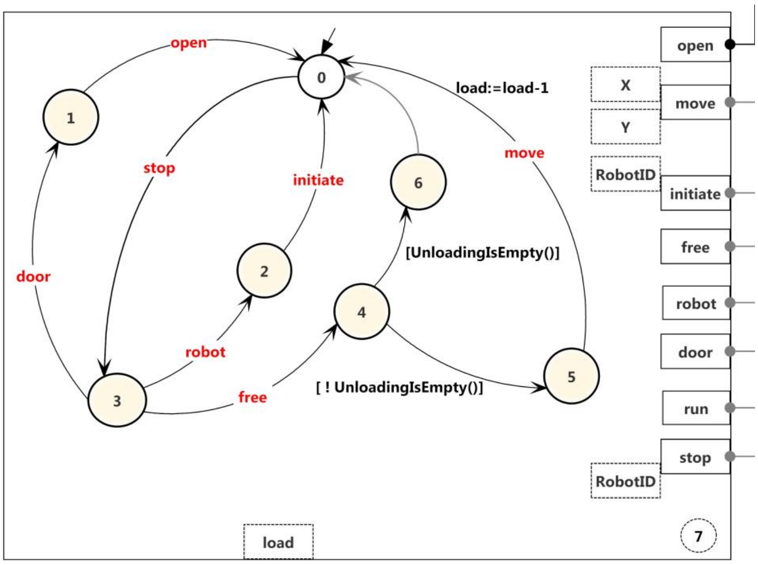
BIP MODEL: THE DOOR VIRTUAL ENTITY

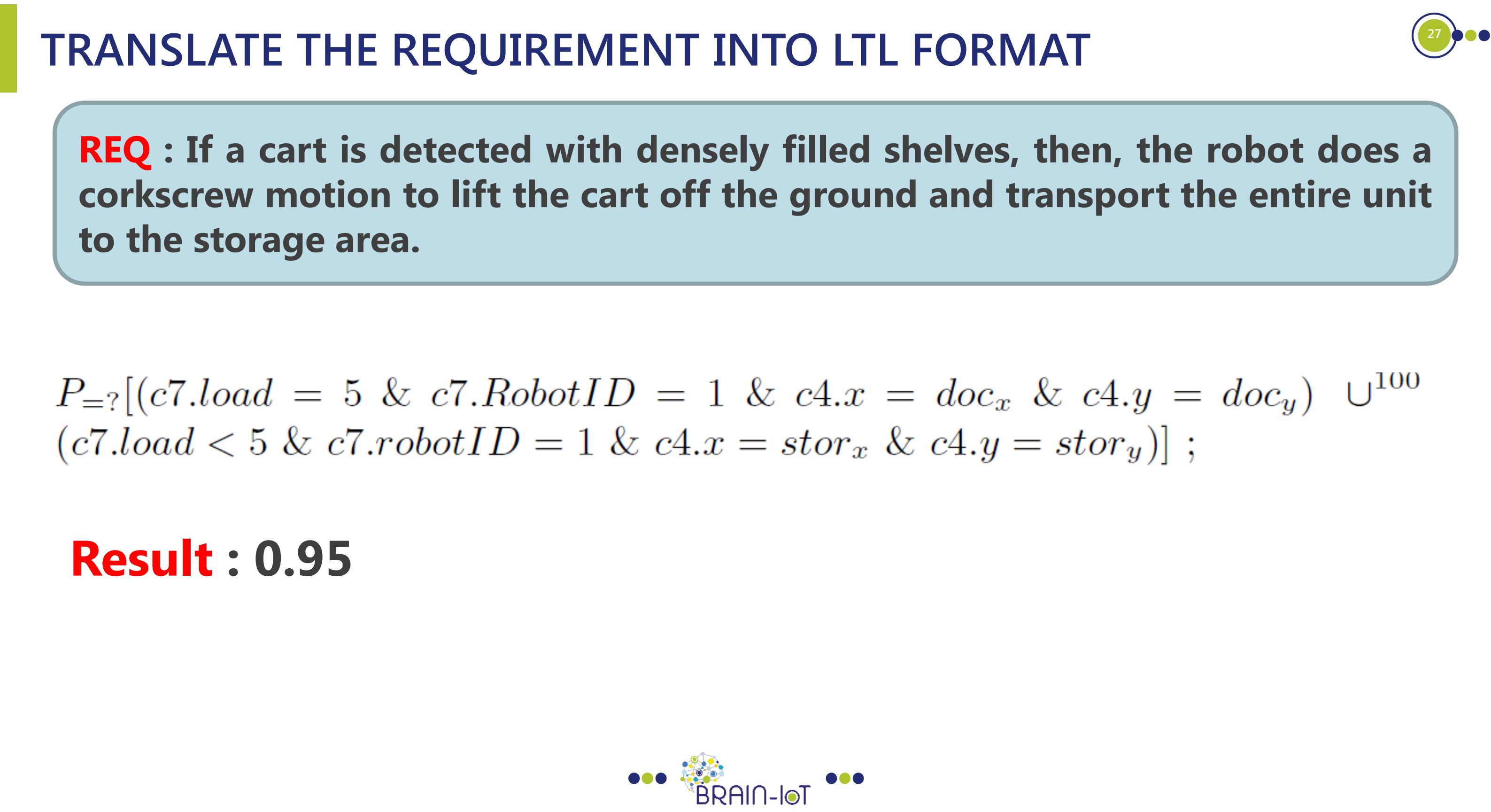
Order to open the door



Closing the door after 5 seconds

BIP MODEL: THE ORCHESTRATOR





TRANSLATE THE REQUIREMENT INTO LTL FORMAT

27

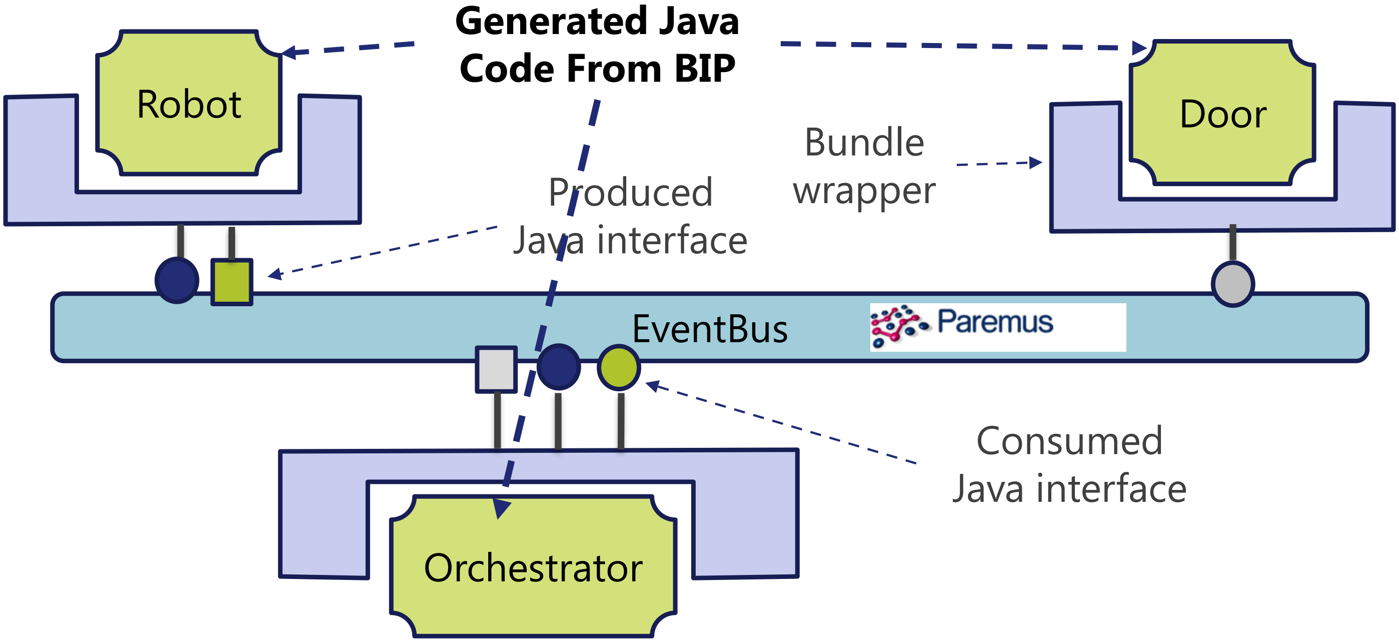
REQ : If a cart is detected with densely filled shelves, then, the robot does a corkscrew motion to lift the cart off the ground and transport the entire unit to the storage area.

$$P_{=?}[(c7.load = 5 \ \& \ c7.RobotID = 1 \ \& \ c4.x = doc_x \ \& \ c4.y = doc_y) \ \cup^{100} (c7.load < 5 \ \& \ c7.robotID = 1 \ \& \ c4.x = stor_x \ \& \ c4.y = stor_y)] \ ;$$

Result : 0.95

BRAIN-IoT

SERVICE ROBOTIC (ROB) USING BUNDLES AND EVENT BUS

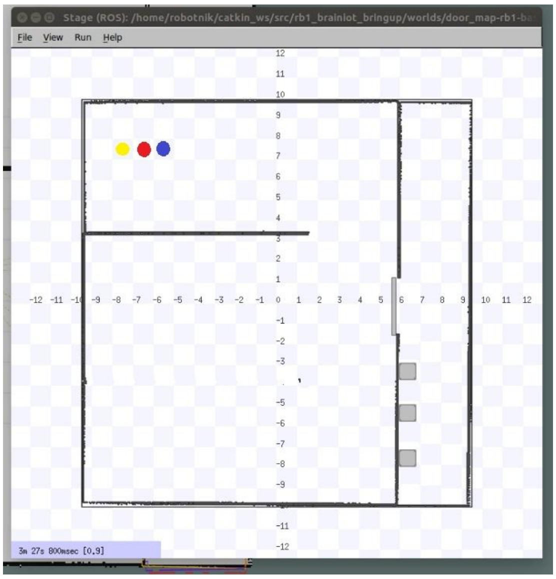


SIMULATION

Ubuntu-16.04 desktop Intel core i7-950@3.07 GHz and ROS Kinetic with STAGE and rviz GUI

We use rviz to plan the intelligent robot's movement within a 3D movement area and STAGE to capture a robot's movement into 2D plan.

SIMULATION (SNAPSHOT 1)

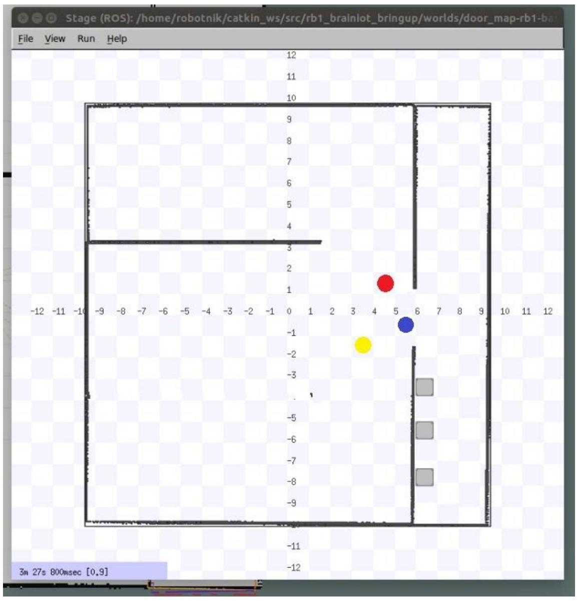


Stage (ROS): /home/robotnik/catkin_ws/src/rb1_brainiot_bringup/worlds/door_map-rb1-ba

3m 27s 800msec [0.9]

BRAIN-IoT

SIMULATION (SNAPSHOT 2)

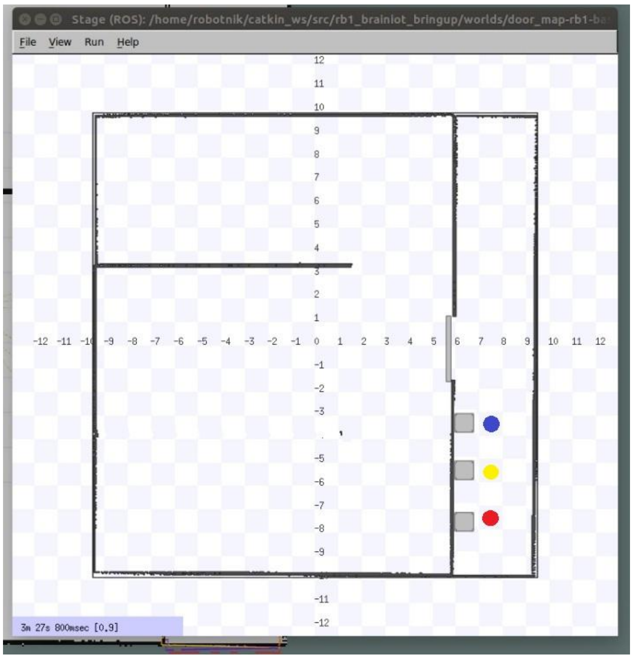


Stage (ROS): /home/robotnik/catkin_ws/src/rb1_brainiot_bringup/worlds/door_map-rb1-ba

```
3m 27s 800msec [0.9]
```

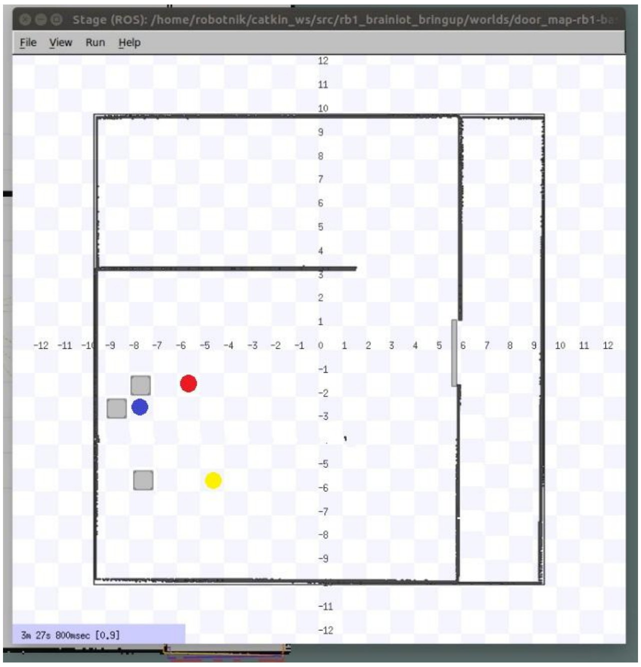
BRAIN-IoT

SIMULATION (SNAPSHOT 3)


Stage (ROS): /home/robotnik/catkin_ws/src/rb1_brainiot_bringup/worlds/door_map-rb1-ba

```
3m 27s 800msec [0.9]
```

SIMULATION (SNAPSHOT 4)



Stage (ROS): /home/robotnik/catkin_ws/src/rb1_brainiot_bringup/worlds/door_map-rb1-ba

3m 27s 800msec [0.9]

BRAIN-IoT

CONTACTS

BAOUYA ABDELHAKIM

RESEARCHER

UNIVERSITY GRENOBLE ALPES

Abdelhakim.baouya@univ-grenoble-alpes.fr

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780089.

BRAIN-IoT

model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems

CONTACTS

CHEHIDA SALIM

RESEARCHER

UNIVERSITY GRENOBLE ALPES

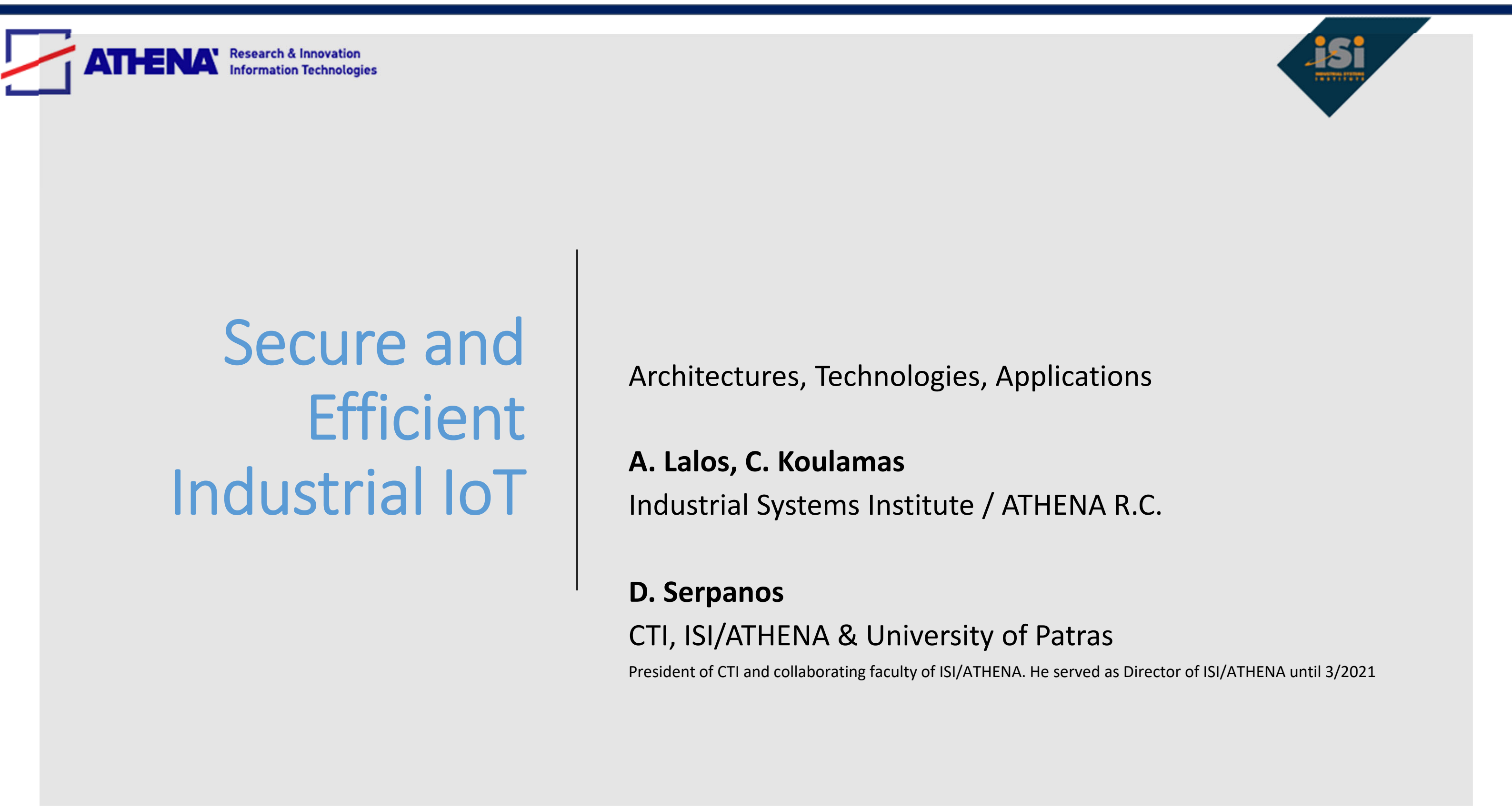
Salim.Chehida@univ-grenoble-alpes.fr

thank you
LINKS
cea
UNIVERSITÉ Grenoble Alpes
Paremus
improving metrics
life.augmented
SIEMENS
ECLIPSE FOUNDATION
IDATE DIGIWORLD
AIRBUS
Robotnik
emalcsa

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 780089.

BRAIN-IoT

model-Based fRamework for dependable sensing and Actuation in INtelligent decentralized IoT systems



Secure and Efficient Industrial IoT

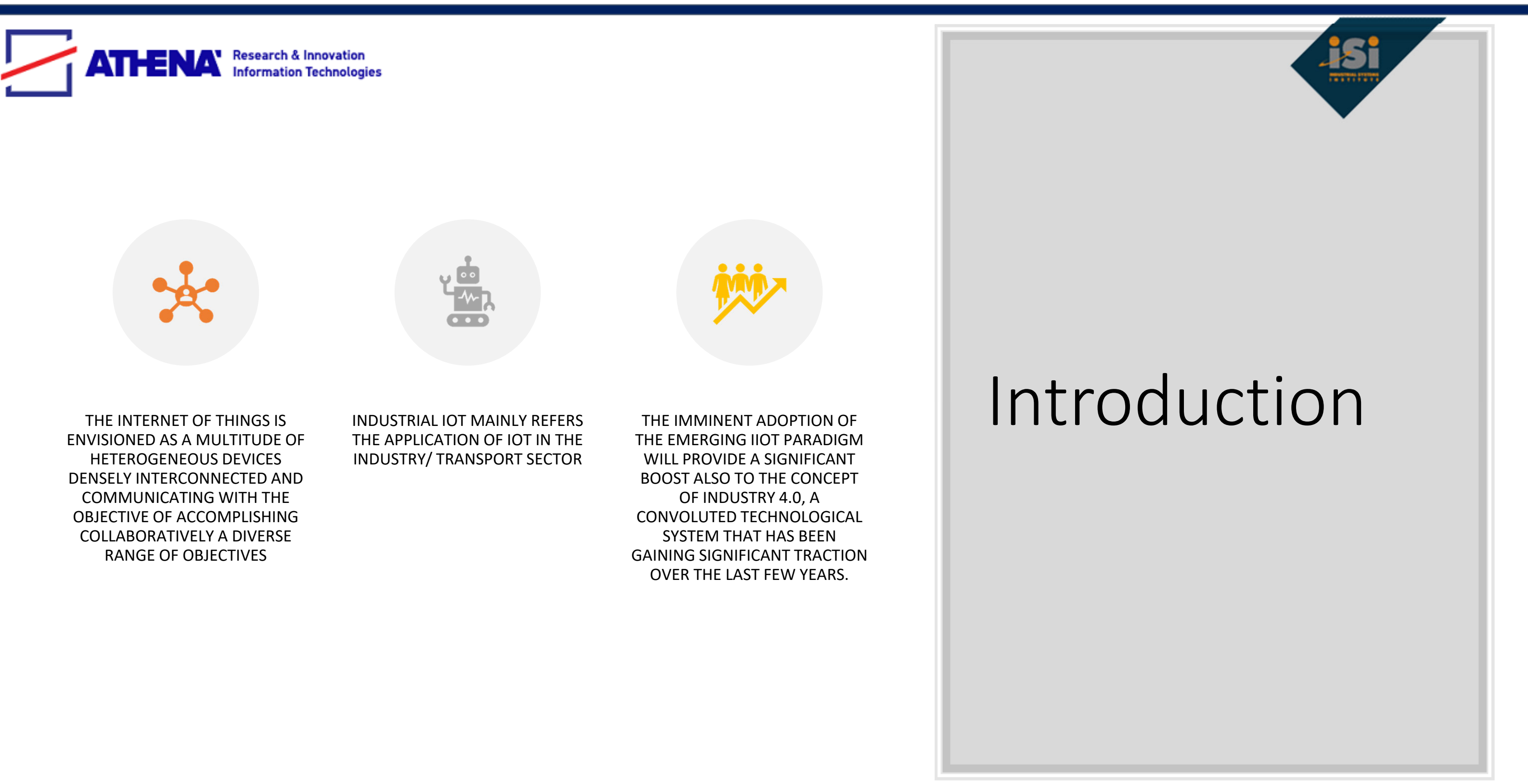
Architectures, Technologies, Applications

A. Lalos, C. Koulamas
Industrial Systems Institute / ATHENA R.C.

D. Serpanos
CTI, ISI/ATHENA & University of Patras
President of CTI and collaborating faculty of ISI/ATHENA. He served as Director of ISI/ATHENA until 3/2021

Outline

- Introduction
- IIoT Layered Architecture Review
- Proposed General architecture
- Building blocks
- **Artificial Intelligence solutions that** support in order **to strengthen reliability, fault tolerance and security at system level**
- Applications in the automotive and manufacturing domains



Introduction

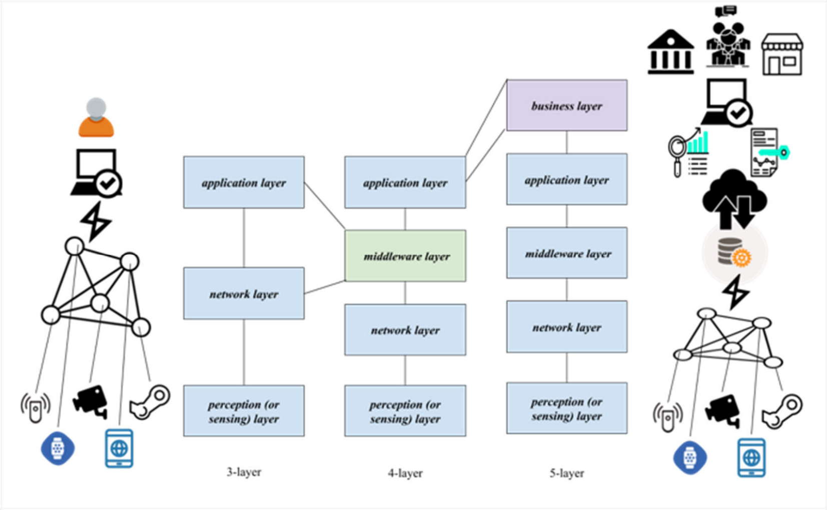
THE INTERNET OF THINGS IS ENVISIONED AS A MULTITUDE OF HETEROGENEOUS DEVICES DENSELY INTERCONNECTED AND COMMUNICATING WITH THE OBJECTIVE OF ACCOMPLISHING COLLABORATIVELY A DIVERSE RANGE OF OBJECTIVES

INDUSTRIAL IOT MAINLY REFERS THE APPLICATION OF IOT IN THE INDUSTRY/ TRANSPORT SECTOR

THE IMMINENT ADOPTION OF THE EMERGING IIOT PARADIGM WILL PROVIDE A SIGNIFICANT BOOST ALSO TO THE CONCEPT OF INDUSTRY 4.0, A CONVOLUTED TECHNOLOGICAL SYSTEM THAT HAS BEEN GAINING SIGNIFICANT TRACTION OVER THE LAST FEW YEARS.

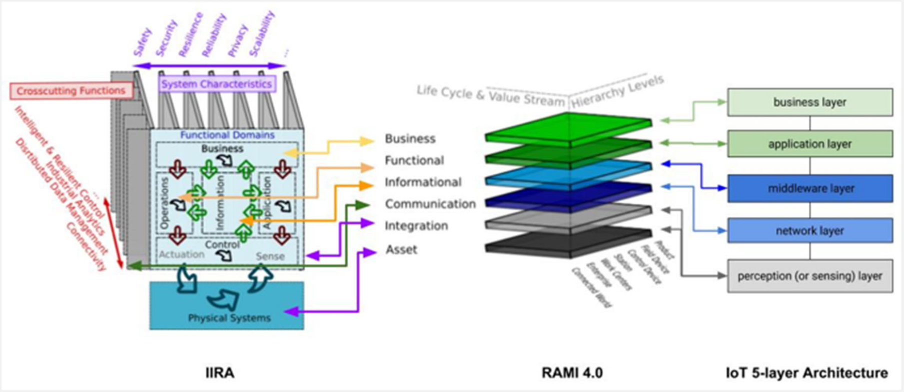
ATHENA Research & Innovation Information Technologies

IIoT layered Architecture Review



- ➢ The perception (or sensing) layer being the physical layer, consisting of smart objects/devices such as sensors and actuators that are able for sensing and gathering information about the environment as well as interacting with it and its elements.
- ➢ The network layer realizing the connection and communication of the smart objects, network devices, and servers. Furthermore, the network layer is responsible for the transmission and processing of sensor data.
- ➢ The application layer consisting of applications that deliver IoT-based services to the end users, including smart homes, smart energy, smart health and smart cities.

IIRA, RAMI 4.0 and IoT five layered architecture



- Contrary to the RAMI 4.0, which is specialized in the manufacturing business processes, IIRA deals with a wider range of IIoT applications, from transportation to energy.
- IIRA also follows a three dimensional model, but with a different approach to RAMI 4.0.

RAMI 4.0 is based on a three-dimensional model covering all the industrial aspects from the industrial hierarchy to the product life cycle. Its three dimensions are:

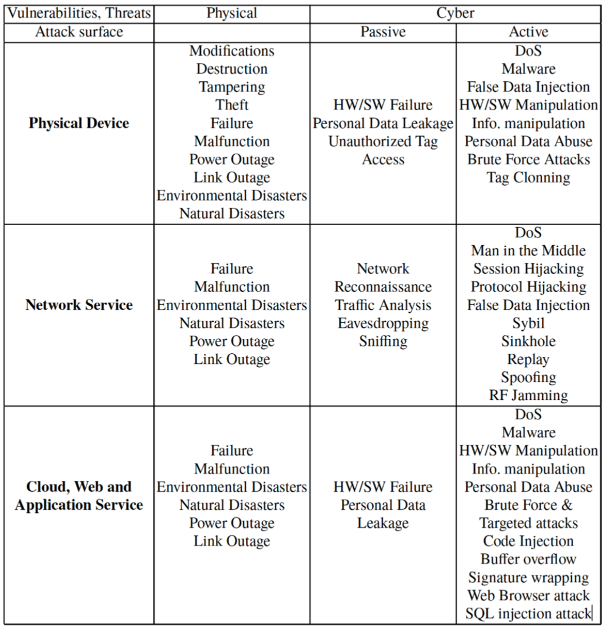
a) the Hierarchy defining the functional areas of the IIoT applications selecting from Smart Product, Smart Factory and Connected World;

b) Architecture, which provides the system architecture, and finally

c) the Product Life Cycle, which cover development, production, and maintenance aspects.

ATHENA Research & Innovation Information Technologies

Vulnerabilities and Threats in IIoT systems



Vulnerabilities, Threats	Physical	Cyber	
Attack surface		Passive	Active
Physical Device	Modifications Destruction Tampering Theft Failure Malfunction Power Outage Link Outage Environmental Disasters Natural Disasters	HW/SW Failure Personal Data Leakage Unauthorized Tag Access	DoS Malware False Data Injection HW/SW Manipulation Info. manipulation Personal Data Abuse Brute Force Attacks Tag Clonning
Network Service	Failure Malfunction Environmental Disasters Natural Disasters Power Outage Link Outage	Network Reconnaissance Traffic Analysis Eavesdropping Sniffing	DoS Man in the Middle Session Hijacking Protocol Hijacking False Data Injection Sybil Sinkhole Replay Spoofing RF Jamming
Cloud, Web and Application Service	Failure Malfunction Environmental Disasters Natural Disasters Power Outage Link Outage	HW/SW Failure Personal Data Leakage	DoS Malware HW/SW Manipulation Info. manipulation Personal Data Abuse Brute Force & Targeted attacks Code Injection Buffer overflow Signature wrapping Web Browser attack SQL injection attack

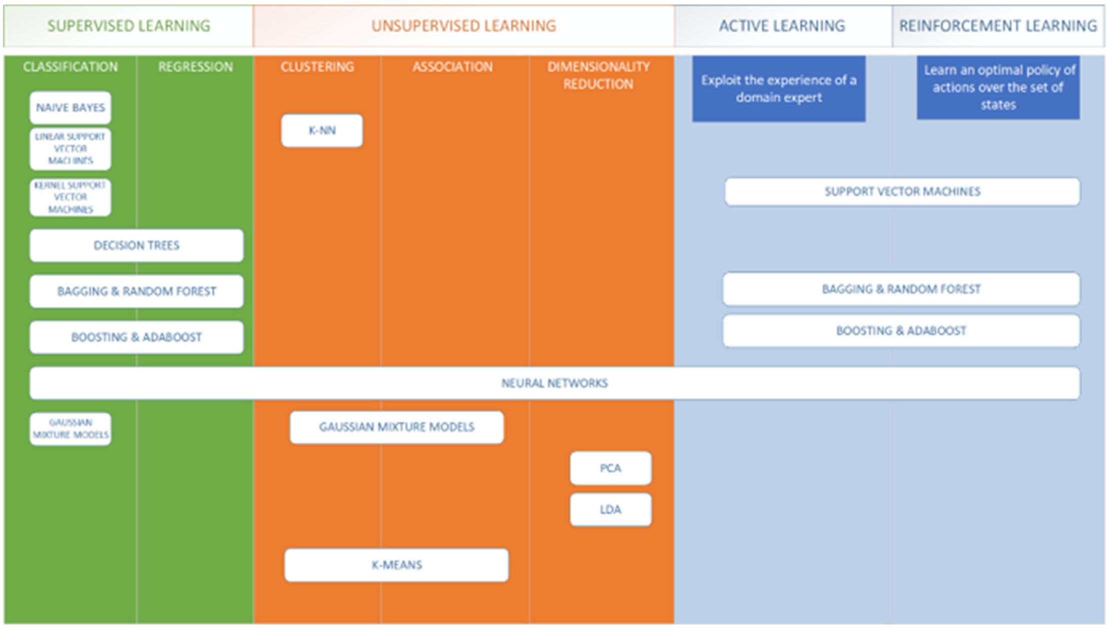
- There are already various existing studies and proposals in the literature to identify the peculiarities of IoT security threats (Humayed et al., 2017; Mena et al., 2018; Chen et al., 2018).

- According to (ENISA Report, 2017, 2018a,b,c) there are 8-9 high-level threat groups, and a large number of identified threats, depending on the case

- On a different perspective, the OWASP-IoT approach starts from the definition of the set of areas of the attack surface, for which then the various vulnerabilities are enumerated.

- Attempting to organize the broad set of threats and areas of the attack surface under the structural view presented in the previous slides is shown in the table

Machine learning methods for IIoT security



SUPERVISED LEARNING

CLASSIFICATION

REGRESSION

NAIVE BAYES

LINEAR SUPPORT VECTOR MACHINES

KERNEL SUPPORT VECTOR MACHINES

DECISION TREES

BAGGING & RANDOM FOREST

BOOSTING & ADABOOST

GAUSSIAN MIXTURE MODELS

UNSUPERVISED LEARNING

CLUSTERING

ASSOCIATION

DIMENSIONALITY REDUCTION

K-NN

GAUSSIAN MIXTURE MODELS

PCA

LDA

K-MEANS

ACTIVE LEARNING

Exploit the experience of a domain expert

REINFORCEMENT LEARNING

Learn an optimal policy of actions over the set of states

SUPPORT VECTOR MACHINES

BAGGING & RANDOM FOREST

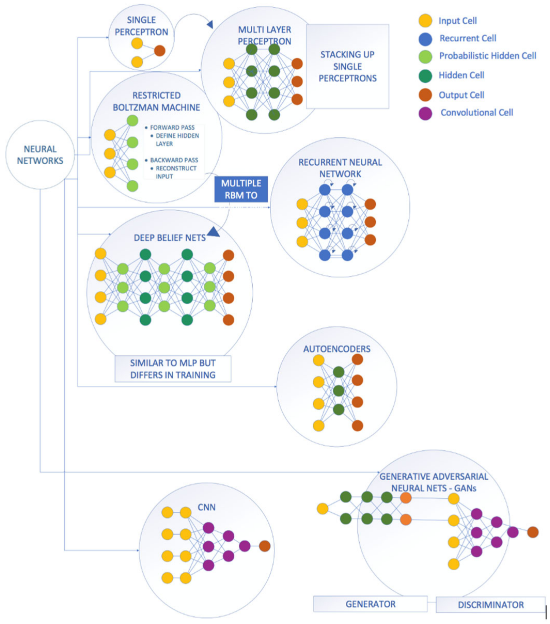
BOOSTING & ADABOOST

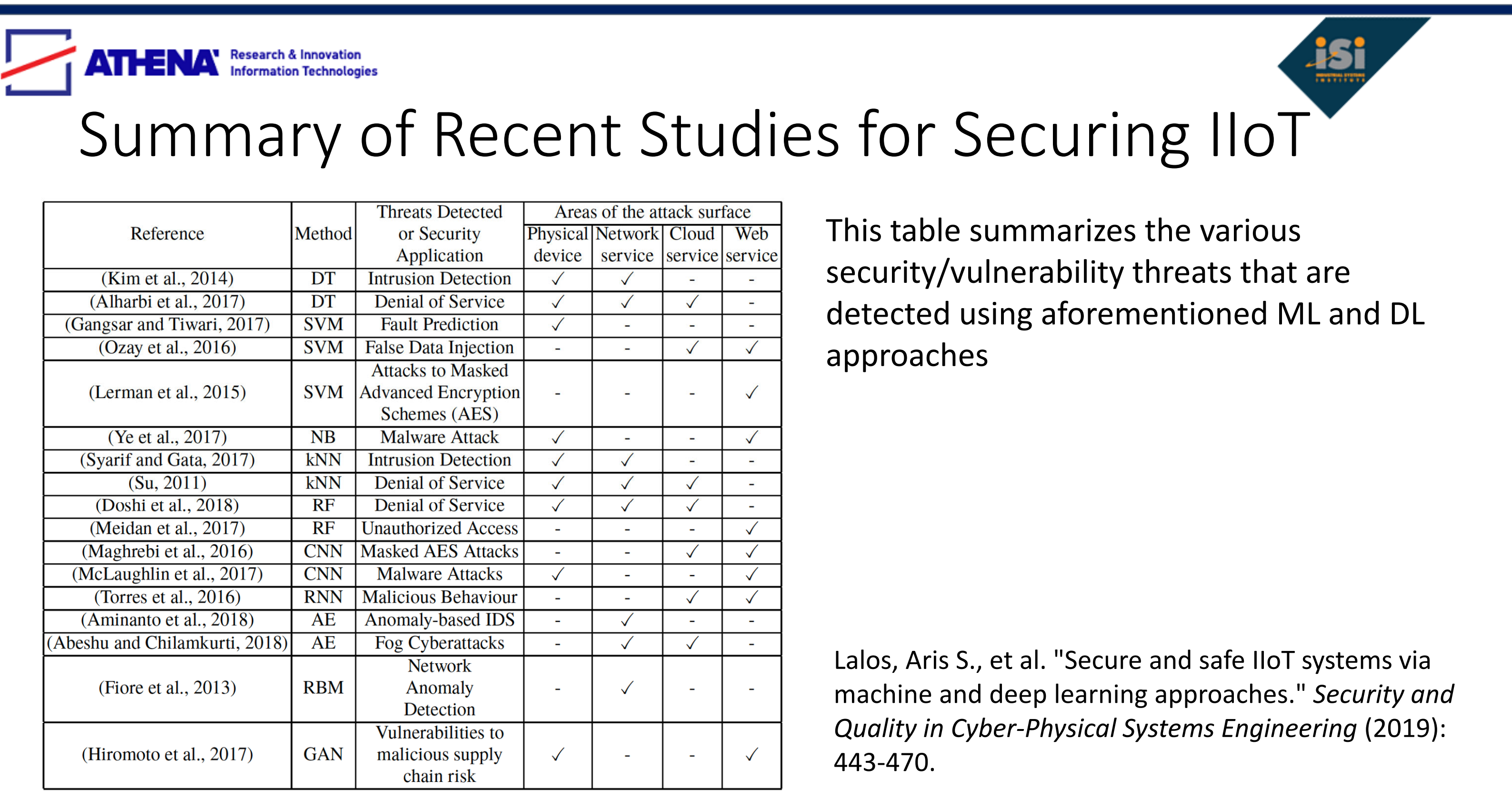
NEURAL NETWORKS

Deep Learning Methods for IIoT Security

- Most modern deep learning methods are based on Neural Networks (NNs) (please refer the to Figure)

- Learning can be supervised, alternatively known as discriminative (e.g. Convolutional and recurrent NN), unsupervised (generative learning, e.g. generative adversarial networks) or semi-supervised (e.g. auto-encoders, deep belief networks, restricted Boltzmann machines).





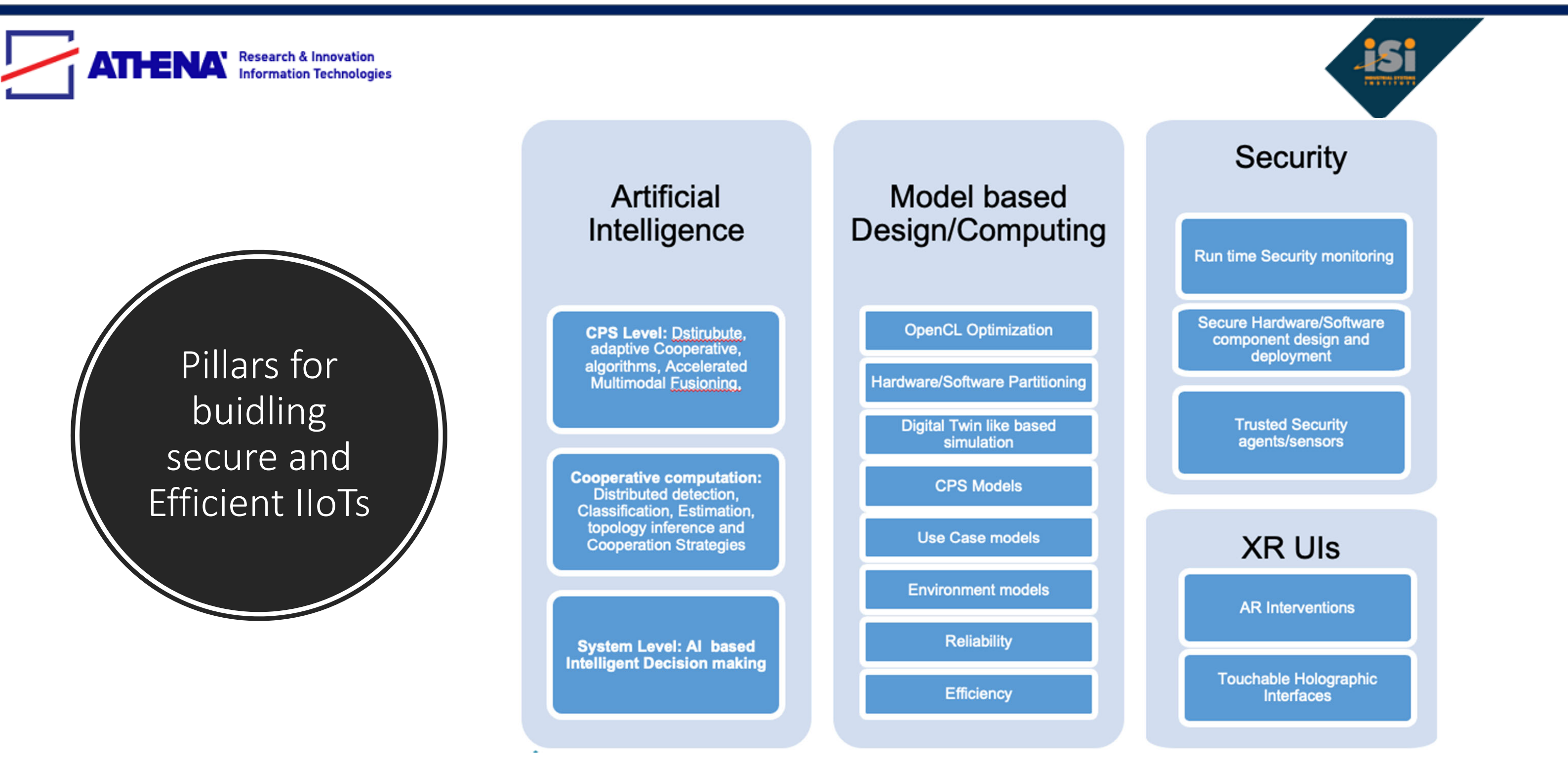
ATHENA Research & Innovation Information Technologies
isi

Summary of Recent Studies for Securing IIoT

Reference	Method	Threats Detected or Security Application	Areas of the attack surface			
			Physical device	Network service	Cloud service	Web service
(Kim et al., 2014)	DT	Intrusion Detection	✓	✓	-	-
(Alharbi et al., 2017)	DT	Denial of Service	✓	✓	✓	-
(Gangsar and Tiwari, 2017)	SVM	Fault Prediction	✓	-	-	-
(Ozay et al., 2016)	SVM	False Data Injection	-	-	✓	✓
(Lerman et al., 2015)	SVM	Attacks to Masked Advanced Encryption Schemes (AES)	-	-	-	✓
(Ye et al., 2017)	NB	Malware Attack	✓	-	-	✓
(Syarif and Gata, 2017)	kNN	Intrusion Detection	✓	✓	-	-
(Su, 2011)	kNN	Denial of Service	✓	✓	✓	-
(Doshi et al., 2018)	RF	Denial of Service	✓	✓	✓	-
(Meidan et al., 2017)	RF	Unauthorized Access	-	-	-	✓
(Maghrebi et al., 2016)	CNN	Masked AES Attacks	-	-	✓	✓
(McLaughlin et al., 2017)	CNN	Malware Attacks	✓	-	-	✓
(Torres et al., 2016)	RNN	Malicious Behaviour	-	-	✓	✓
(Aminanto et al., 2018)	AE	Anomaly-based IDS	-	✓	-	-
(Abeshu and Chilamkurti, 2018)	AE	Fog Cyberattacks	-	✓	✓	-
(Fiore et al., 2013)	RBM	Network Anomaly Detection	-	✓	-	-
(Hiromoto et al., 2017)	GAN	Vulnerabilities to malicious supply chain risk	✓	-	-	✓

This table summarizes the various security/vulnerability threats that are detected using aforementioned ML and DL approaches

Lalos, Aris S., et al. "Secure and safe IIoT systems via machine and deep learning approaches." *Security and Quality in Cyber-Physical Systems Engineering* (2019): 443-470.



Pillars for buidling secure and Efficient IIoTs

Artificial Intelligence

- **CPS Level:** Dstirubute, adaptive Cooperative, algorithms, Accelerated Multimodal Fusioning.
- **Cooperative computation:** Distributed detection, Classification, Estimation, topology inference and Cooperation Strategies
- **System Level: AI based Intelligent Decision making**

Model based Design/Computing

- OpenCL Optimization
- Hardware/Software Partitioning
- Digital Twin like based simulation
- CPS Models
- Use Case models
- Environment models
- Reliability
- Efficiency

Security

- Run time Security monitoring
- Secure Hardware/Software component design and deployment
- Trusted Security agents/sensors

XR UIs

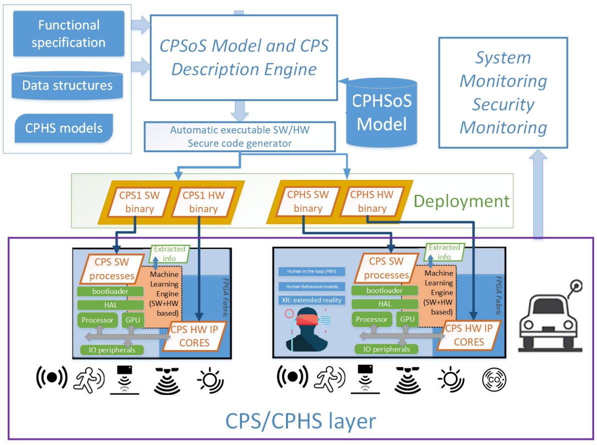
- AR Interventions
- Touchable Holographic Interfaces

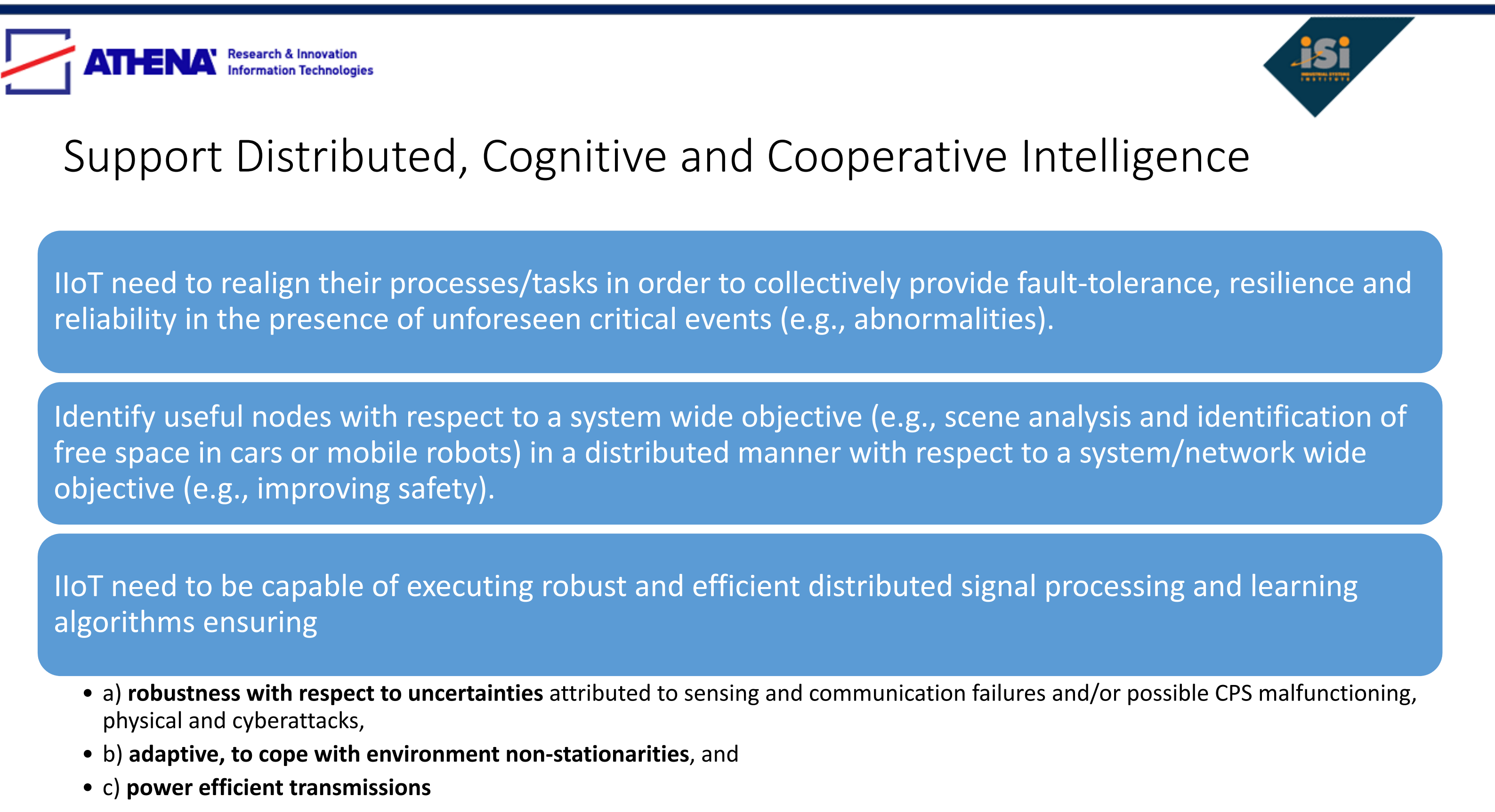
ATHENA Research & Innovation Information Technologies

Conceptual Architecture

Two architectural layers

- **System layer (CPSoS)**: responsible for the functionality of the overall System
- **IoT/CPS layer**: responsible for the functionality of each IoT/CPS device





ATHENA Research & Innovation Information Technologies

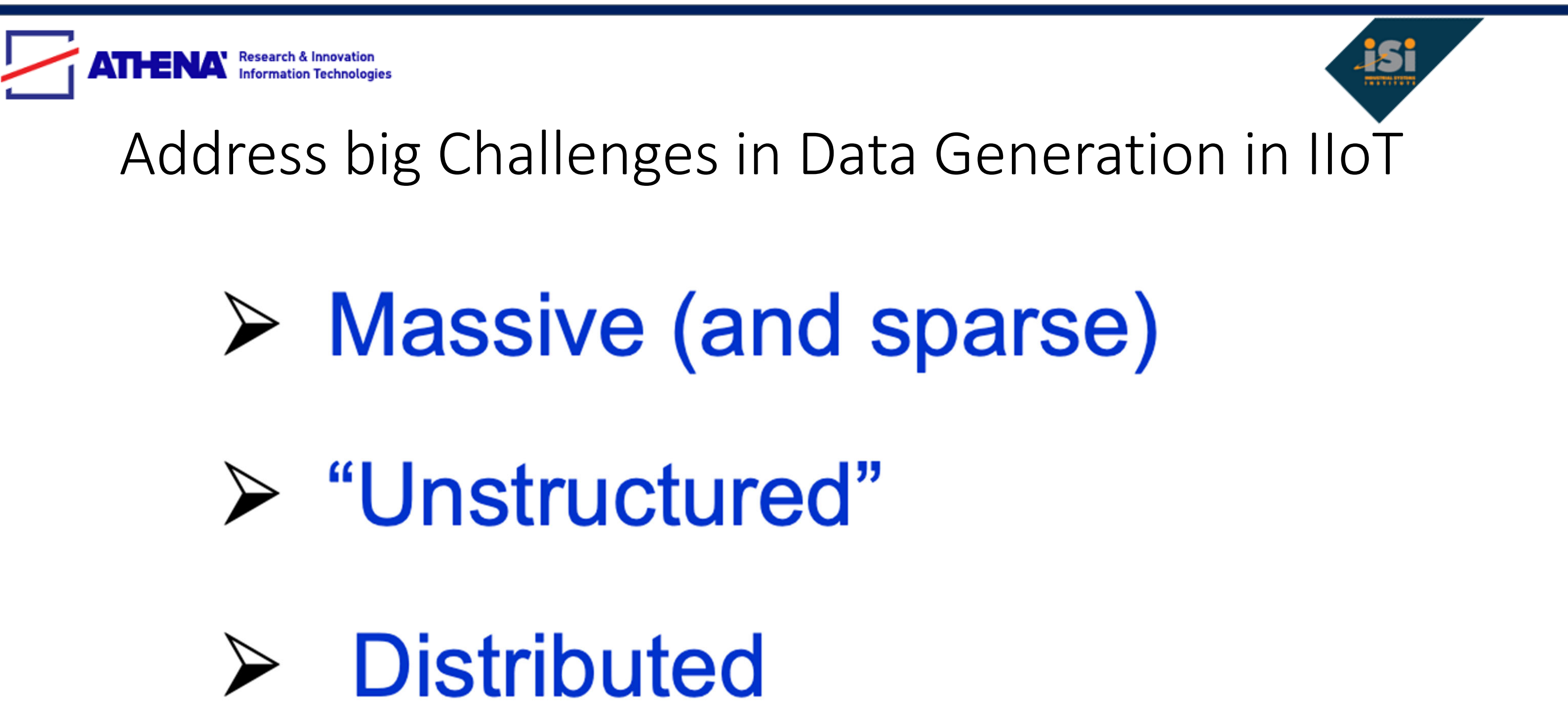
Support Distributed, Cognitive and Cooperative Intelligence

IIoT need to realign their processes/tasks in order to collectively provide fault-tolerance, resilience and reliability in the presence of unforeseen critical events (e.g., abnormalities).

Identify useful nodes with respect to a system wide objective (e.g., scene analysis and identification of free space in cars or mobile robots) in a distributed manner with respect to a system/network wide objective (e.g., improving safety).

IIoT need to be capable of executing robust and efficient distributed signal processing and learning algorithms ensuring

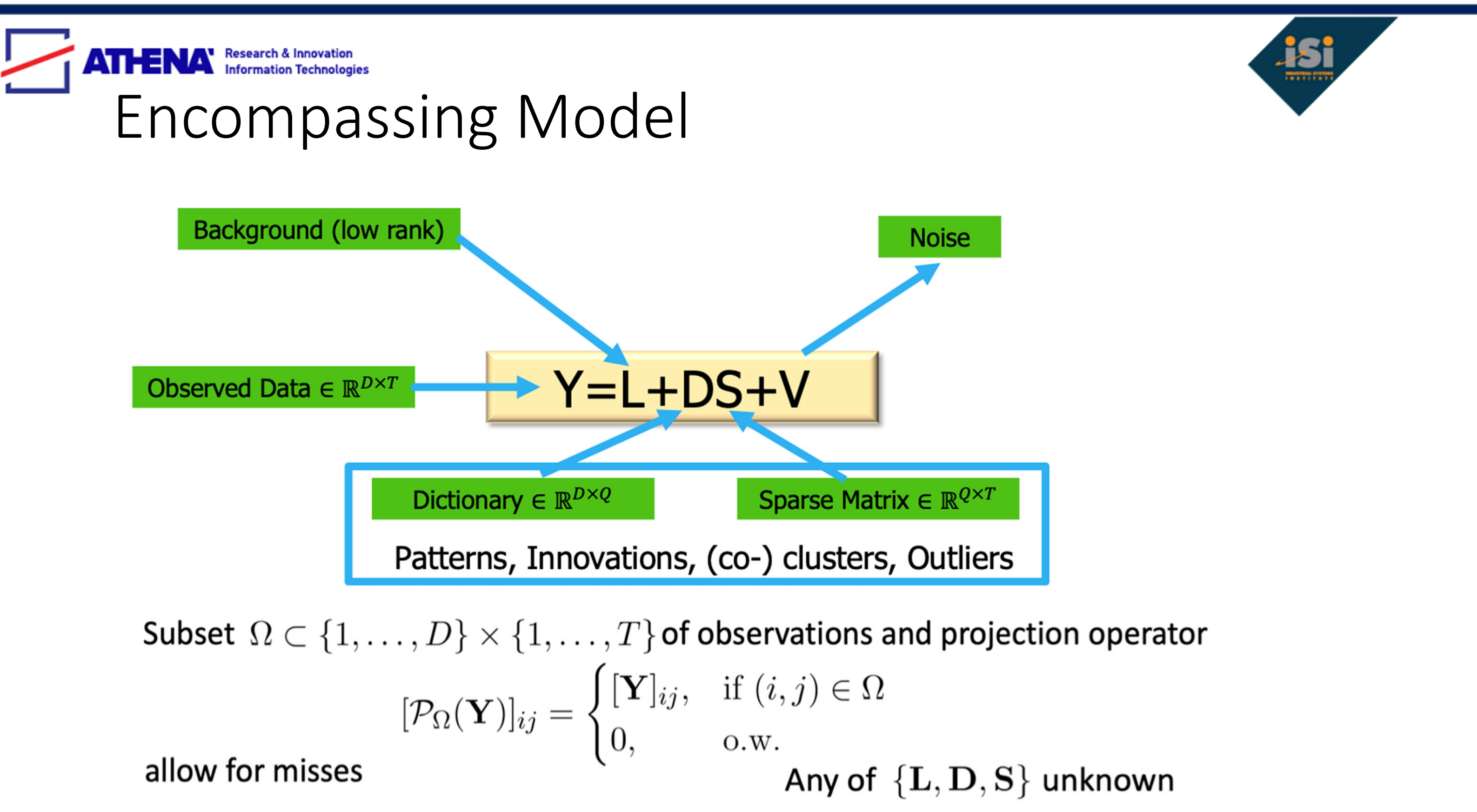
- a) **robustness with respect to uncertainties** attributed to sensing and communication failures and/or possible CPS malfunctioning, physical and cyberattacks,
- b) **adaptive, to cope with environment non-stationarities**, and
- c) **power efficient transmissions**



ATHENA Research & Innovation Information Technologies

Address big Challenges in Data Generation in IIoT

- Massive (and sparse)
- "Unstructured"
- Distributed



Encompassing Model

Background (low rank)

Noise

Observed Data ∈ $\mathbb{R}^{D\times T}$

Y=L+DS+V

Dictionary ∈ $\mathbb{R}^{D\times Q}$

Sparse Matrix ∈ $\mathbb{R}^{Q\times T}$

Patterns, Innovations, (co-) clusters, Outliers

Subset $\Omega \subset \{1,\ldots,D\}\times\{1,\ldots,T\}$ of observations and projection operator

$$[\mathcal{P}_\Omega(\mathbf{Y})]_{ij} = \begin{cases} [\mathbf{Y}]_{ij}, & \text{if } (i,j)\in\Omega \\ 0, & \text{o.w.} \end{cases}$$

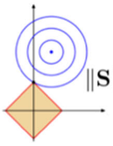
allow for misses

Any of $\{\mathbf{L},\mathbf{D},\mathbf{S}\}$ unknown

Subsumed Paradigms

- Problem formulation (for given dictionary D).

$$\min_{\{L,S\}} \frac{1}{2} \|P_{\Omega}(Y - L - DS)\|_F^2 + \lambda\|L\|_* + \lambda_1\|S\|_1$$



ℓ_1-norm

$\|\mathbf{S}\|_1 := \sum_{q,t} |s_{q,t}|$

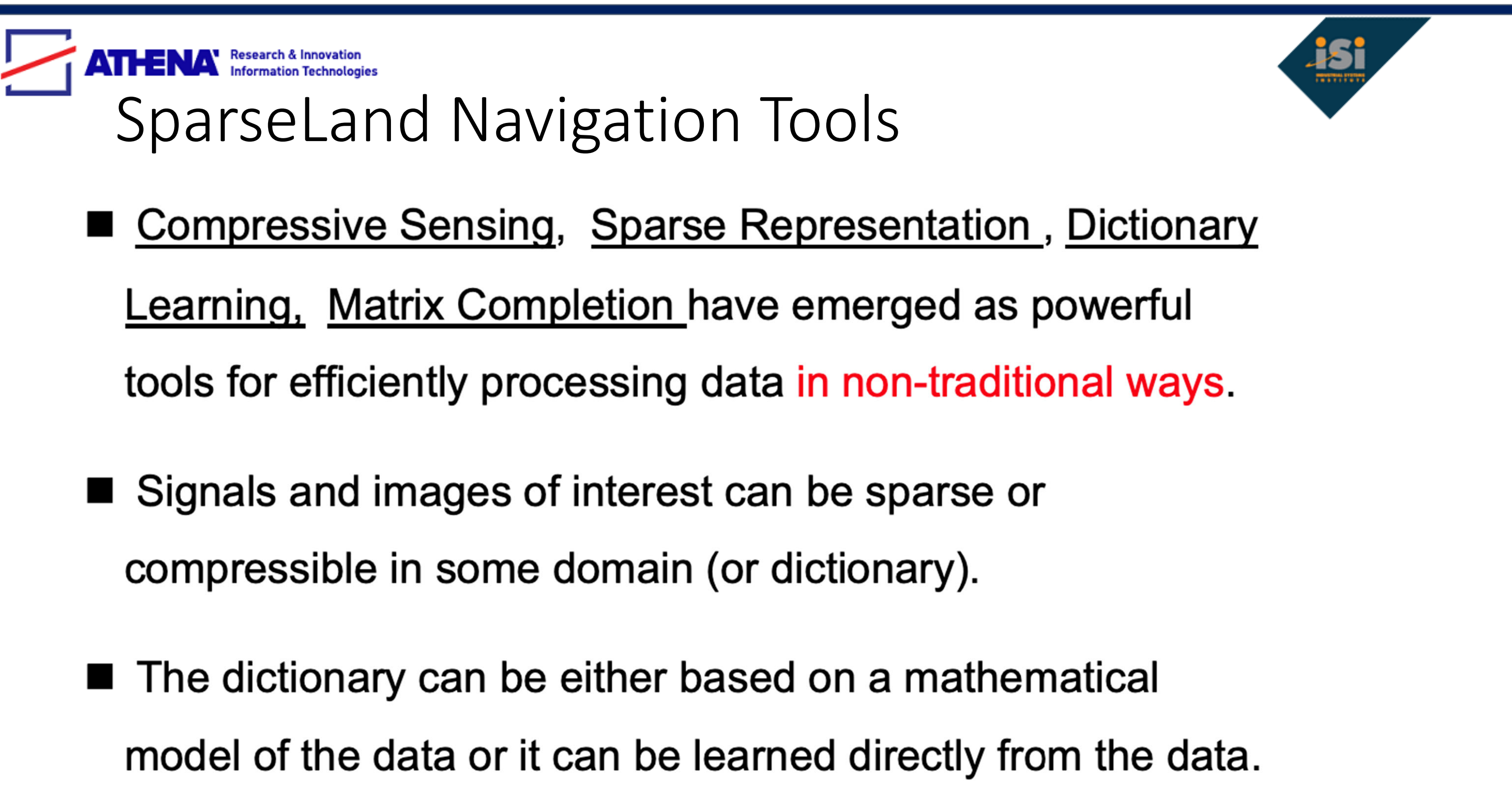
$\|\cdot\|_F$: Frobenius norm, $\|\cdot\|_*$: Nuclear norm, $\|\cdot\|_1$:l_1 norm.

Cases captured by the model:

Nuclear norm: $\|\boldsymbol{L}\|_* := \sum_{j=1}^{\mathrm{rank}(\boldsymbol{L})} \sigma_j(\boldsymbol{L})$

$\{\sigma_j(\boldsymbol{L})\}_{j=1}^{\mathrm{rank}(\boldsymbol{L})}$: singular val. of $\boldsymbol{L}$

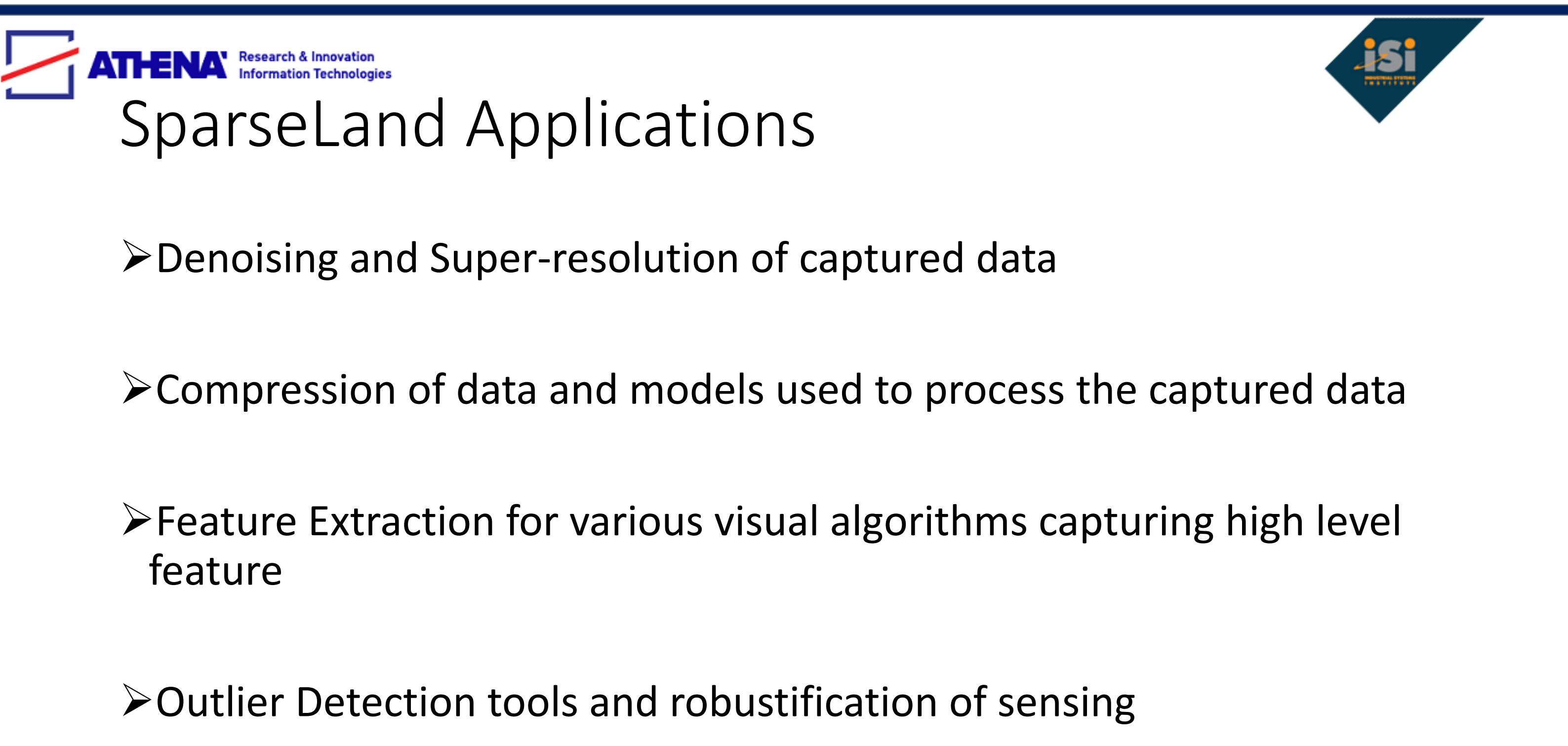
- Compressed sensing for $L = 0$ and no $P_{\Omega}(\cdot)$.
- Dictionary learning for $L = 0$, unknown D and no $P_{\Omega}(\cdot)$.
  - Non negative matrix factorization if $S_{ij} > 0$ and $D_{ij} > 0$.
- Robust PCA, for $D = I$ and $V = 0$ and no $P_{\Omega}(\cdot)$.
- PCA, for $S = 0$ and $V \neq 0$ and no $P_{\Omega}(\cdot)$.
- Matrix completion with $P_{\Omega}(\cdot)$.



ATHENA Research & Innovation Information Technologies

SparseLand Navigation Tools

- Compressive Sensing, Sparse Representation , Dictionary Learning, Matrix Completion have emerged as powerful tools for efficiently processing data in non-traditional ways.
- Signals and images of interest can be sparse or compressible in some domain (or dictionary).
- The dictionary can be either based on a mathematical model of the data or it can be learned directly from the data.



ATHENA Research & Innovation Information Technologies
isi

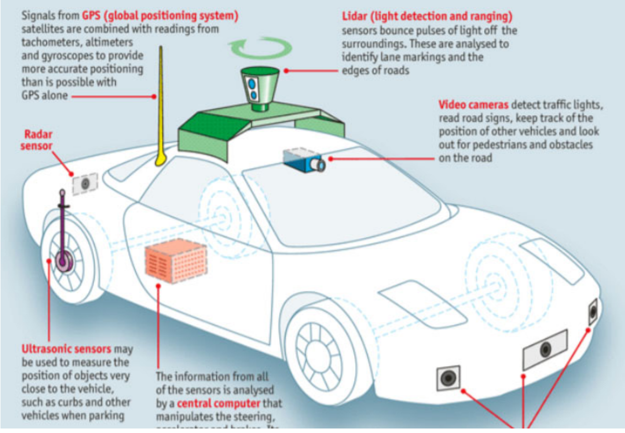
SparseLand Applications

- Denoising and Super-resolution of captured data
- Compression of data and models used to process the captured data
- Feature Extraction for various visual algorithms capturing high level feature
- Outlier Detection tools and robustification of sensing

ATHENA Research & Innovation Information Technologies

Automotive Applications -Physical Ecosystem of autonomous Car

- Global Positioning System (GPS).
- Light Detection and Ranging (LIDAR)
- Cameras (Video).
- Ultrasonic Sensors
- Central Computer
- Dedicated Short-Range Communications-Based Receiver V2X.



Signals from **GPS (global positioning system)** satellites are combined with readings from tachometers, altimeters and gyroscopes to provide more accurate positioning than is possible with GPS alone

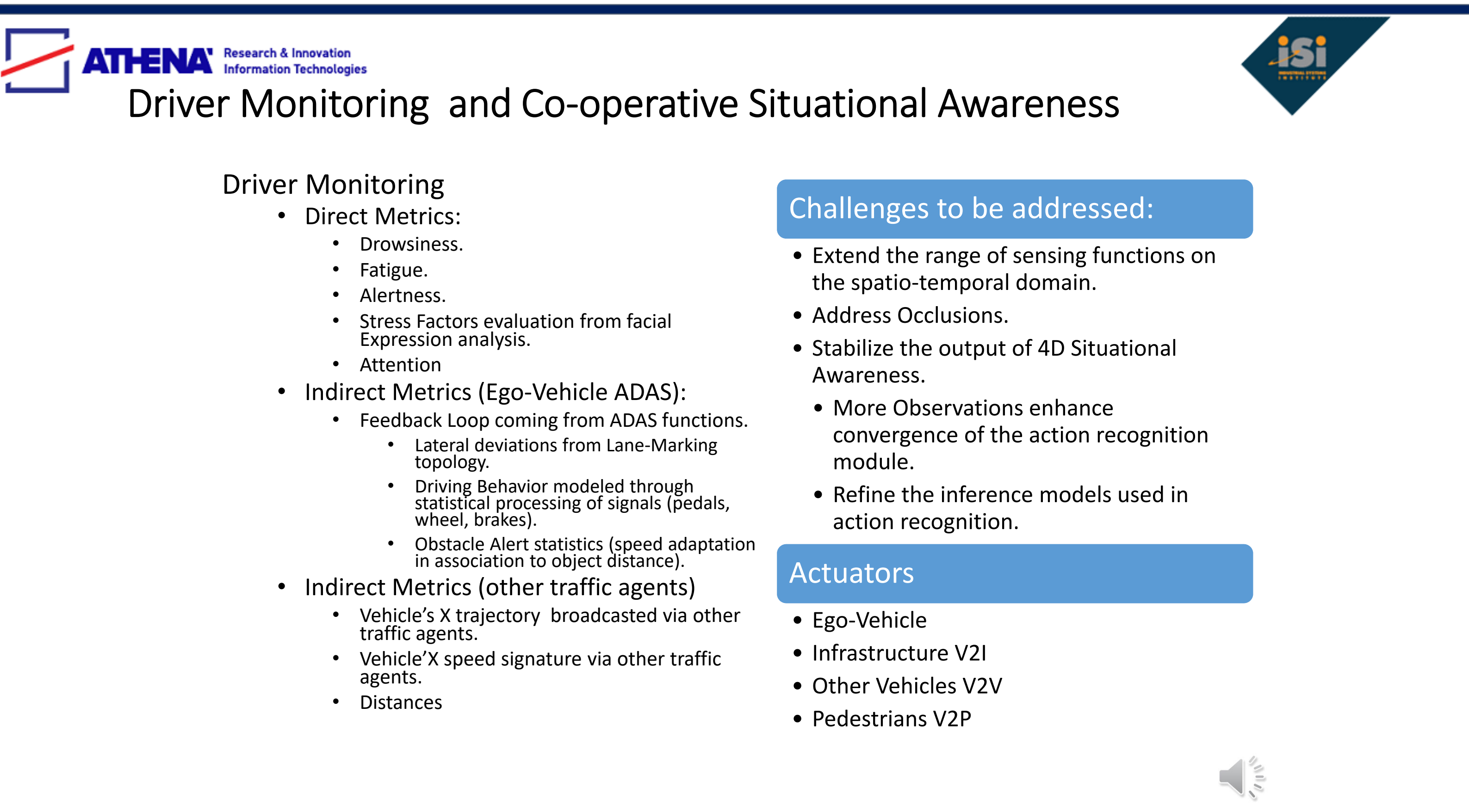
Lidar (light detection and ranging) sensors bounce pulses of light off the surroundings. These are analysed to identify lane markings and the edges of roads

Video cameras detect traffic lights, read road signs, keep track of the position of other vehicles and look out for pedestrians and obstacles on the road

Radar sensor

Ultrasonic sensors may be used to measure the position of objects very close to the vehicle, such as curbs and other vehicles when parking

The information from all of the sensors is analysed by a **central computer** that manipulates the steering,



ATHENA Research & Innovation Information Technologies

Driver Monitoring and Co-operative Situational Awareness

Driver Monitoring

- Direct Metrics:
  - Drowsiness.
  - Fatigue.
  - Alertness.
  - Stress Factors evaluation from facial Expression analysis.
  - Attention
- Indirect Metrics (Ego-Vehicle ADAS):
  - Feedback Loop coming from ADAS functions.
    - Lateral deviations from Lane-Marking topology.
    - Driving Behavior modeled through statistical processing of signals (pedals, wheel, brakes).
    - Obstacle Alert statistics (speed adaptation in association to object distance).
- Indirect Metrics (other traffic agents)
  - Vehicle's X trajectory broadcasted via other traffic agents.
  - Vehicle'X speed signature via other traffic agents.
  - Distances

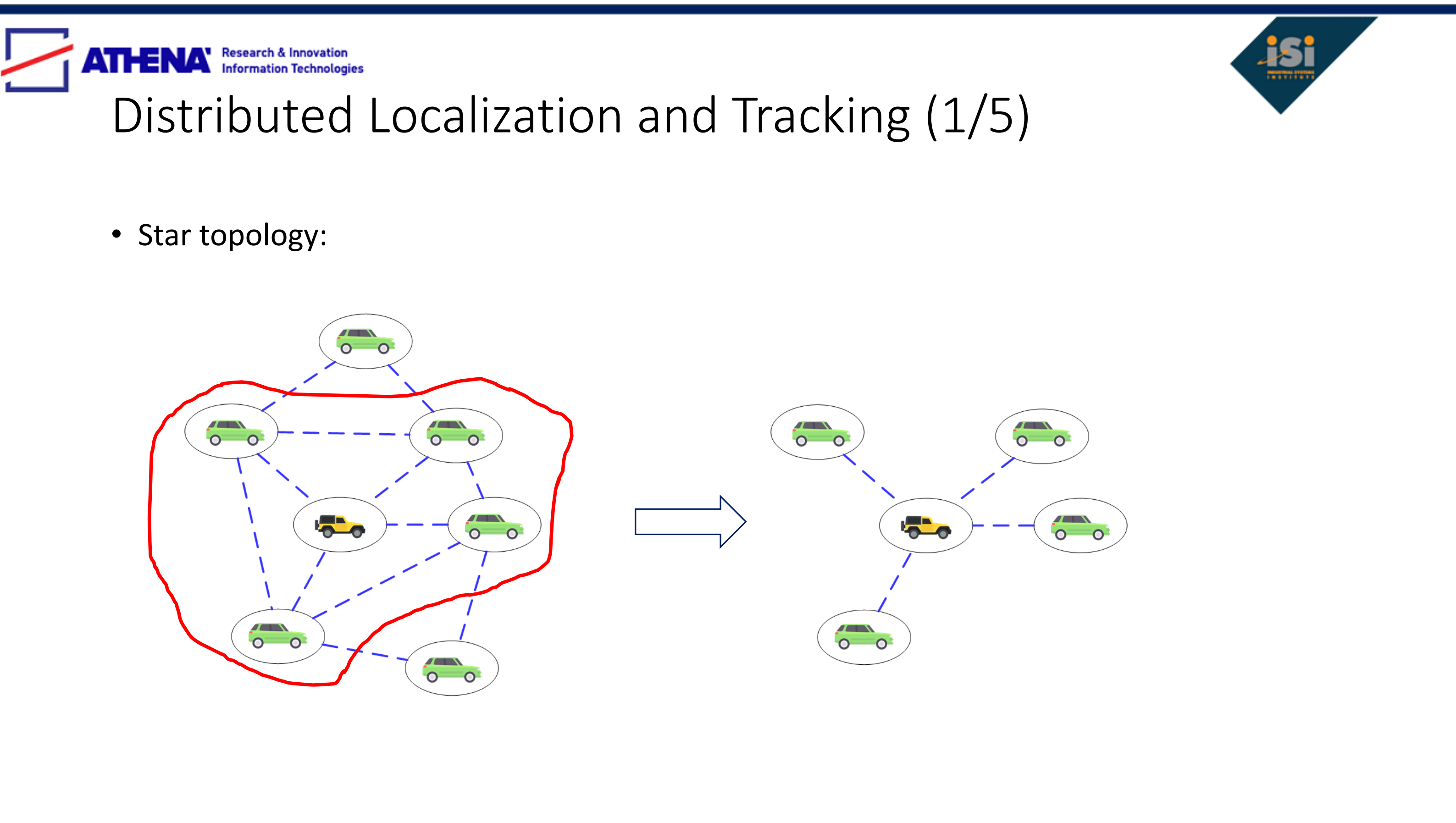
Challenges to be addressed:

- Extend the range of sensing functions on the spatio-temporal domain.
- Address Occlusions.
- Stabilize the output of 4D Situational Awareness.
  - More Observations enhance convergence of the action recognition module.
  - Refine the inference models used in action recognition.

Actuators

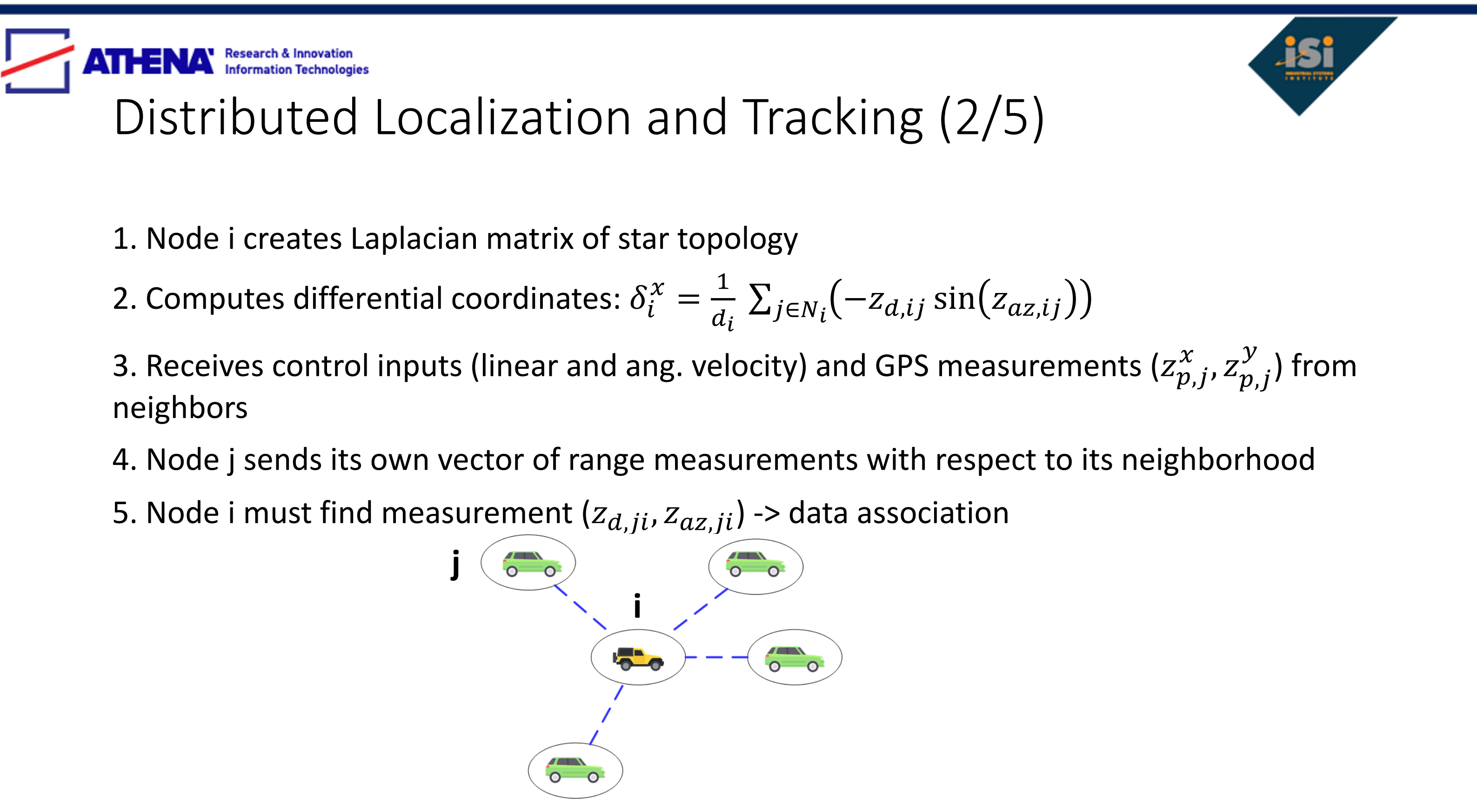
- Ego-Vehicle
- Infrastructure V2I
- Other Vehicles V2V
- Pedestrians V2P

Robust 4D Awareness



Distributed Localization and Tracking (1/5)

- Star topology:



Distributed Localization and Tracking (2/5)

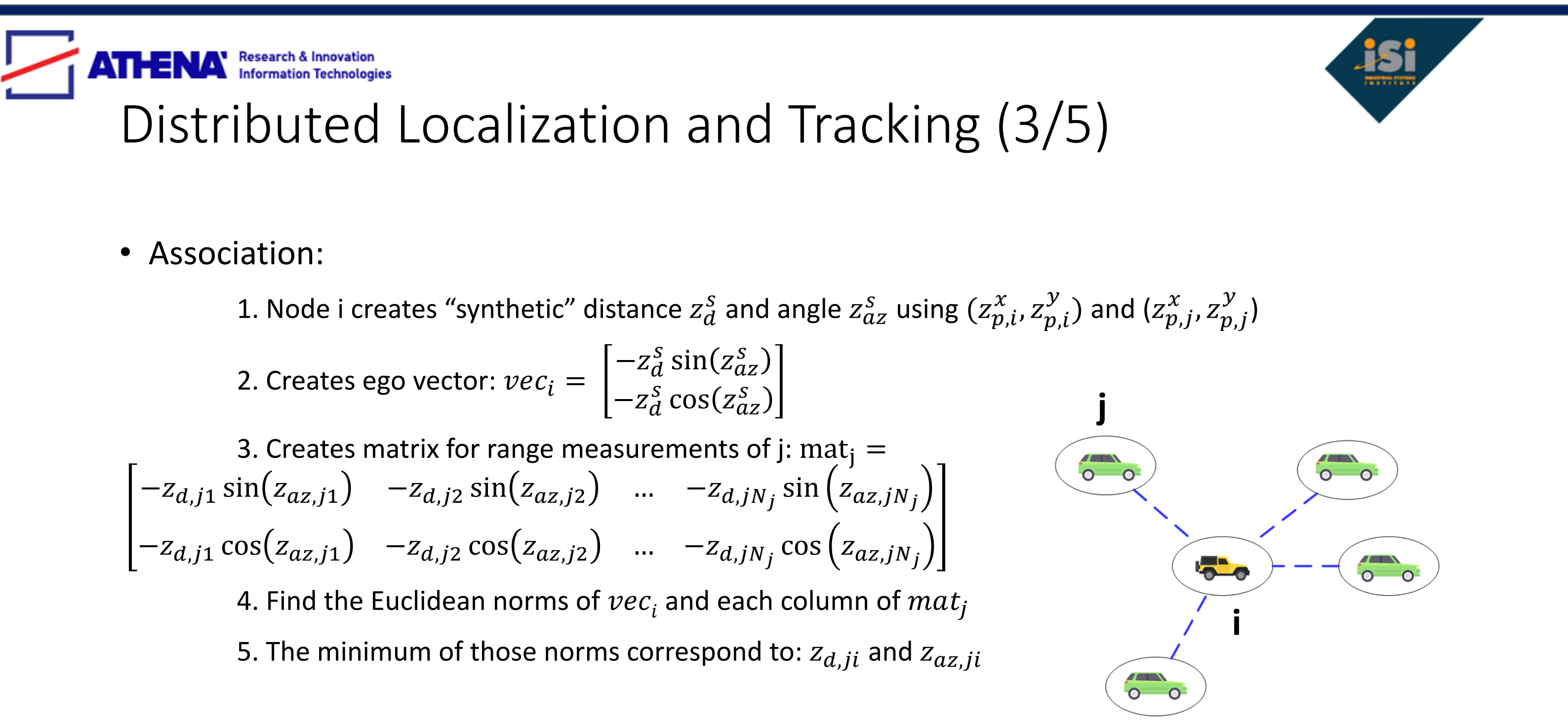
1. Node i creates Laplacian matrix of star topology

2. Computes differential coordinates: $\delta_i^x = \frac{1}{d_i} \sum_{j \in N_i} \left(-z_{d,ij} \sin\left(z_{az,ij}\right)\right)$

3. Receives control inputs (linear and ang. velocity) and GPS measurements $(z_{p,j}^x, z_{p,j}^y)$ from neighbors

4. Node j sends its own vector of range measurements with respect to its neighborhood

5. Node i must find measurement $(z_{d,ji}, z_{az,ji})$ -> data association



ATHENA Research & Innovation Information Technologies

Distributed Localization and Tracking (3/5)

- Association:

1. Node i creates “synthetic” distance z_d^s and angle z_{az}^s using $(z_{p,i}^x, z_{p,i}^y)$ and $(z_{p,j}^x, z_{p,j}^y)$

2. Creates ego vector: $vec_i = \begin{bmatrix} -z_d^s \sin(z_{az}^s) \\ -z_d^s \cos(z_{az}^s) \end{bmatrix}$

3. Creates matrix for range measurements of j: $\mathrm{mat_j} =$

$$\begin{bmatrix} -z_{d,j1}\sin\left(z_{az,j1}\right) & -z_{d,j2}\sin\left(z_{az,j2}\right) & \dots & -z_{d,jN_j}\sin\left(z_{az,jN_j}\right) \\ -z_{d,j1}\cos\left(z_{az,j1}\right) & -z_{d,j2}\cos\left(z_{az,j2}\right) & \dots & -z_{d,jN_j}\cos\left(z_{az,jN_j}\right) \end{bmatrix}$$

4. Find the Euclidean norms of vec_i and each column of mat_j

5. The minimum of those norms correspond to: $z_{d,ji}$ and $z_{az,ji}$

ATHENA Research & Innovation Information Technologies

Distributed Localization and Tracking (4/5)

- Least squares minimization:

$$argmin_{\boldsymbol{x_i}} \left\| \widetilde{\boldsymbol{L}}_{\boldsymbol{i}} \boldsymbol{x_i} - \boldsymbol{b}_{\boldsymbol{i}}^{\boldsymbol{x}} \right\|_2^2$$

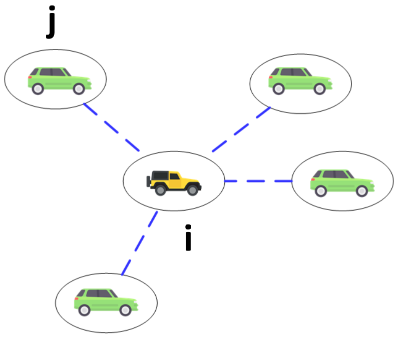
- State vector $\boldsymbol{x_i} \in \mathcal{R}^{N_i+1}$: $\boldsymbol{x}$ positions of ego and neighbors

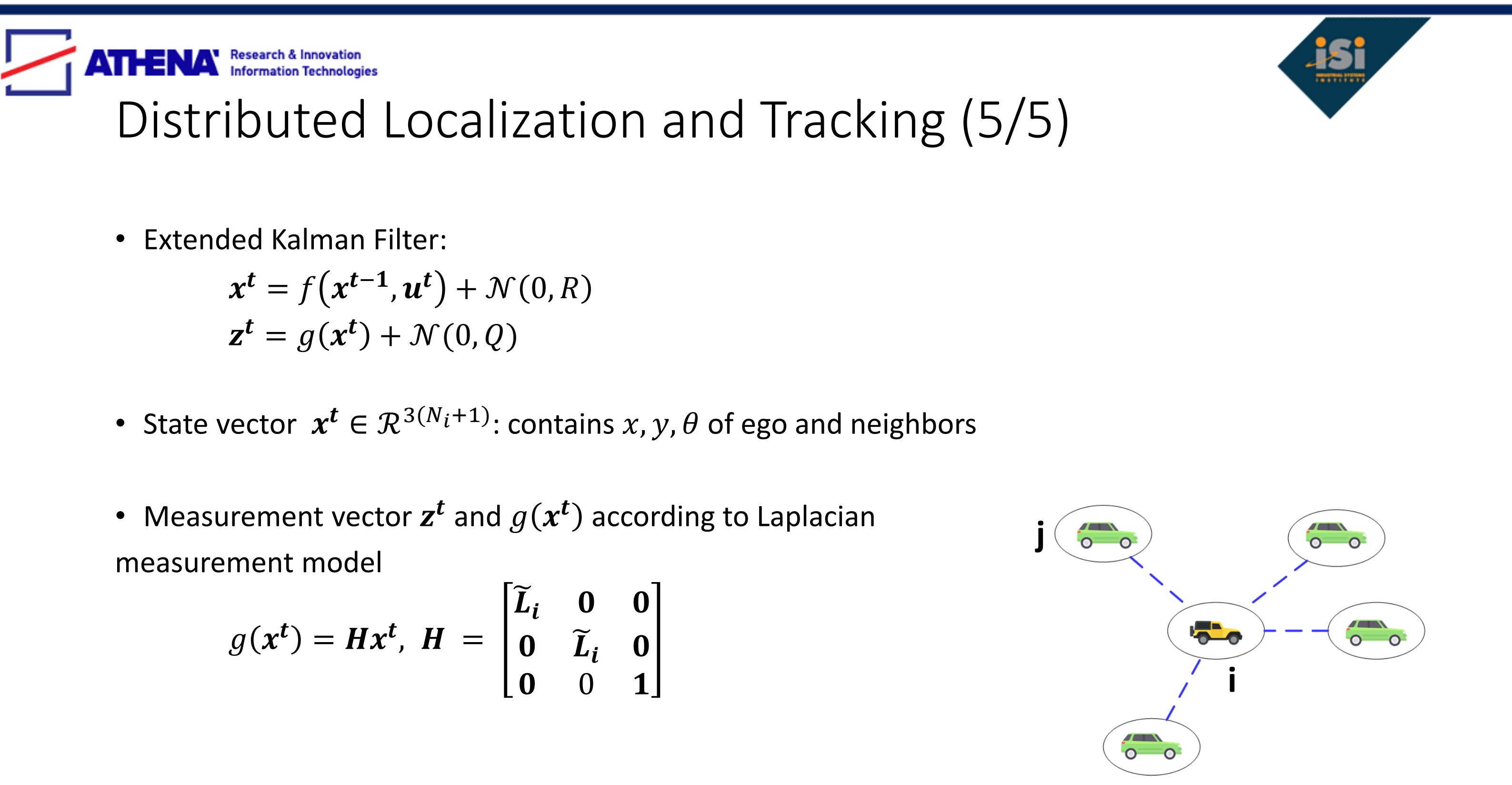
- Measurement vector $\boldsymbol{b}_{\boldsymbol{i}}^{\boldsymbol{x}} \in \mathcal{R}^{2(N_i+1)}$:

$$\boldsymbol{b}_{\boldsymbol{i}}^{\boldsymbol{x}} = \begin{bmatrix} \delta_i^x \\ -z_{d,ji} \sin z_{az,ji} \\ \dots \\ z_{p,i}^x \\ z_{p,j}^x \\ \dots \end{bmatrix}$$

Range measurements of ego and neighbors

GPS measurements of ego and neighbors





Distributed Localization and Tracking (5/5)

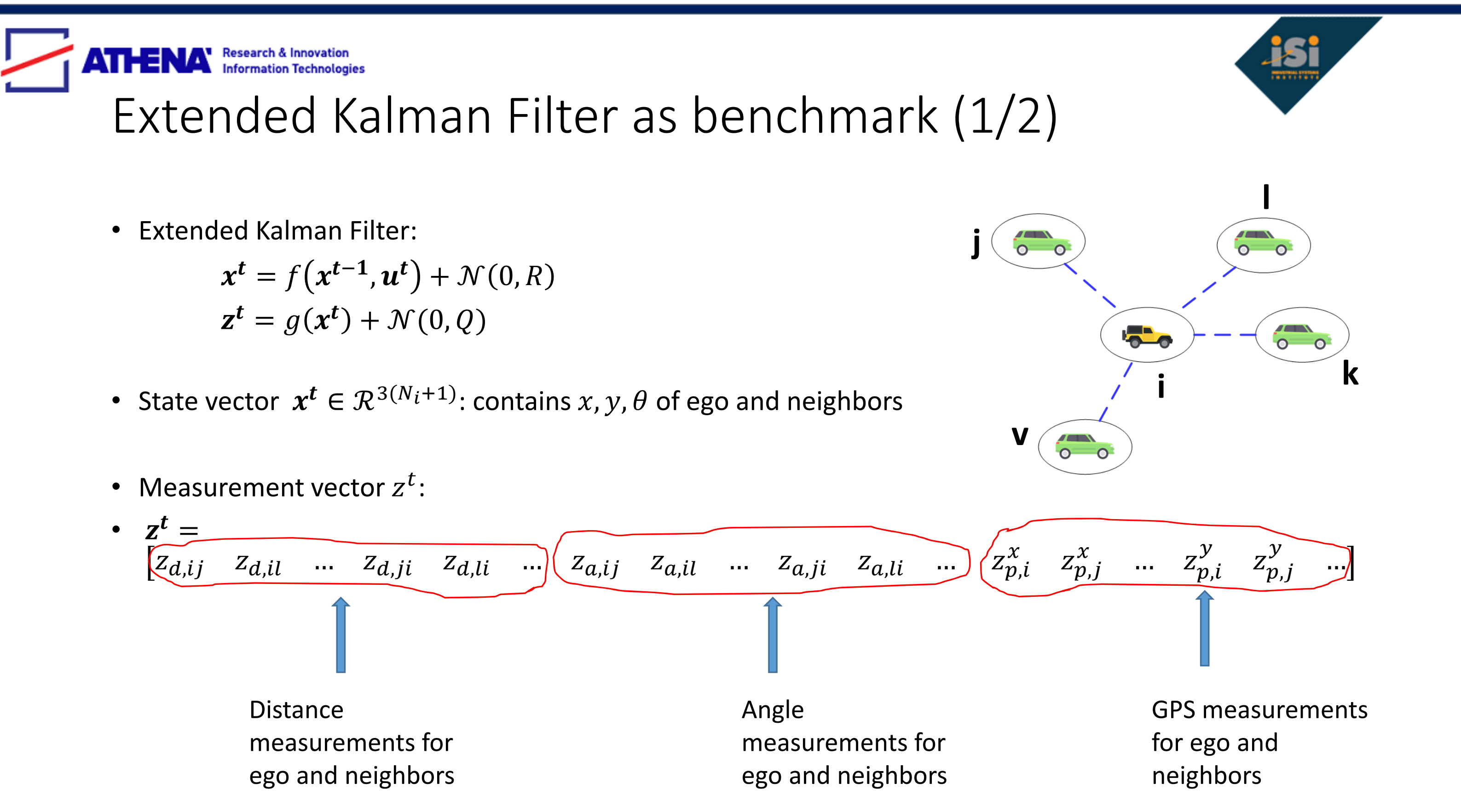
- Extended Kalman Filter:

$$\boldsymbol{x^t} = f\left(\boldsymbol{x^{t-1}}, \boldsymbol{u^t}\right) + \mathcal{N}(0, R)$$
$$\boldsymbol{z^t} = g(\boldsymbol{x^t}) + \mathcal{N}(0, Q)$$

- State vector $\boldsymbol{x^t} \in \mathcal{R}^{3(N_i+1)}$: contains x, y, θ of ego and neighbors

- Measurement vector $\boldsymbol{z^t}$ and $g(\boldsymbol{x^t})$ according to Laplacian measurement model

$$g(\boldsymbol{x^t}) = \boldsymbol{Hx^t},\ \boldsymbol{H} = \begin{bmatrix} \boldsymbol{\tilde{L}_i} & \boldsymbol{0} & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{\tilde{L}_i} & \boldsymbol{0} \\ \boldsymbol{0} & 0 & \boldsymbol{1} \end{bmatrix}$$



Extended Kalman Filter as benchmark (1/2)

- Extended Kalman Filter:

$$\boldsymbol{x^t} = f\left(\boldsymbol{x^{t-1}}, \boldsymbol{u^t}\right) + \mathcal{N}(0, R)$$
$$\boldsymbol{z^t} = g(\boldsymbol{x^t}) + \mathcal{N}(0, Q)$$

- State vector $\boldsymbol{x^t} \in \mathcal{R}^{3(N_i+1)}$: contains x, y, θ of ego and neighbors

- Measurement vector z^t:

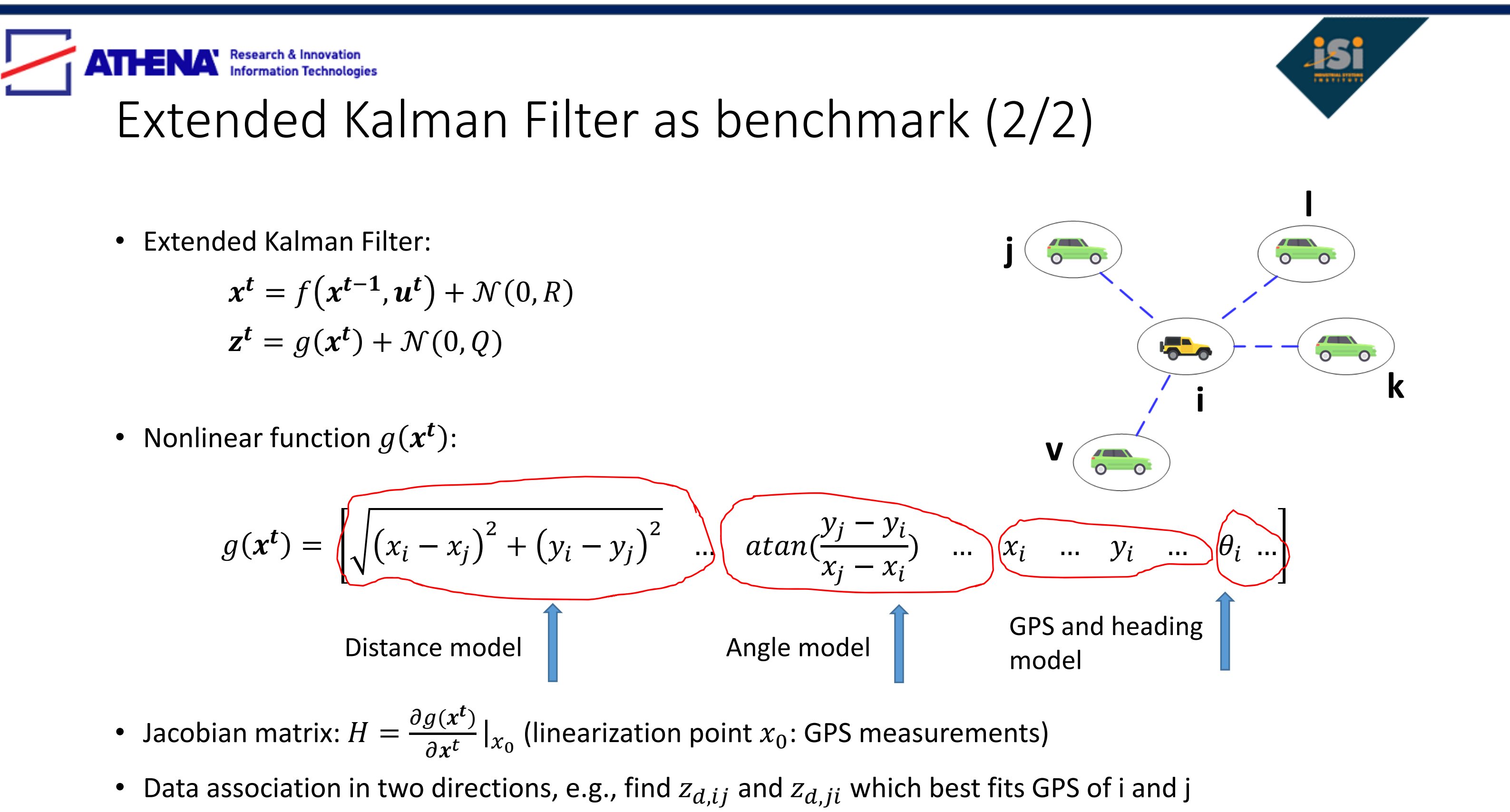
- $\boldsymbol{z^t} = [z_{d,ij} \quad z_{d,il} \quad \dots \quad z_{d,ji} \quad z_{d,li} \quad \dots \quad z_{a,ij} \quad z_{a,il} \quad \dots \quad z_{a,ji} \quad z_{a,li} \quad \dots \quad z_{p,i}^{x} \quad z_{p,j}^{x} \quad \dots \quad z_{p,i}^{y} \quad z_{p,j}^{y} \quad \dots]$

Distance measurements for ego and neighbors

Angle measurements for ego and neighbors

GPS measurements for ego and neighbors

©MECO.net


ATHENA Research & Innovation Information Technologies
isi
j
l
i
k
v

Extended Kalman Filter as benchmark (2/2)

- Extended Kalman Filter:

$$\boldsymbol{x}^{\boldsymbol{t}} = f\left(\boldsymbol{x}^{\boldsymbol{t-1}}, \boldsymbol{u}^{\boldsymbol{t}}\right) + \mathcal{N}(0, R)$$
$$\boldsymbol{z}^{\boldsymbol{t}} = g(\boldsymbol{x}^{\boldsymbol{t}}) + \mathcal{N}(0, Q)$$

- Nonlinear function $g(\boldsymbol{x}^{\boldsymbol{t}})$:

$$g(\boldsymbol{x}^{\boldsymbol{t}}) = \left[\sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad \dots \quad atan(\frac{y_j - y_i}{x_j - x_i}) \quad \dots \quad x_i \quad \dots \quad y_i \quad \dots \quad \theta_i \quad \dots\right]$$

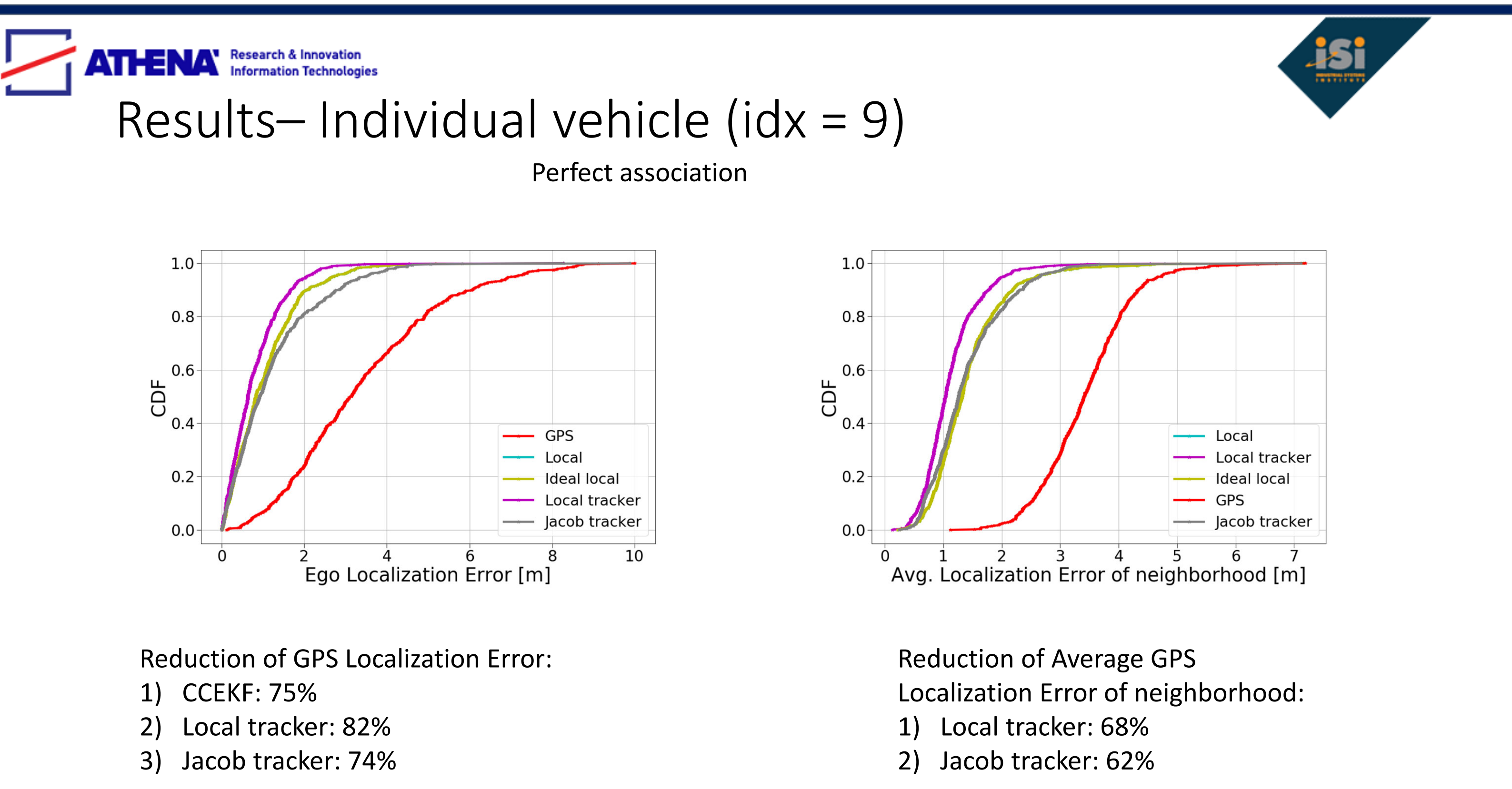
Distance model

Angle model

GPS and heading model

- Jacobian matrix: $H = \frac{\partial g(\boldsymbol{x}^{\boldsymbol{t}})}{\partial \boldsymbol{x}^{t}}|_{x_0}$ (linearization point x_0: GPS measurements)
- Data association in two directions, e.g., find $z_{d,ij}$ and $z_{d,ji}$ which best fits GPS of i and j

©MECO.net



Results– Individual vehicle (idx = 9)

Perfect association

Reduction of GPS Localization Error:

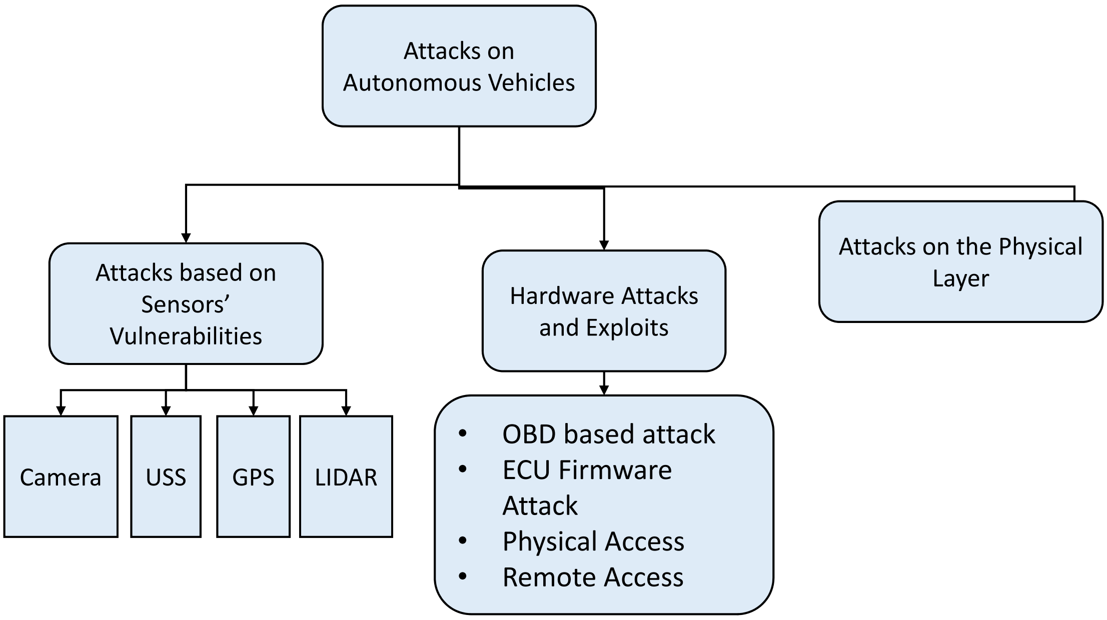
1) CCEKF: 75%
2) Local tracker: 82%
3) Jacob tracker: 74%

Reduction of Average GPS Localization Error of neighborhood:

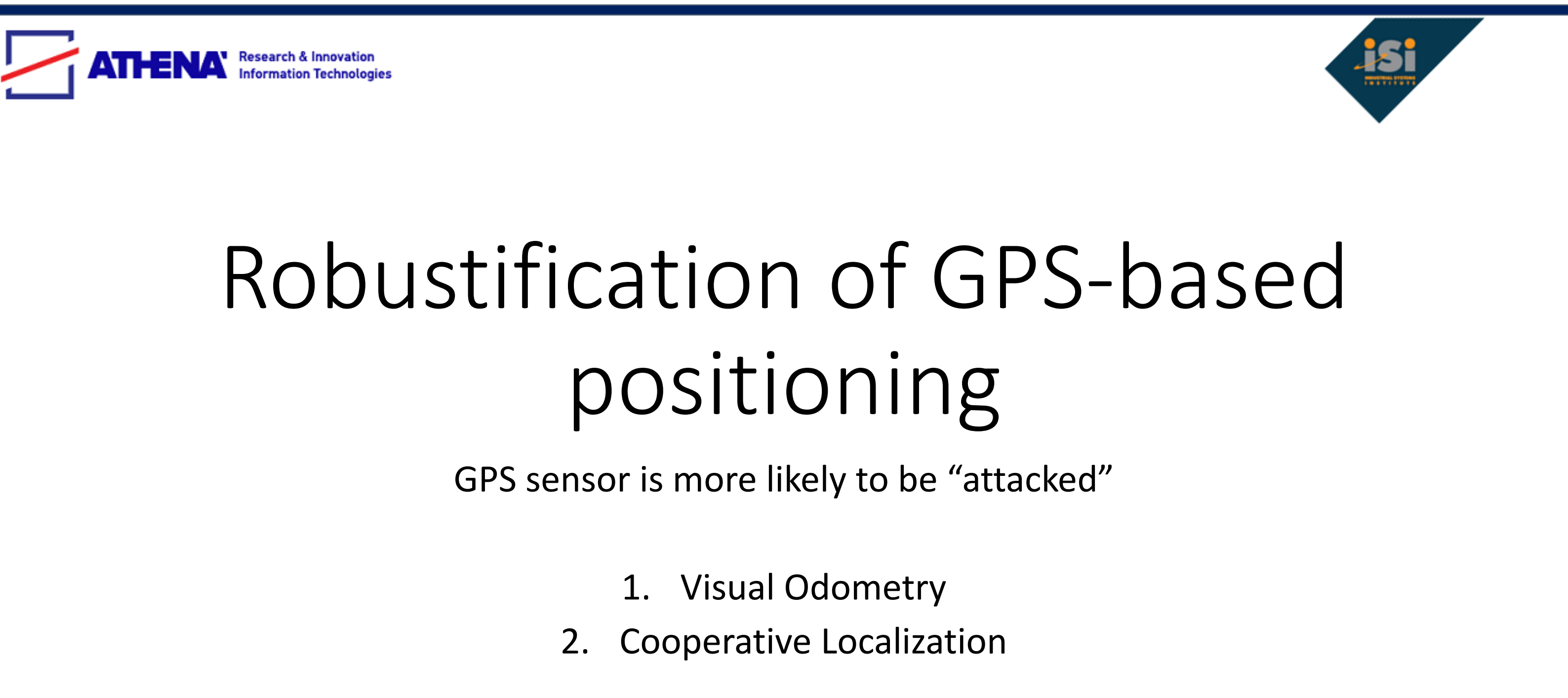
1) Local tracker: 68%
2) Jacob tracker: 62%

ATHENA Research & Innovation Information Technologies

Cyber Attacks on Autonomous Driving


Attacks on Autonomous Vehicles
Attacks based on Sensors' Vulnerabilities
Hardware Attacks and Exploits
Attacks on the Physical Layer
Camera
USS
GPS
LIDAR

- OBD based attack
- ECU Firmware Attack
- Physical Access
- Remote Access



Robustification of GPS-based positioning

GPS sensor is more likely to be "attacked"

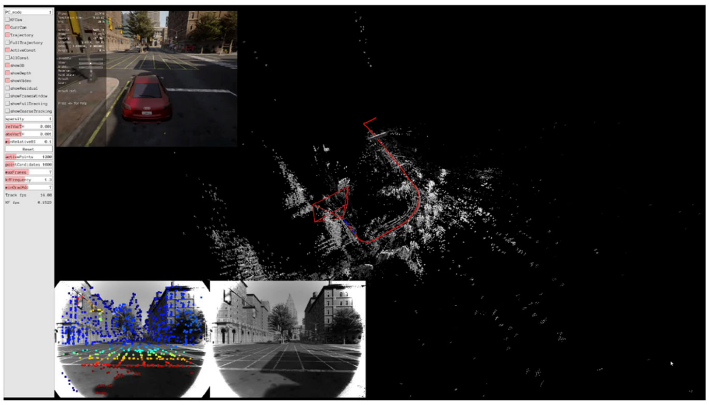
1. Visual Odometry
2. Cooperative Localization

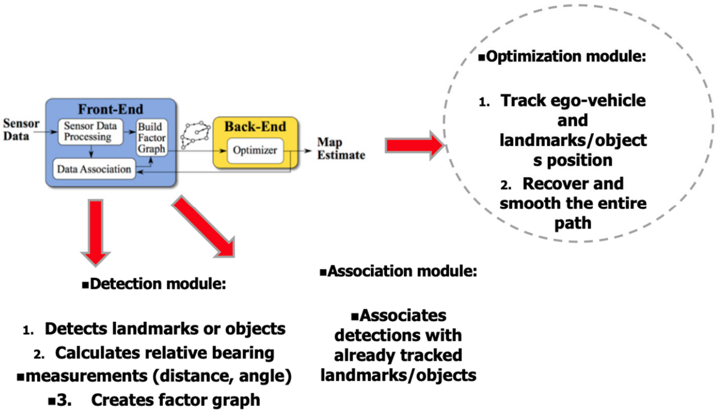
ATHENA Research & Innovation Information Technologies

Visual Odometry

- Localize camera sensor (integrated to the vehicle) and map the unknown environment.

- Direct Sparse Odometry (DSO) is popular approach.





▪Optimization module:

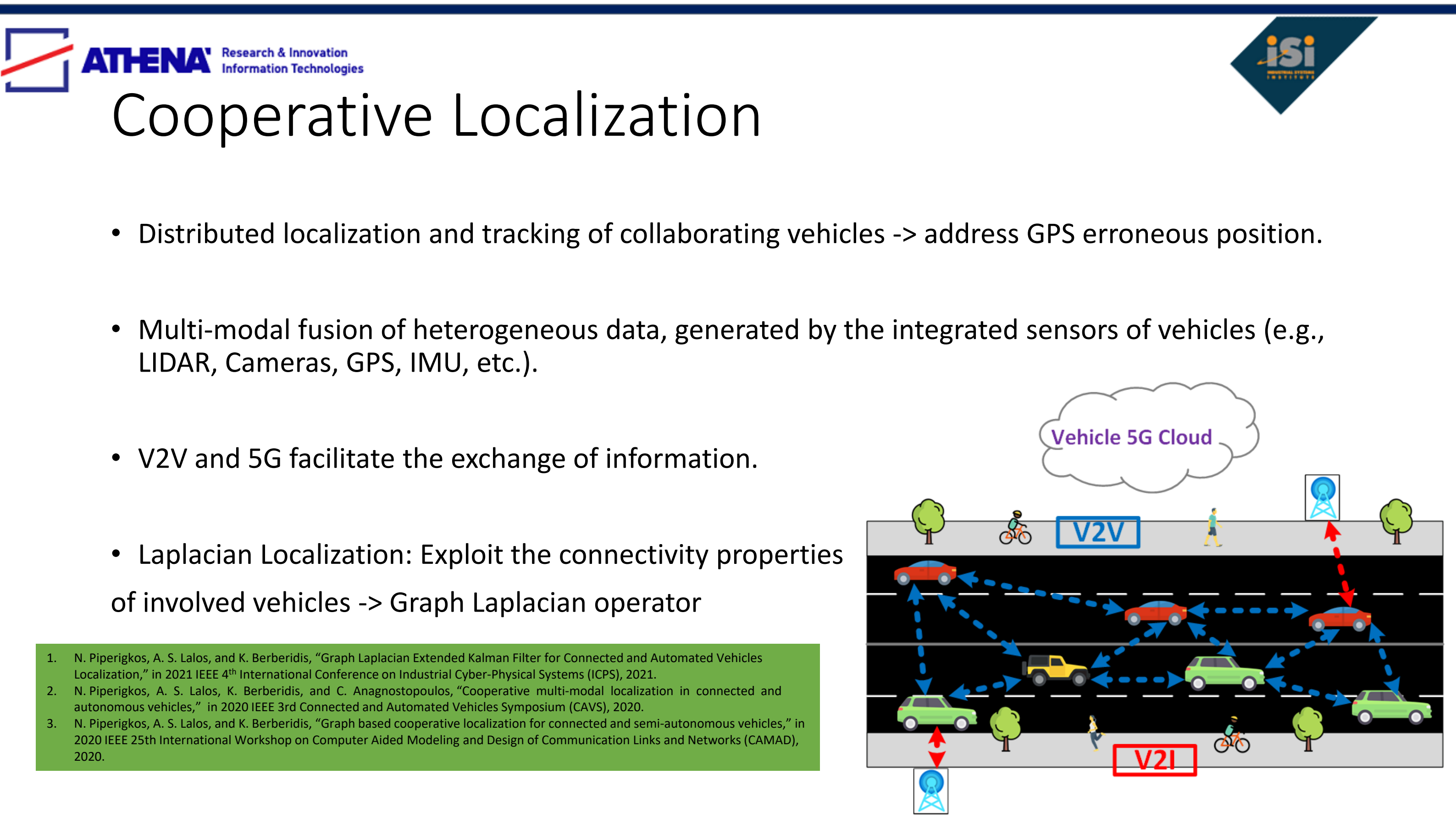
1. Track ego-vehicle and landmarks/objects position
2. Recover and smooth the entire path

▪Detection module:

1. Detects landmarks or objects
2. Calculates relative bearing ▪measurements (distance, angle)
▪3. Creates factor graph

▪Association module:

▪Associates detections with already tracked landmarks/objects


Vehicle 5G Cloud
V2V
V2I

Cooperative Localization

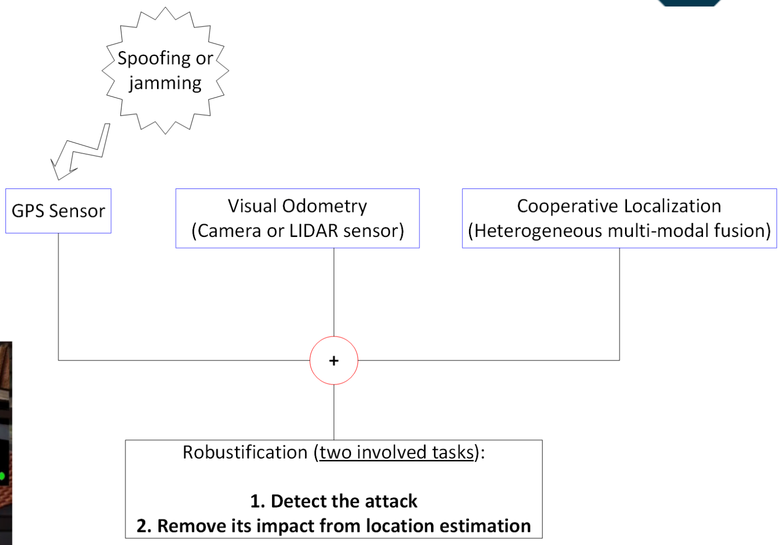
- Distributed localization and tracking of collaborating vehicles -> address GPS erroneous position.
- Multi-modal fusion of heterogeneous data, generated by the integrated sensors of vehicles (e.g., LIDAR, Cameras, GPS, IMU, etc.).
- V2V and 5G facilitate the exchange of information.
- Laplacian Localization: Exploit the connectivity properties of involved vehicles -> Graph Laplacian operator

1. N. Piperigkos, A. S. Lalos, and K. Berberidis, "Graph Laplacian Extended Kalman Filter for Connected and Automated Vehicles Localization," in 2021 IEEE 4th International Conference on Industrial Cyber-Physical Systems (ICPS), 2021.
2. N. Piperigkos, A. S. Lalos, K. Berberidis, and C. Anagnostopoulos, "Cooperative multi-modal localization in connected and autonomous vehicles," in 2020 IEEE 3rd Connected and Automated Vehicles Symposium (CAVS), 2020.
3. N. Piperigkos, A. S. Lalos, and K. Berberidis, "Graph based cooperative localization for connected and semi-autonomous vehicles," in 2020 IEEE 25th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD), 2020.

ATHENA Research & Innovation Information Technologies

Robustification

- General architecture diagram:



Spoofing or jamming

GPS Sensor

Visual Odometry (Camera or LIDAR sensor)

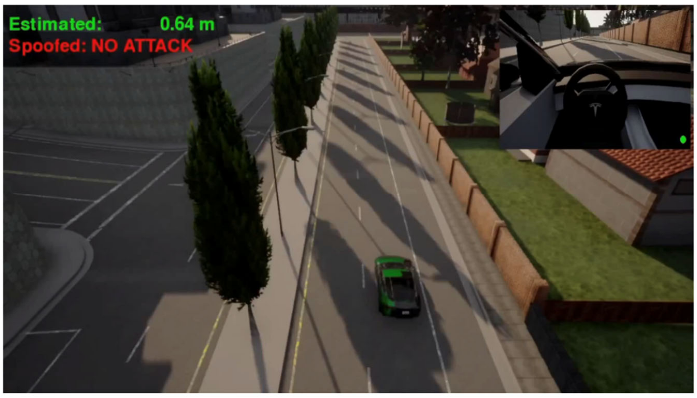
Cooperative Localization (Heterogeneous multi-modal fusion)

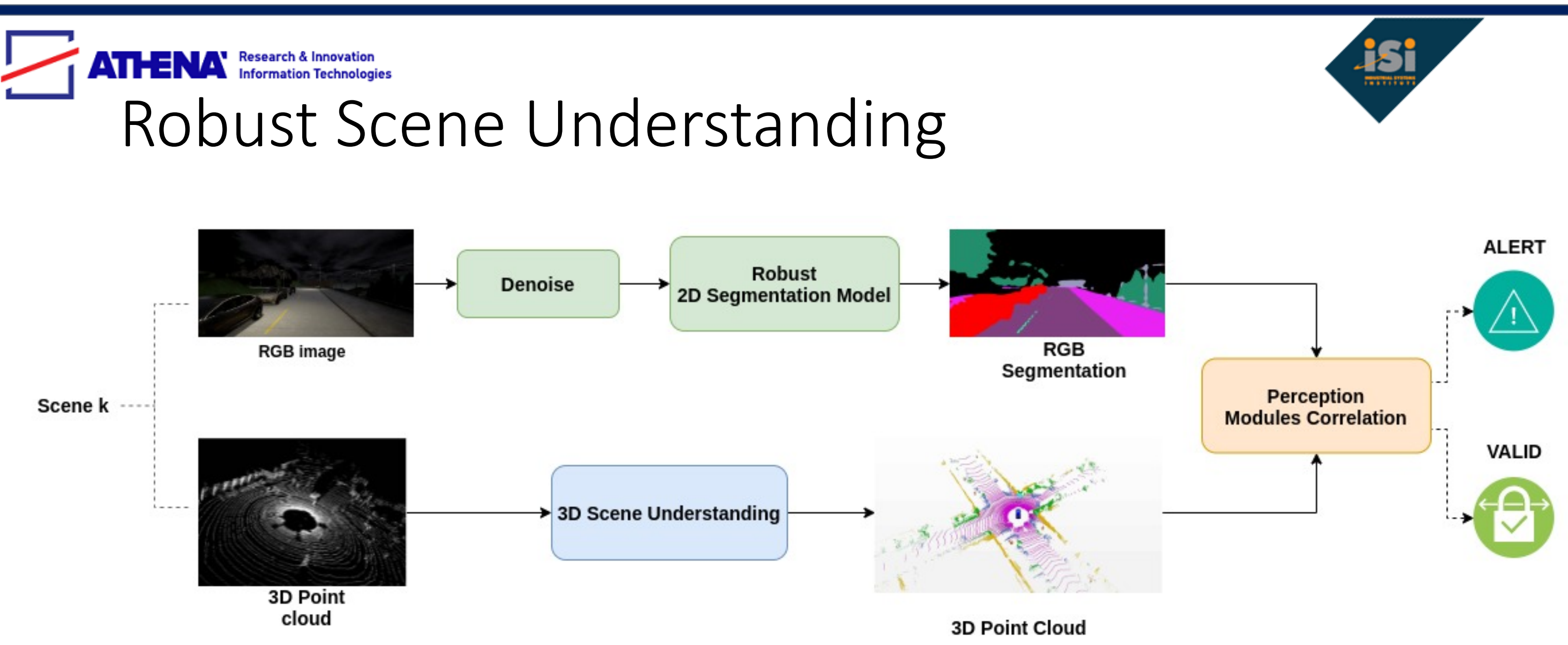
+

Robustification (two involved tasks):

1. Detect the attack

2. Remove its impact from location estimation





ATHENA Research & Innovation Information Technologies

Robust Scene Understanding

Scene k

RGB image

Denoise

Robust 2D Segmentation Model

RGB Segmentation

3D Point cloud

3D Scene Understanding

3D Point Cloud

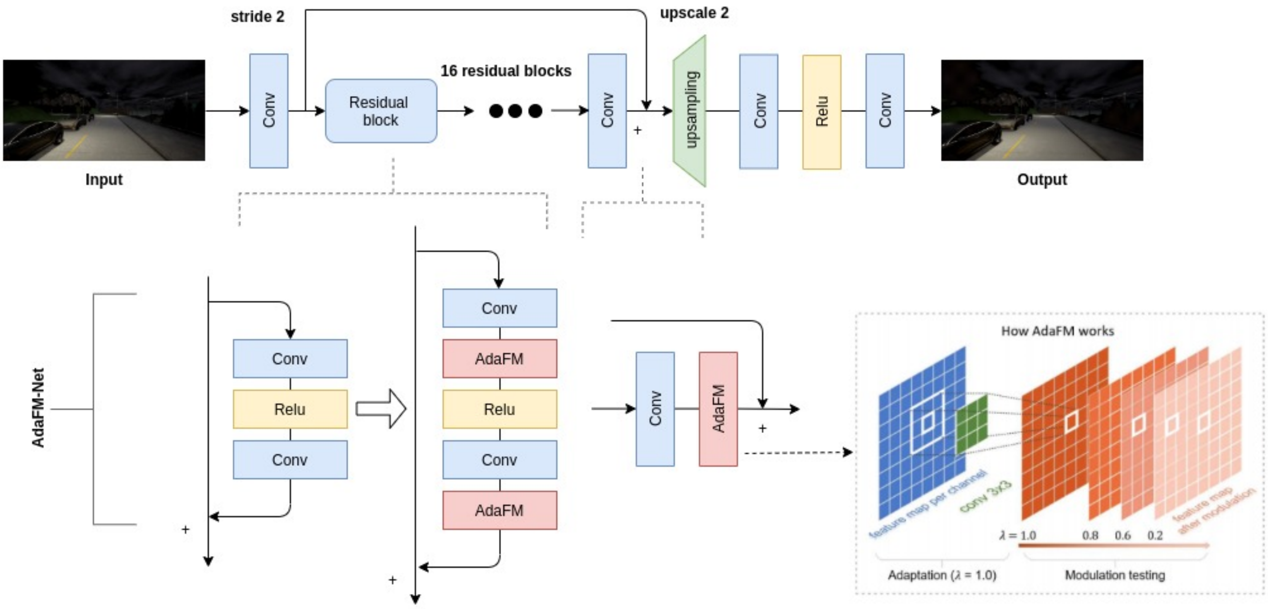
Perception Modules Correlation

ALERT

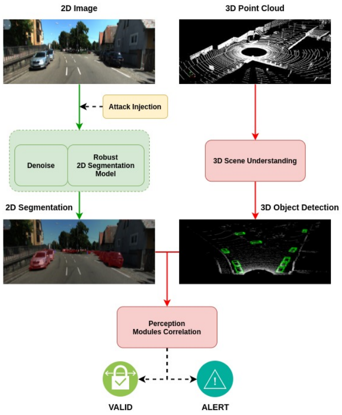
VALID

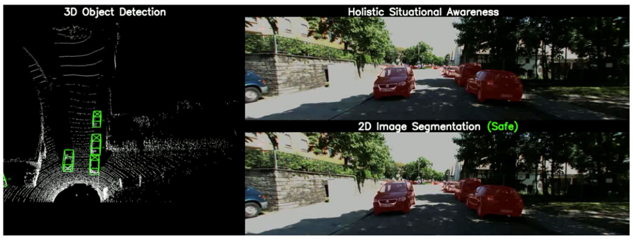
ATHENA Research & Innovation Information Technologies

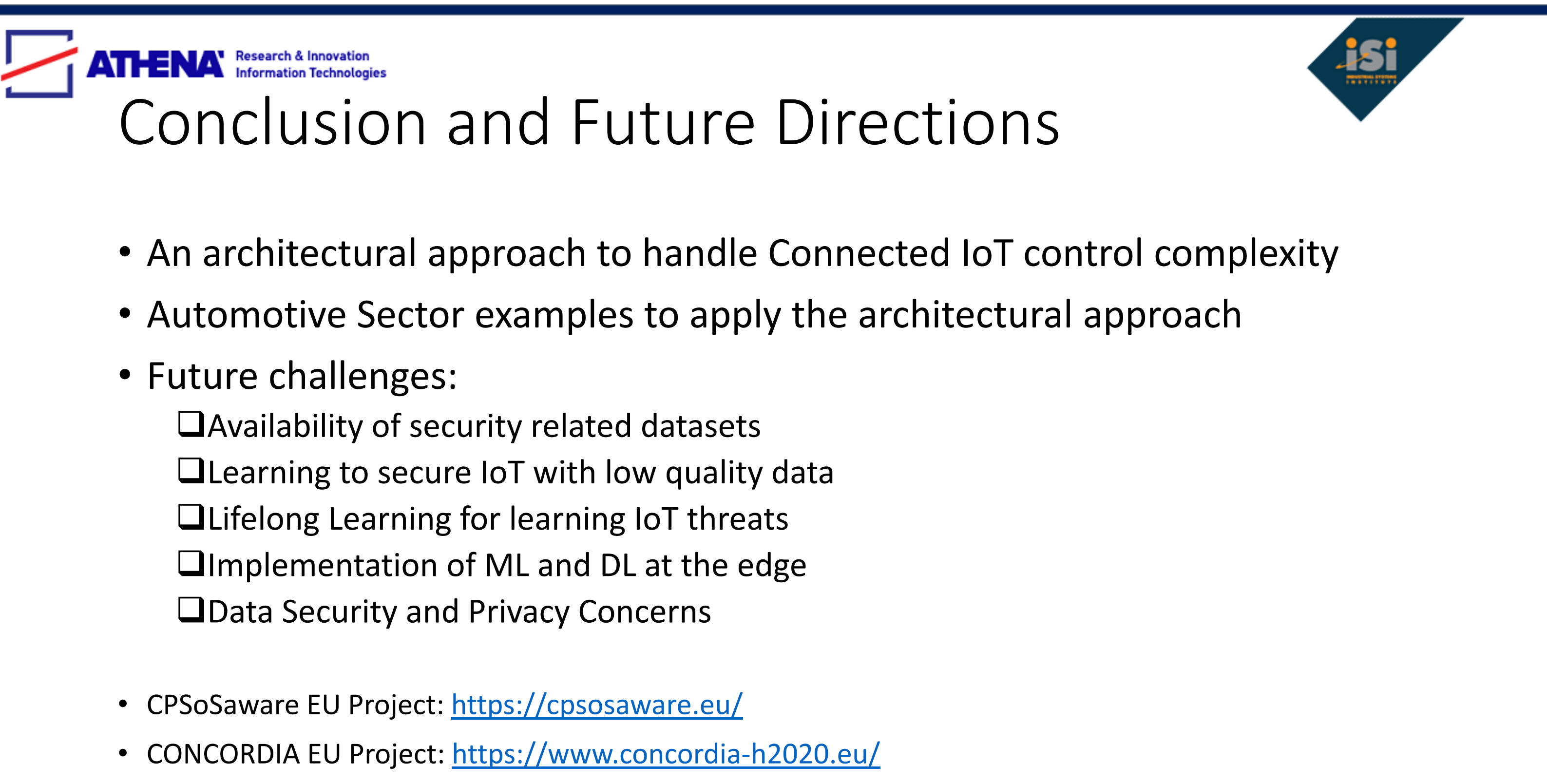
DNN robust to advrsarial noise



Improved Situational Awareness



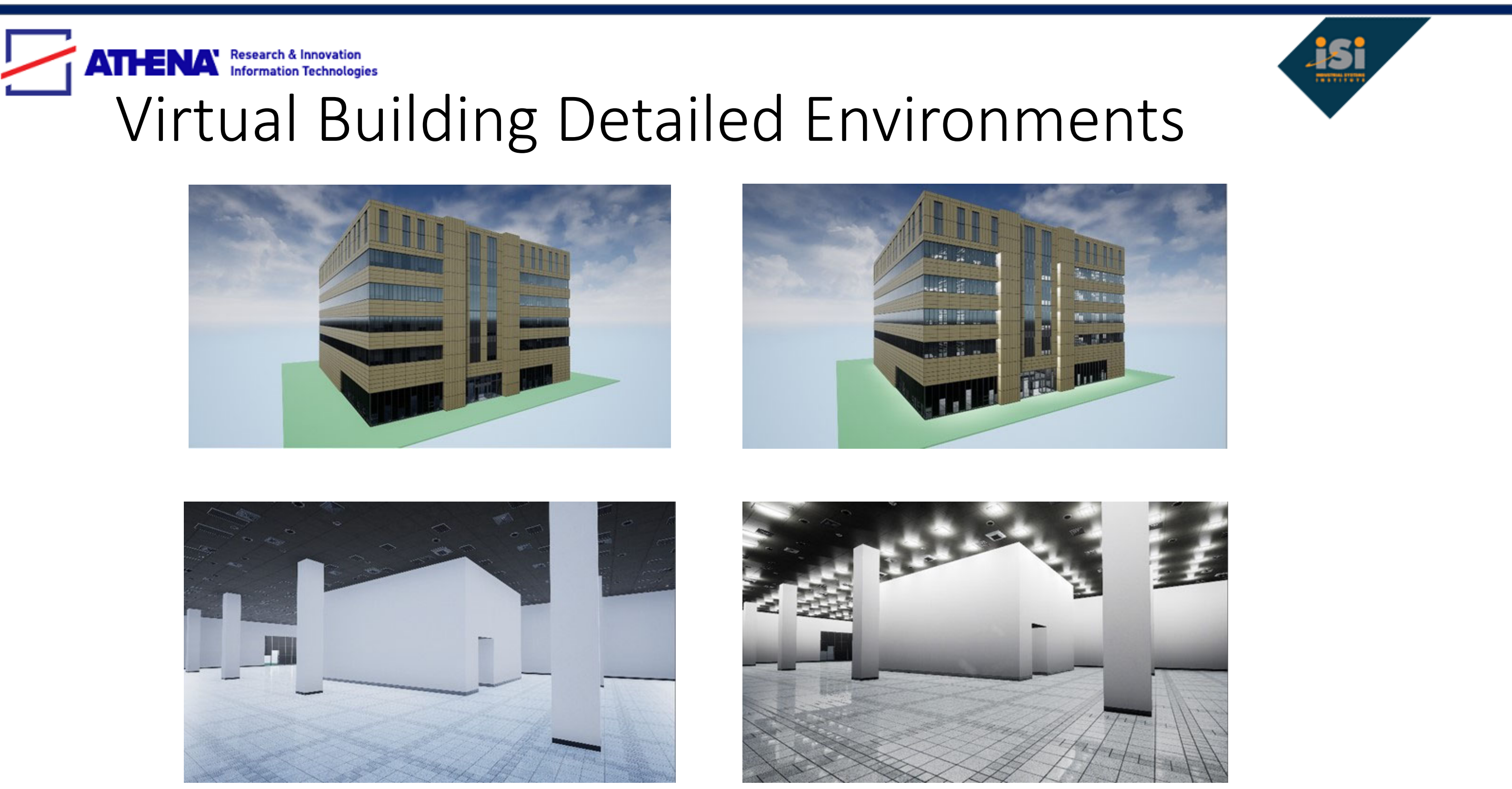




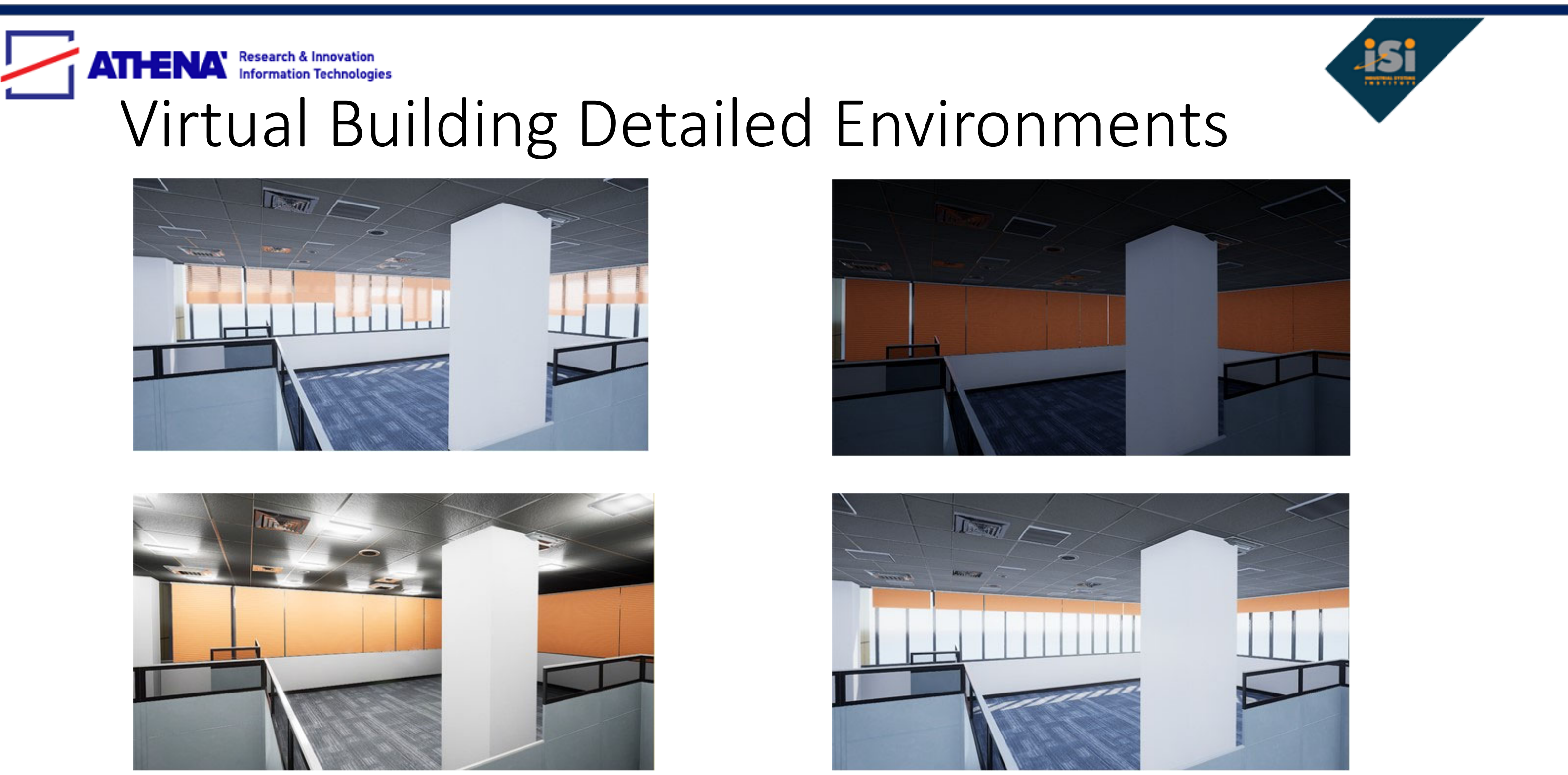
Conclusion and Future Directions

- An architectural approach to handle Connected IoT control complexity
- Automotive Sector examples to apply the architectural approach
- Future challenges:
  - ❑Availability of security related datasets
  - ❑Learning to secure IoT with low quality data
  - ❑Lifelong Learning for learning IoT threats
  - ❑Implementation of ML and DL at the edge
  - ❑Data Security and Privacy Concerns

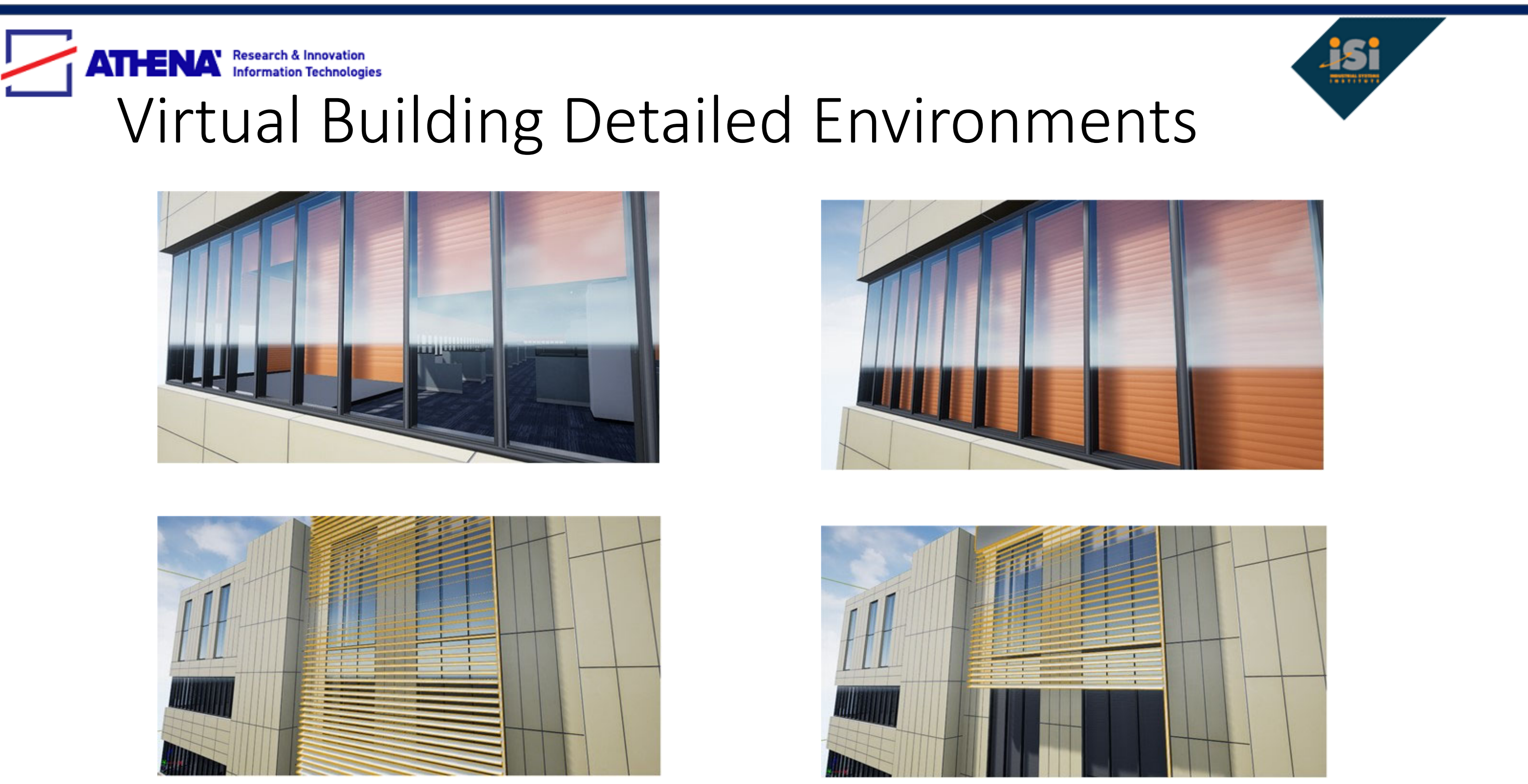
- CPSoSaware EU Project: https://cpsosaware.eu/
- CONCORDIA EU Project: https://www.concordia-h2020.eu/



Virtual Building Detailed Environments

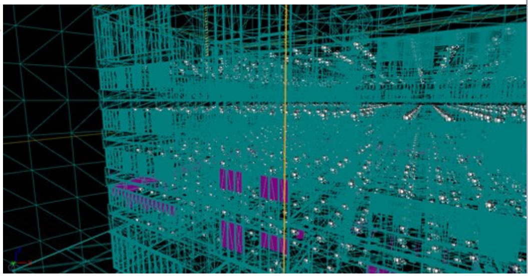


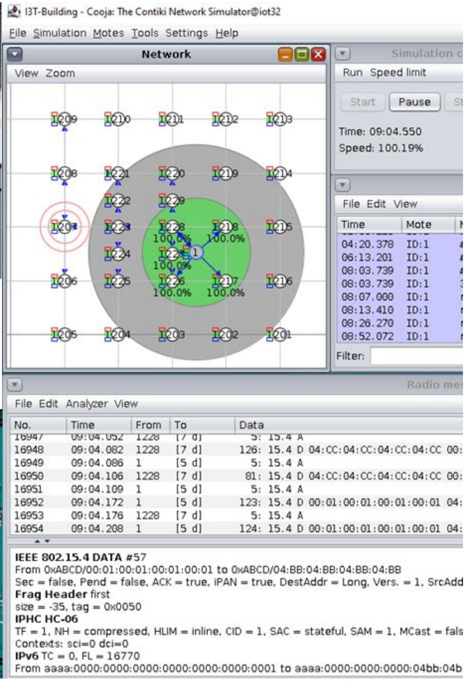
Virtual Building Detailed Environments



Virtual Building Detailed Environments

Distributed Simulation



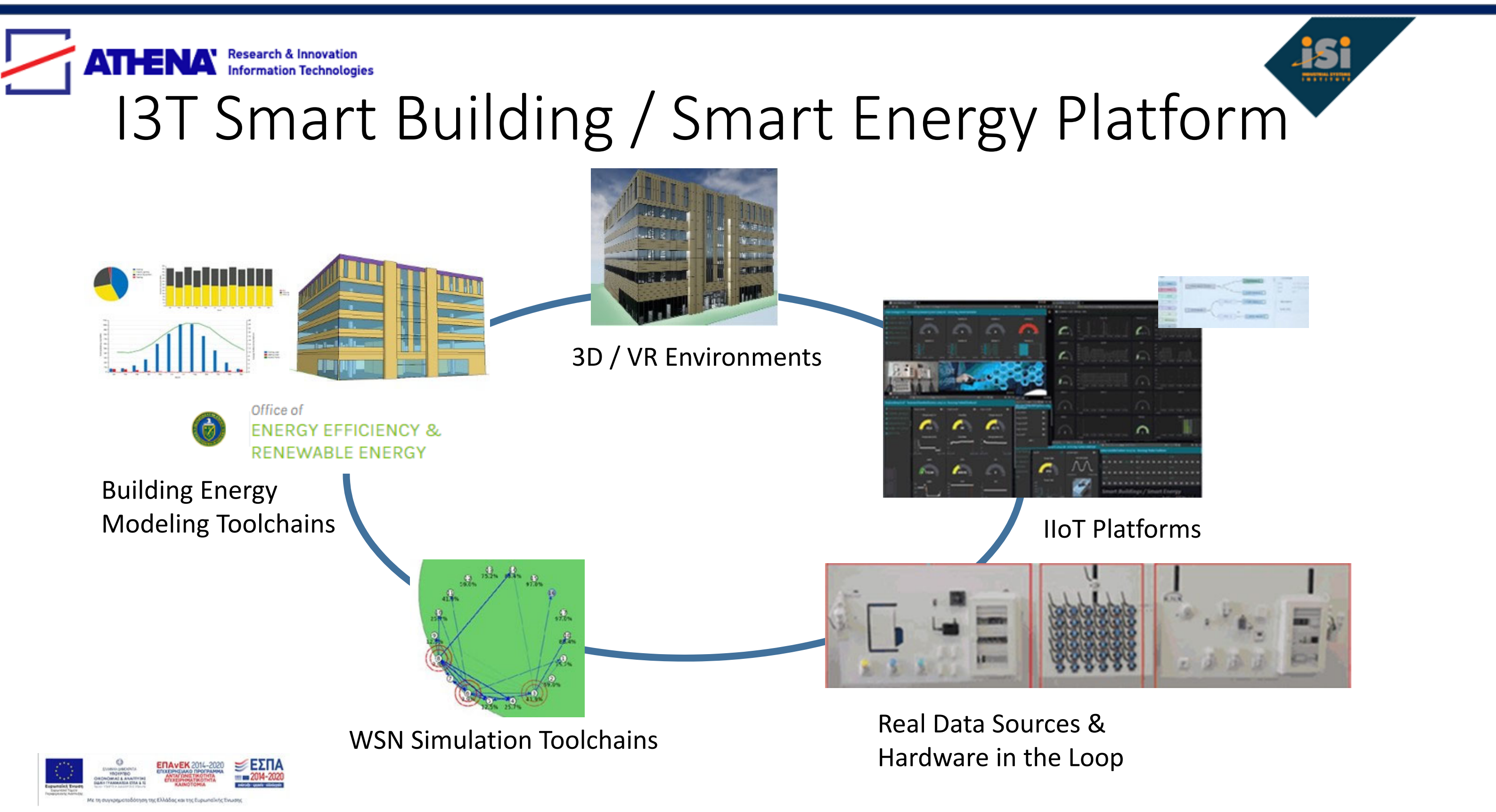


Time: 09:04.550
Speed: 100.19%

```
Time       Mote
04:20.378  ID:1
06:13.201  ID:1
08:03.739  ID:1
08:03.739  ID:1
08:07.000  ID:1
08:13.410  ID:1
08:26.270  ID:1
08:52.072  ID:1
```

```
No.    Time       From  To     Data
16947  09:04.052  1228  [7 d]    5: 15.4 A
16948  09:04.082  1228  [7 d]  126: 15.4 D 04:CC:04:CC:04:CC:04:CC 00:
16949  09:04.086  1     [5 d]    5: 15.4 A
16950  09:04.106  1228  [7 d]   81: 15.4 D 04:CC:04:CC:04:CC:04:CC 00:
16951  09:04.109  1     [5 d]    5: 15.4 A
16952  09:04.172  1     [5 d]  123: 15.4 D 00:01:00:01:00:01:00:01 04:
16953  09:04.176  1228  [7 d]    5: 15.4 A
16954  09:04.208  1     [5 d]  124: 15.4 D 00:01:00:01:00:01:00:01 04:
```

```
IEEE 802.15.4 DATA #57
From 0xABCD/00:01:00:01:00:01:00:01 to 0xABCD/04:BB:04:BB:04:BB:04:BB
Sec = false, Pend = false, ACK = true, iPAN = true, DestAddr = Long, Vers. = 1, SrcAdd
Frag Header first
size = -35, tag = 0x0050
IPHC HC-06
TF = 1, NH = compressed, HLIM = inline, CID = 1, SAC = stateful, SAM = 1, MCast = fals
Contexts: sci=0 dci=0
IPv6 TC = 0, FL = 16770
From aaaa:0000:0000:0000:0000:0000:0000:0001 to aaaa:0000:0000:0000:04bb:04b
```



ATHENA Research & Innovation Information Technologies

I3T Smart Building / Smart Energy Platform

3D / VR Environments

IIoT Platforms

Real Data Sources &
Hardware in the Loop

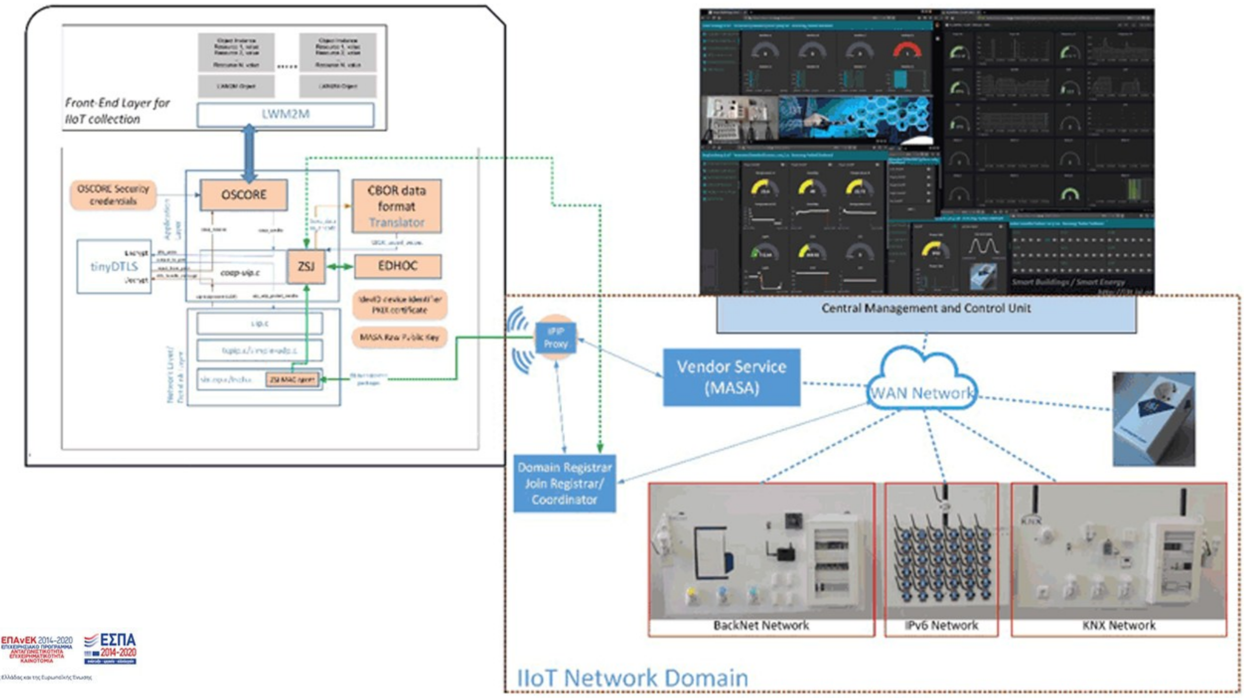
WSN Simulation Toolchains

Building Energy
Modeling Toolchains

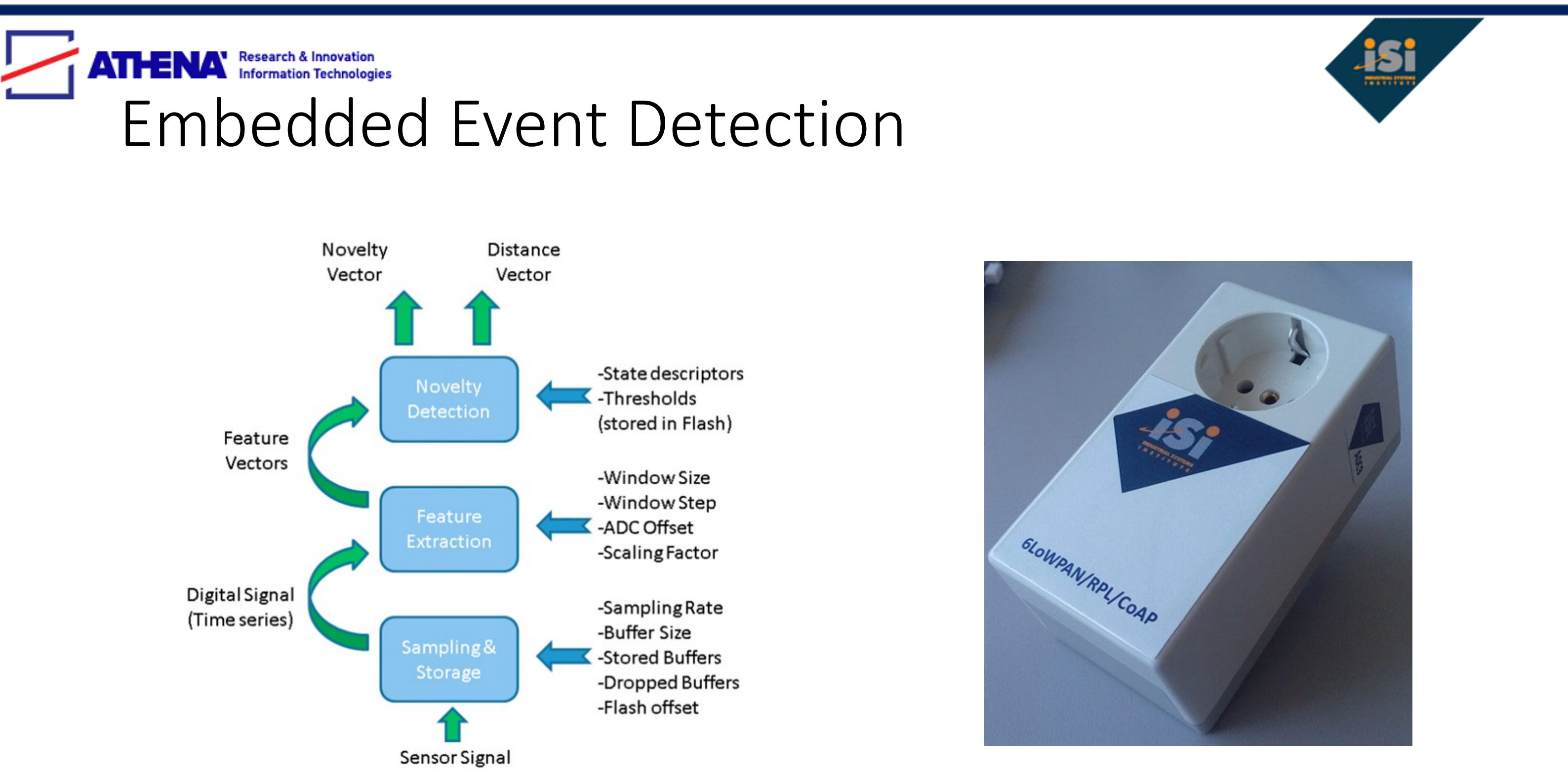
Office of
ENERGY EFFICIENCY &
RENEWABLE ENERGY

ATHENA Research & Innovation Information Technologies

I3T Smart Building / Smart Energy Platform


Front-End Layer for IIoT collection
LWM2M
OSCORE Security credentials
OSCORE
CBOR data format Translator
tinyDTLS
Encrypt
Decrypt
coap-uip.c
ZSJ
EDHOC
IdevID device identifier PKIX certificate
MASA Raw Public Key
uip.c
ZSJ MAC agent
Application Layer
Network Layer/ Data-link Layer
Central Management and Control Unit
Smart Buildings / Smart Energy
IPIP Proxy
Vendor Service (MASA)
WAN Network
Domain Registrar Join Registrar/ Coordinator
BackNet Network
IPv6 Network
KNX Network
IIoT Network Domain

ΕΠΑνΕΚ 2014-2020 ΕΣΠΑ 2014-2020

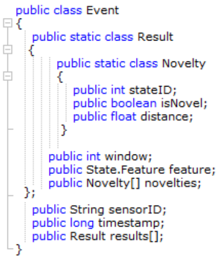


ATHENA Research & Innovation Information Technologies

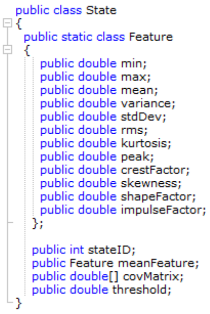
Embedded Event Detection

ATHENA Research & Innovation Information Technologies

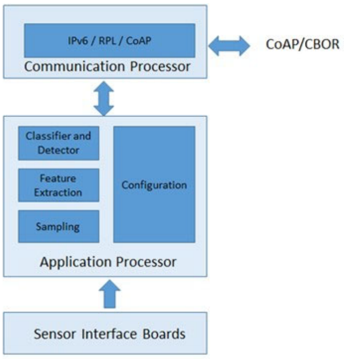
Different Realizations

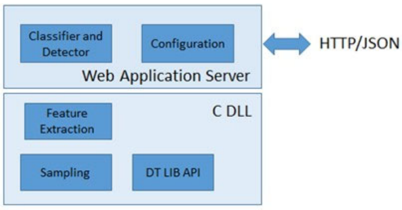


```
public class Event
{
    public static class Result
    {
        public static class Novelty
        {
            public int stateID;
            public boolean isNovel;
            public float distance;
        }

        public int window;
        public State.Feature feature;
        public Novelty[] novelties;
    };
    public String sensorID;
    public long timestamp;
    public Result results[];
}
```

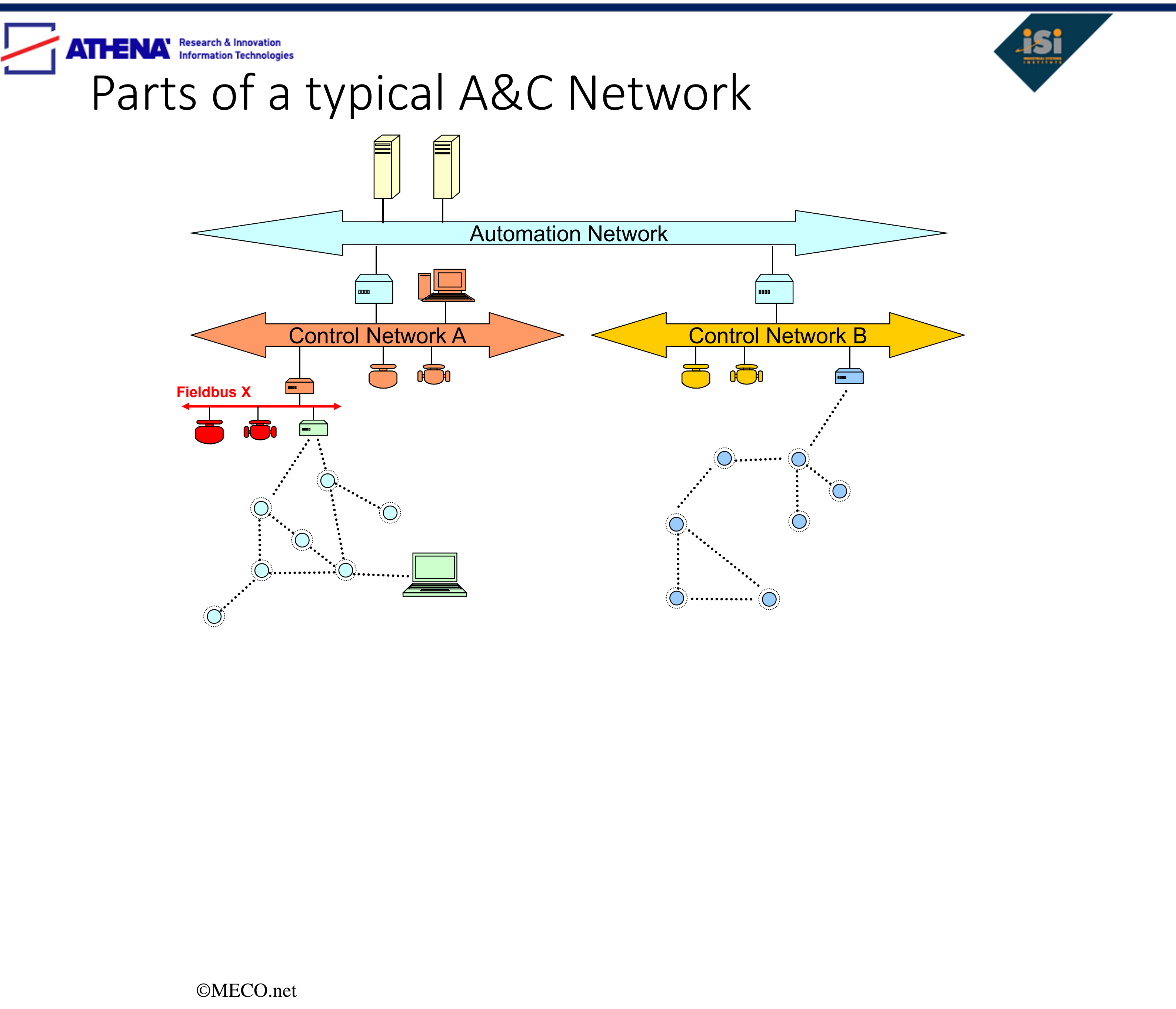


```
public class State
{
    public static class Feature
    {
        public double min;
        public double max;
        public double mean;
        public double variance;
        public double stdDev;
        public double rms;
        public double kurtosis;
        public double peak;
        public double crestFactor;
        public double skewness;
        public double shapeFactor;
        public double impulseFactor;
    };

    public int stateID;
    public Feature meanFeature;
    public double[] covMatrix;
    public double threshold;
}
```

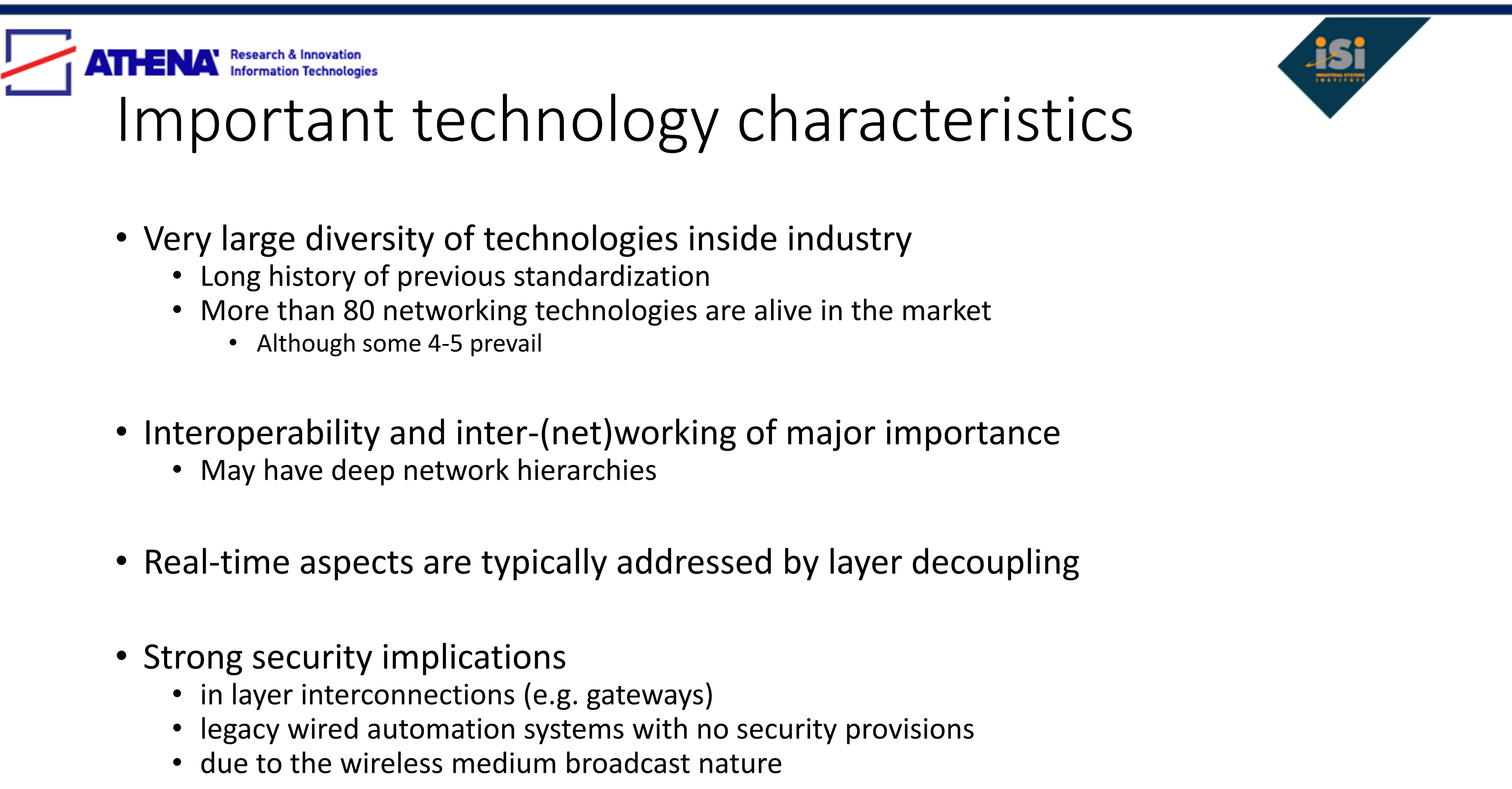




©MECO.net



Parts of a typical A&C Network



ATHENA Research & Innovation Information Technologies

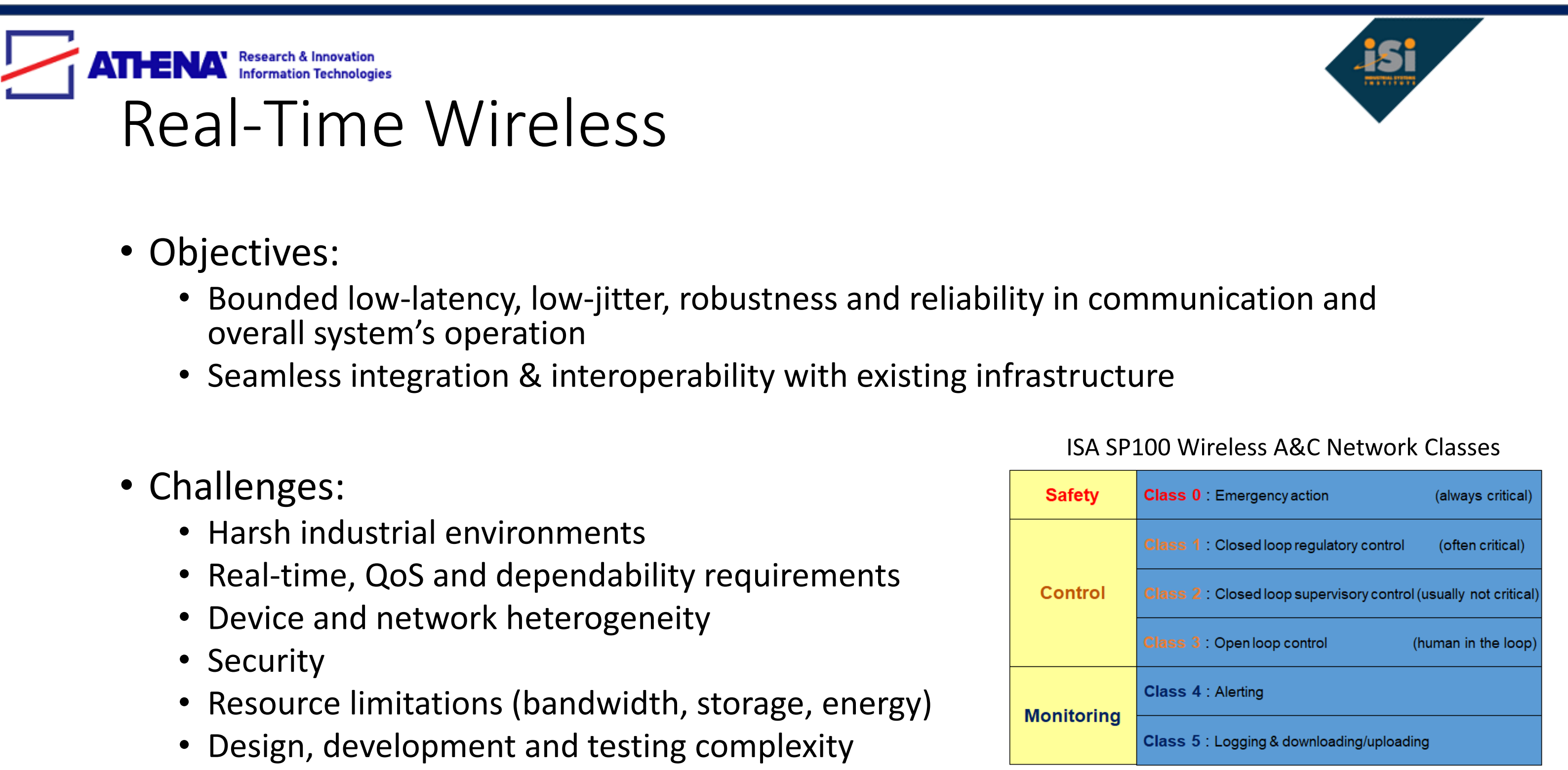
Important technology characteristics

- Very large diversity of technologies inside industry
  - Long history of previous standardization
  - More than 80 networking technologies are alive in the market
    - Although some 4-5 prevail

- Interoperability and inter-(net)working of major importance
  - May have deep network hierarchies

- Real-time aspects are typically addressed by layer decoupling

- Strong security implications
  - in layer interconnections (e.g. gateways)
  - legacy wired automation systems with no security provisions
  - due to the wireless medium broadcast nature



ATHENA Research & Innovation Information Technologies

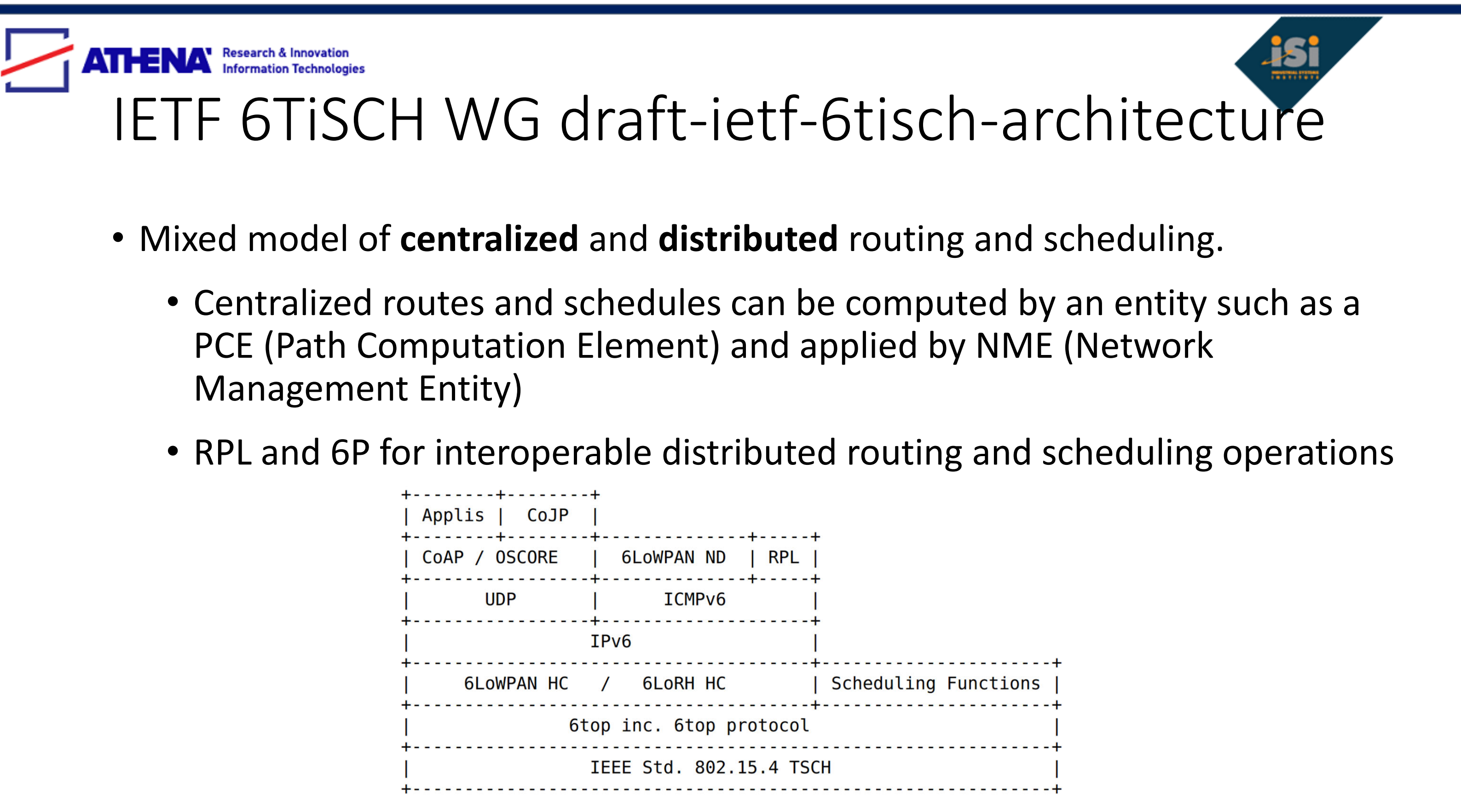
Real-Time Wireless

- Objectives:
  - Bounded low-latency, low-jitter, robustness and reliability in communication and overall system's operation
  - Seamless integration & interoperability with existing infrastructure
- Challenges:
  - Harsh industrial environments
  - Real-time, QoS and dependability requirements
  - Device and network heterogeneity
  - Security
  - Resource limitations (bandwidth, storage, energy)
  - Design, development and testing complexity

ISA SP100 Wireless A&C Network Classes

Safety	Class 0 : Emergency action (always critical)
Control	Class 1 : Closed loop regulatory control (often critical)
	Class 2 : Closed loop supervisory control (usually not critical)
	Class 3 : Open loop control (human in the loop)
Monitoring	Class 4 : Alerting
	Class 5 : Logging & downloading/uploading

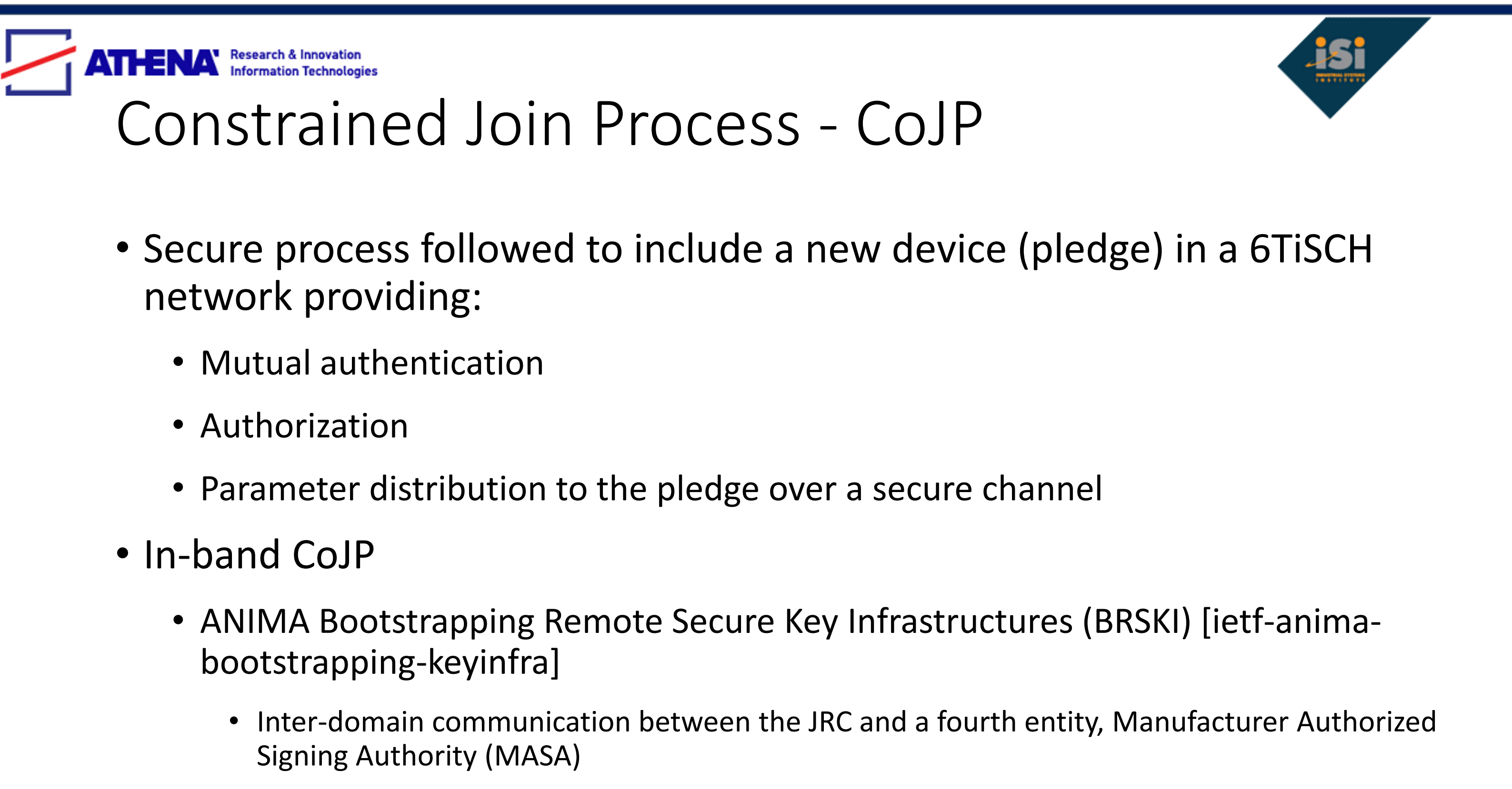
©MECO.net



IETF 6TiSCH WG draft-ietf-6tisch-architecture

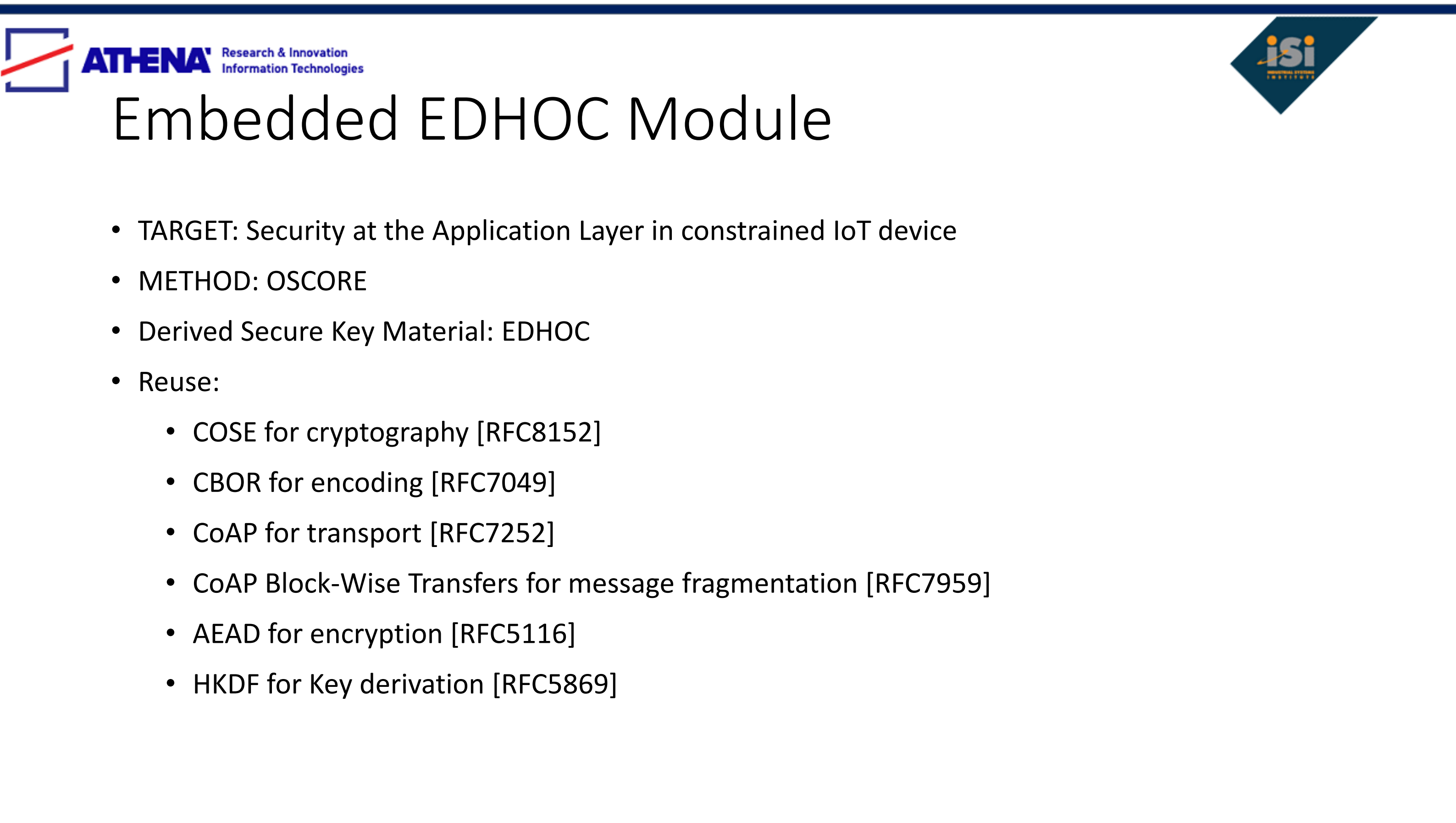
- Mixed model of **centralized** and **distributed** routing and scheduling.
  - Centralized routes and schedules can be computed by an entity such as a PCE (Path Computation Element) and applied by NME (Network Management Entity)
  - RPL and 6P for interoperable distributed routing and scheduling operations

```
+--------+--------+
| Applis |  CoJP  |
+--------+--------+-------------+-----+
| CoAP / OSCORE   |  6LoWPAN ND | RPL |
+-----------------+-------------+-----+
|       UDP       |       ICMPv6      |
+-----------------+-------------------+
|                IPv6                 |
+-------------------------------------+----------------------+
|     6LoWPAN HC  /   6LoRH HC        | Scheduling Functions |
+-------------------------------------+----------------------+
|              6top inc. 6top protocol                       |
+------------------------------------------------------------+
|                IEEE Std. 802.15.4 TSCH                     |
+------------------------------------------------------------+
```



Constrained Join Process - CoJP

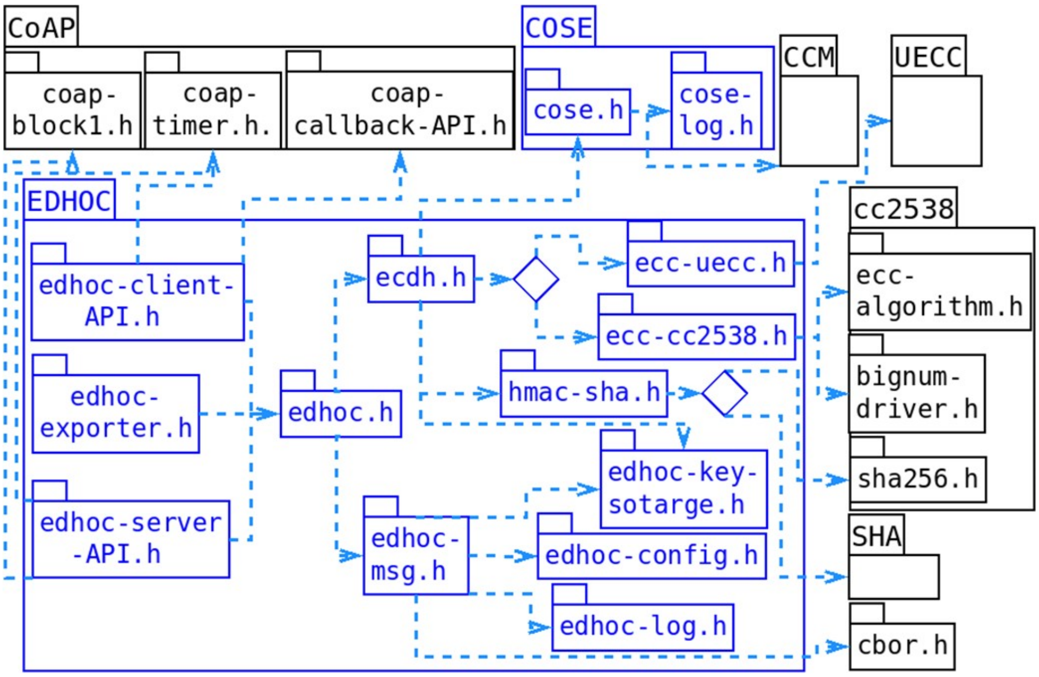
- Secure process followed to include a new device (pledge) in a 6TiSCH network providing:
  - Mutual authentication
  - Authorization
  - Parameter distribution to the pledge over a secure channel
- In-band CoJP
  - ANIMA Bootstrapping Remote Secure Key Infrastructures (BRSKI) [ietf-anima-bootstrapping-keyinfra]
    - Inter-domain communication between the JRC and a fourth entity, Manufacturer Authorized Signing Authority (MASA)



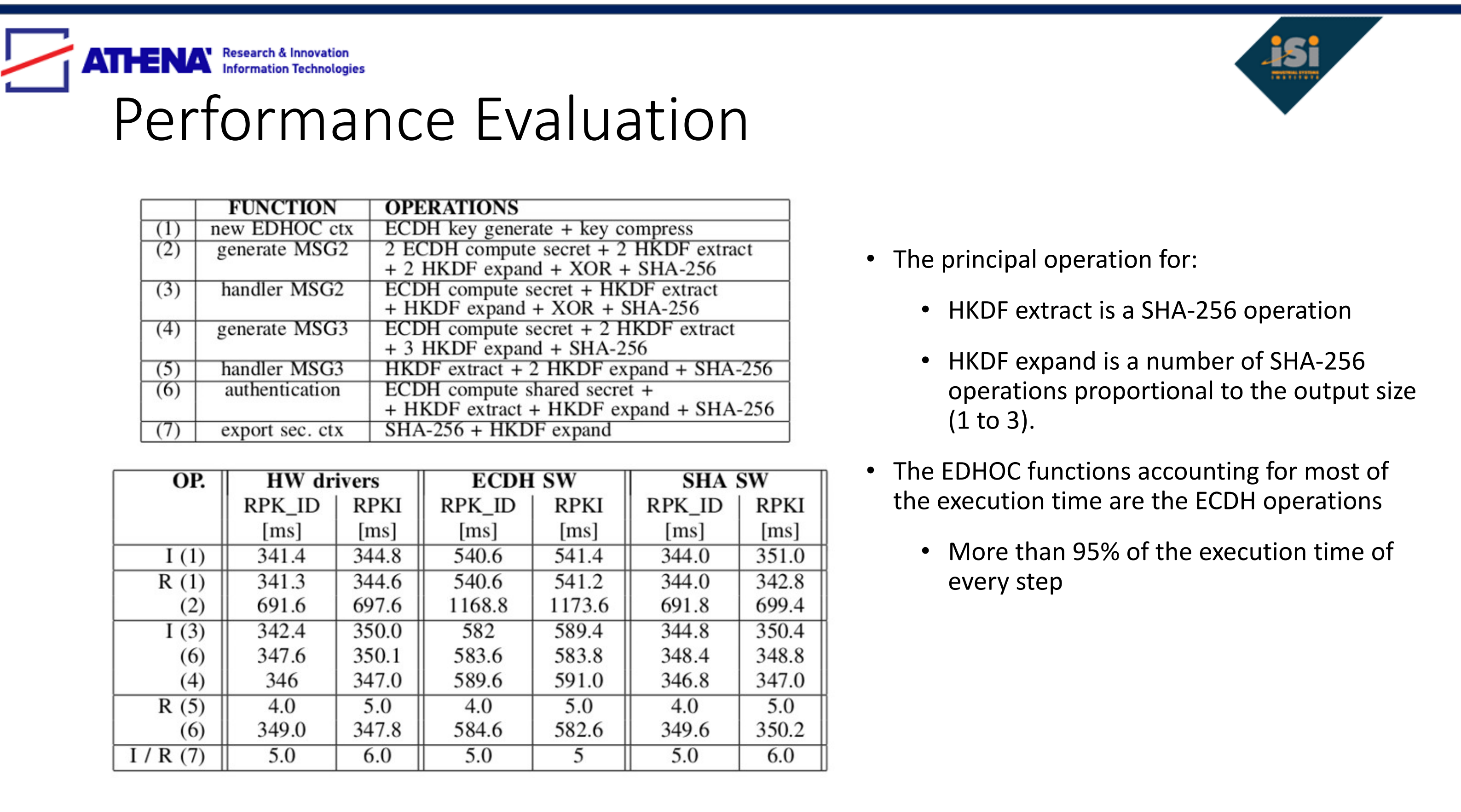
Embedded EDHOC Module

- TARGET: Security at the Application Layer in constrained IoT device
- METHOD: OSCORE
- Derived Secure Key Material: EDHOC
- Reuse:
  - COSE for cryptography [RFC8152]
  - CBOR for encoding [RFC7049]
  - CoAP for transport [RFC7252]
  - CoAP Block-Wise Transfers for message fragmentation [RFC7959]
  - AEAD for encryption [RFC5116]
  - HKDF for Key derivation [RFC5869]

Embedded EDHOC Module



CoAP
coap-block1.h
coap-timer.h.
coap-callback-API.h
COSE
cose.h
cose-log.h
CCM
UECC
EDHOC
edhoc-client-API.h
edhoc-exporter.h
edhoc-server-API.h
edhoc.h
ecdh.h
hmac-sha.h
ecc-uecc.h
ecc-cc2538.h
edhoc-key-sotarge.h
edhoc-msg.h
edhoc-config.h
edhoc-log.h
cc2538
ecc-algorithm.h
bignum-driver.h
sha256.h
SHA
cbor.h



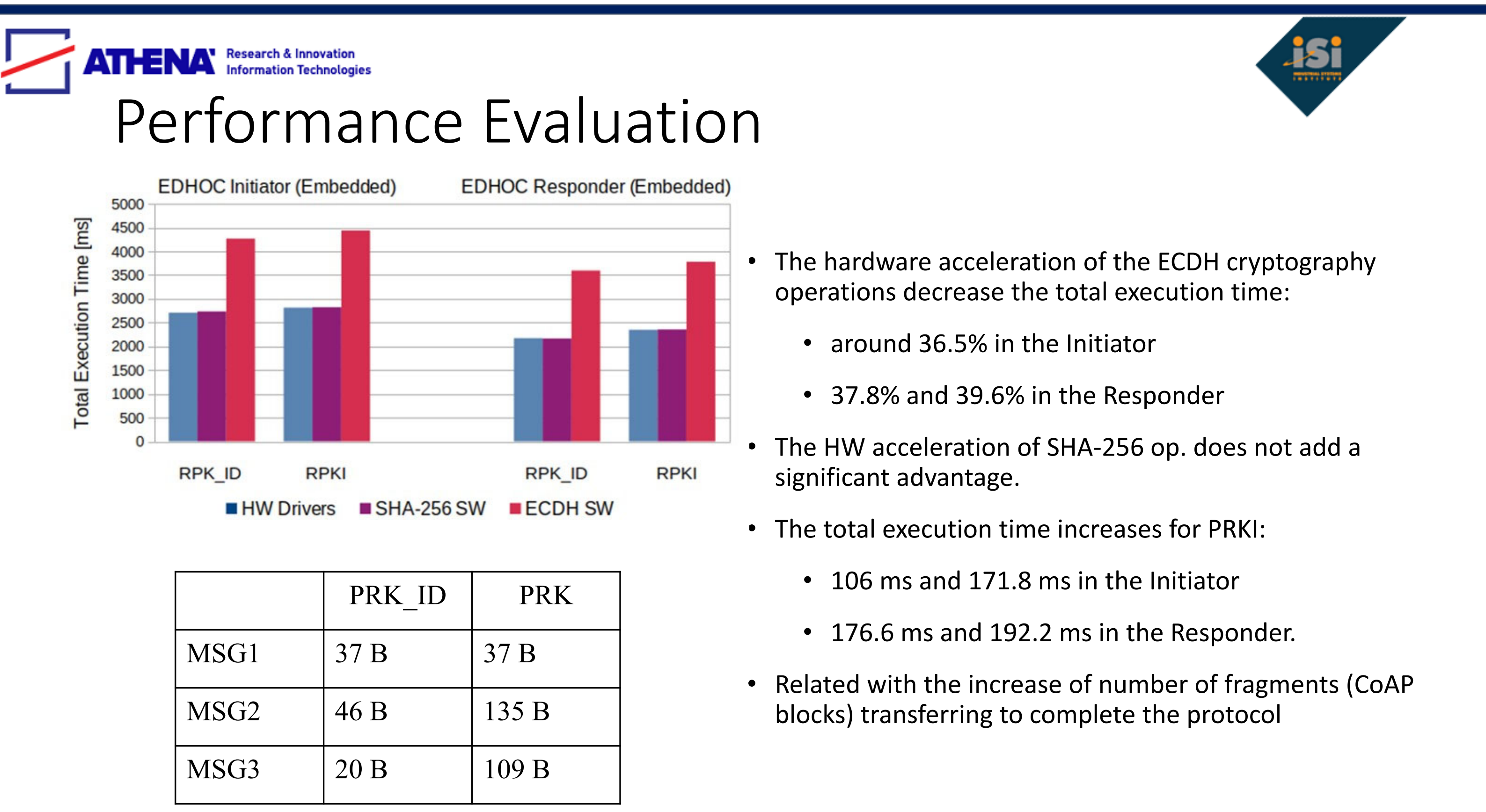
ATHENA Research & Innovation Information Technologies

Performance Evaluation

	FUNCTION	OPERATIONS
(1)	new EDHOC ctx	ECDH key generate + key compress
(2)	generate MSG2	2 ECDH compute secret + 2 HKDF extract + 2 HKDF expand + XOR + SHA-256
(3)	handler MSG2	ECDH compute secret + HKDF extract + HKDF expand + XOR + SHA-256
(4)	generate MSG3	ECDH compute secret + 2 HKDF extract + 3 HKDF expand + SHA-256
(5)	handler MSG3	HKDF extract + 2 HKDF expand + SHA-256
(6)	authentication	ECDH compute shared secret + + HKDF extract + HKDF expand + SHA-256
(7)	export sec. ctx	SHA-256 + HKDF expand

OP.	HW drivers		ECDH SW		SHA SW	
	RPK_ID [ms]	RPKI [ms]	RPK_ID [ms]	RPKI [ms]	RPK_ID [ms]	RPKI [ms]
I (1)	341.4	344.8	540.6	541.4	344.0	351.0
R (1)	341.3	344.6	540.6	541.2	344.0	342.8
(2)	691.6	697.6	1168.8	1173.6	691.8	699.4
I (3)	342.4	350.0	582	589.4	344.8	350.4
(6)	347.6	350.1	583.6	583.8	348.4	348.8
(4)	346	347.0	589.6	591.0	346.8	347.0
R (5)	4.0	5.0	4.0	5.0	4.0	5.0
(6)	349.0	347.8	584.6	582.6	349.6	350.2
I / R (7)	5.0	6.0	5.0	5	5.0	6.0

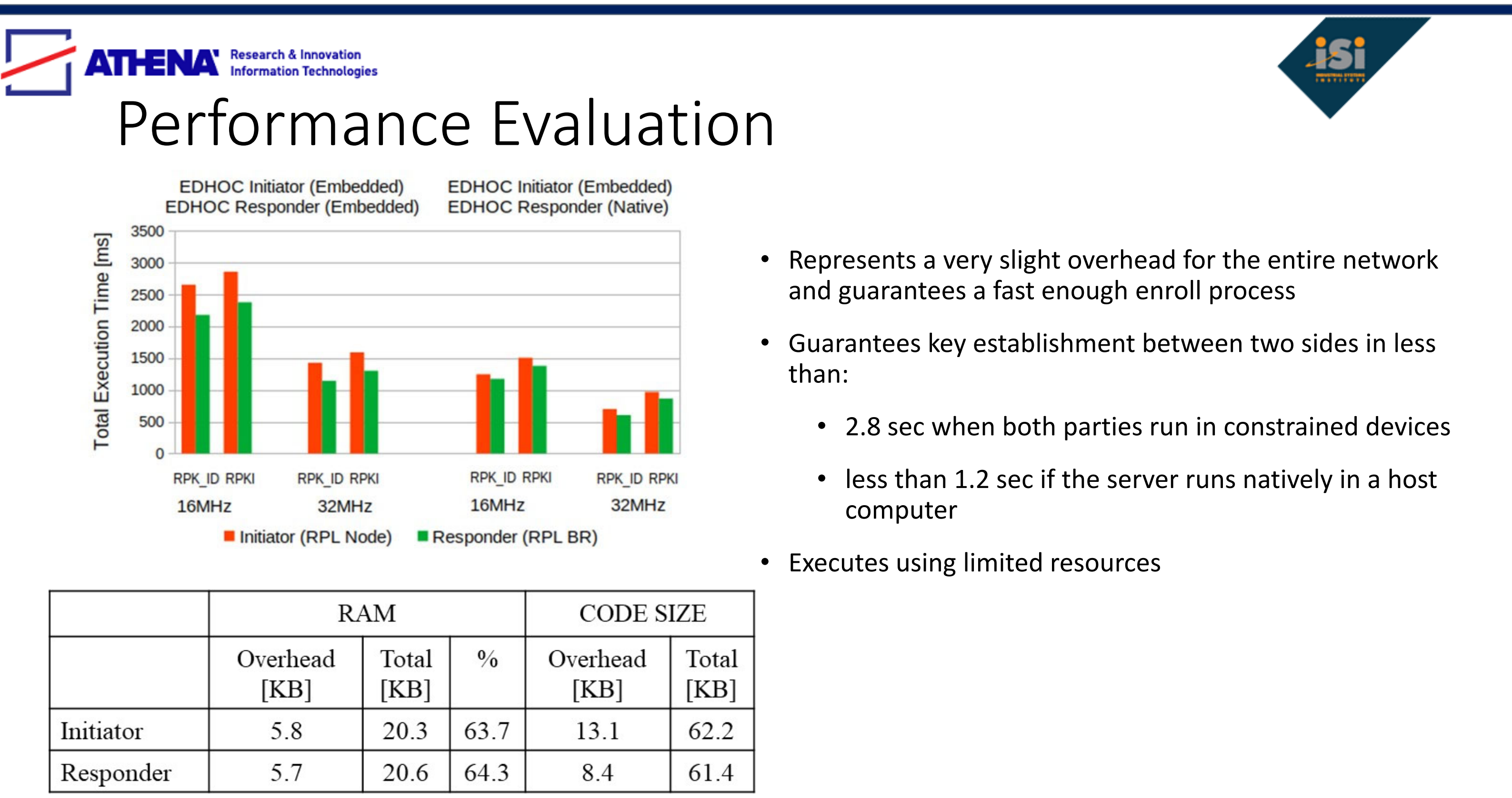
- The principal operation for:
  - HKDF extract is a SHA-256 operation
  - HKDF expand is a number of SHA-256 operations proportional to the output size (1 to 3).
- The EDHOC functions accounting for most of the execution time are the ECDH operations
  - More than 95% of the execution time of every step


ATHENA Research & Innovation Information Technologies
isi
EDHOC Initiator (Embedded)
EDHOC Responder (Embedded)
Total Execution Time [ms]
5000
4500
4000
3500
3000
2500
2000
1500
1000
500
0
RPK_ID
RPKI
RPK_ID
RPKI
HW Drivers
SHA-256 SW
ECDH SW

Performance Evaluation

	PRK_ID	PRK
MSG1	37 B	37 B
MSG2	46 B	135 B
MSG3	20 B	109 B

- The hardware acceleration of the ECDH cryptography operations decrease the total execution time:
  - around 36.5% in the Initiator
  - 37.8% and 39.6% in the Responder
- The HW acceleration of SHA-256 op. does not add a significant advantage.
- The total execution time increases for PRKI:
  - 106 ms and 171.8 ms in the Initiator
  - 176.6 ms and 192.2 ms in the Responder.
- Related with the increase of number of fragments (CoAP blocks) transferring to complete the protocol



ATHENA Research & Innovation Information Technologies

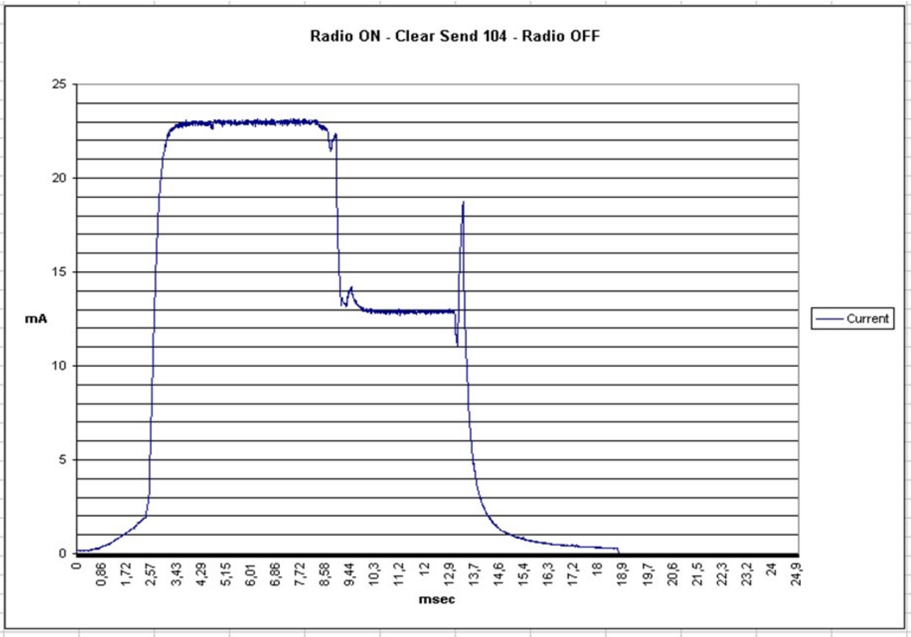
Performance Evaluation

- Represents a very slight overhead for the entire network and guarantees a fast enough enroll process
- Guarantees key establishment between two sides in less than:
  - 2.8 sec when both parties run in constrained devices
  - less than 1.2 sec if the server runs natively in a host computer
- Executes using limited resources

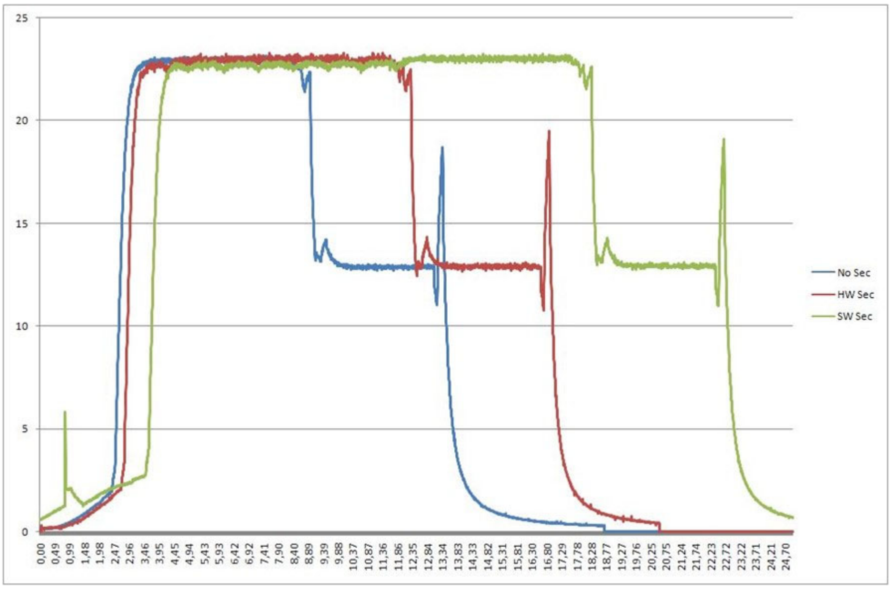
	RAM			CODE SIZE	
	Overhead [KB]	Total [KB]	%	Overhead [KB]	Total [KB]
Initiator	5.8	20.3	63.7	13.1	62.2
Responder	5.7	20.6	64.3	8.4	61.4

ATHENA Research & Innovation Information Technologies

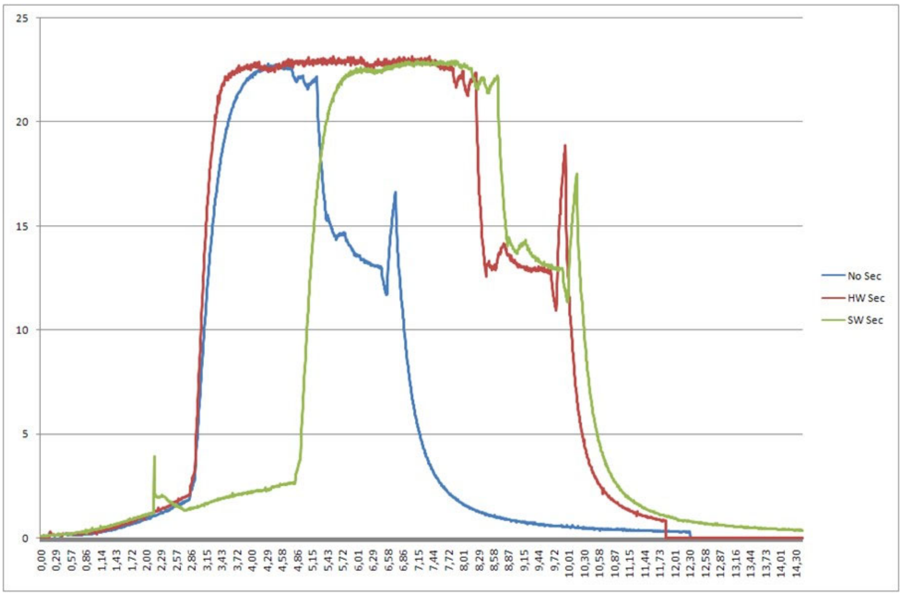
Wireless Frame Transmission

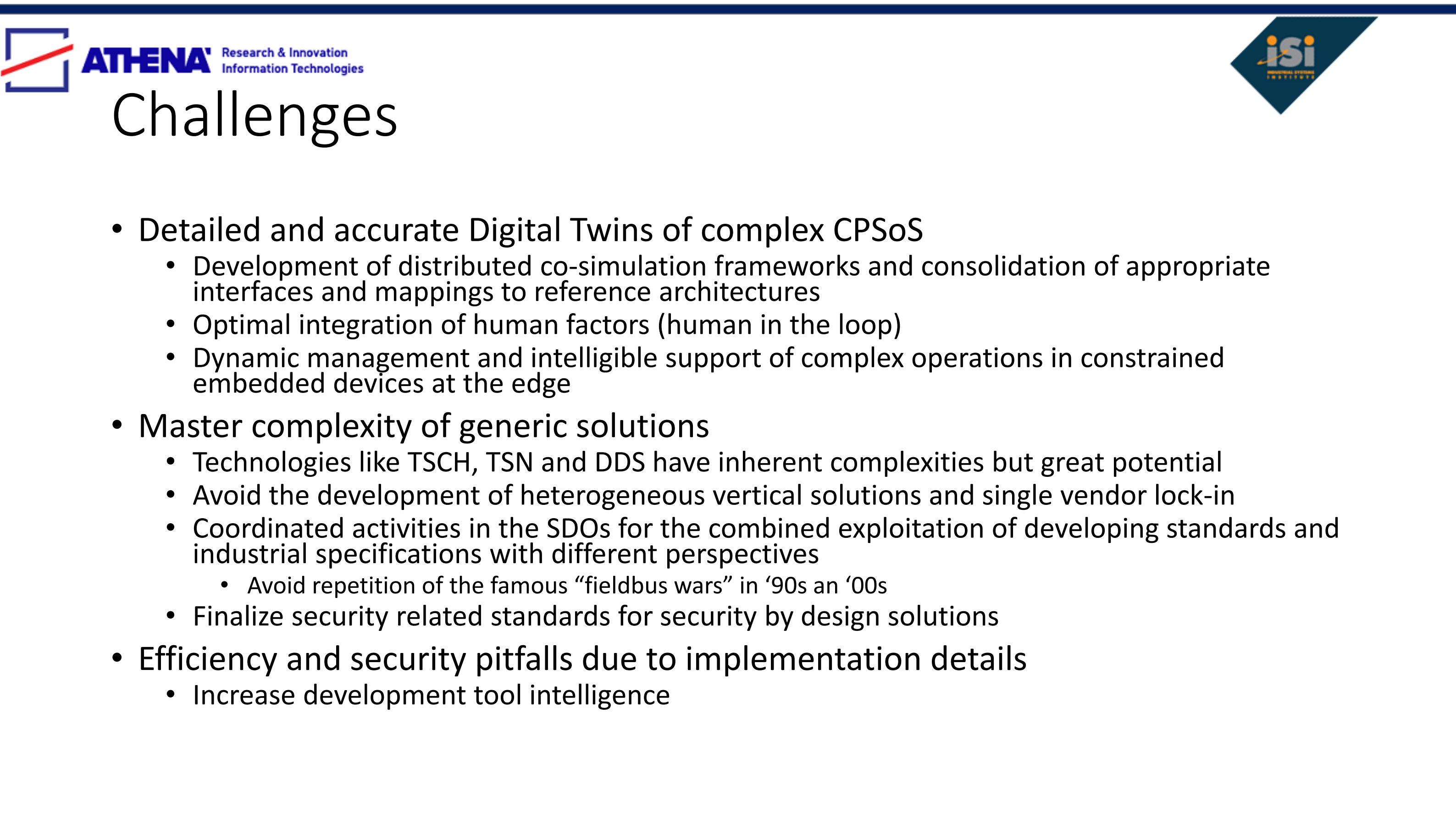


Lower Level Security Costs



Lower Level Security Costs



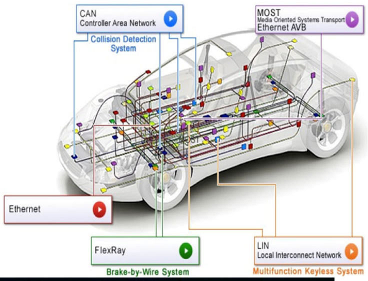


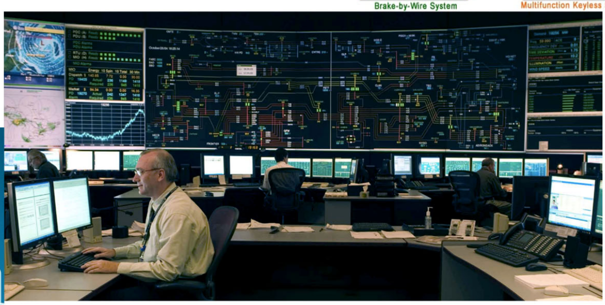
Challenges

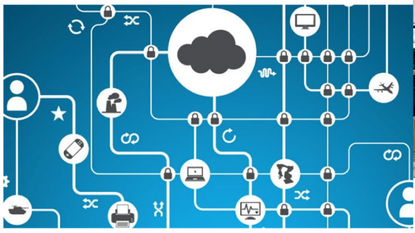
- Detailed and accurate Digital Twins of complex CPSoS
  - Development of distributed co-simulation frameworks and consolidation of appropriate interfaces and mappings to reference architectures
  - Optimal integration of human factors (human in the loop)
  - Dynamic management and intelligible support of complex operations in constrained embedded devices at the edge
- Master complexity of generic solutions
  - Technologies like TSCH, TSN and DDS have inherent complexities but great potential
  - Avoid the development of heterogeneous vertical solutions and single vendor lock-in
  - Coordinated activities in the SDOs for the combined exploitation of developing standards and industrial specifications with different perspectives
    - Avoid repetition of the famous "fieldbus wars" in '90s an '00s
  - Finalize security related standards for security by design solutions
- Efficiency and security pitfalls due to implementation details
  - Increase development tool intelligence

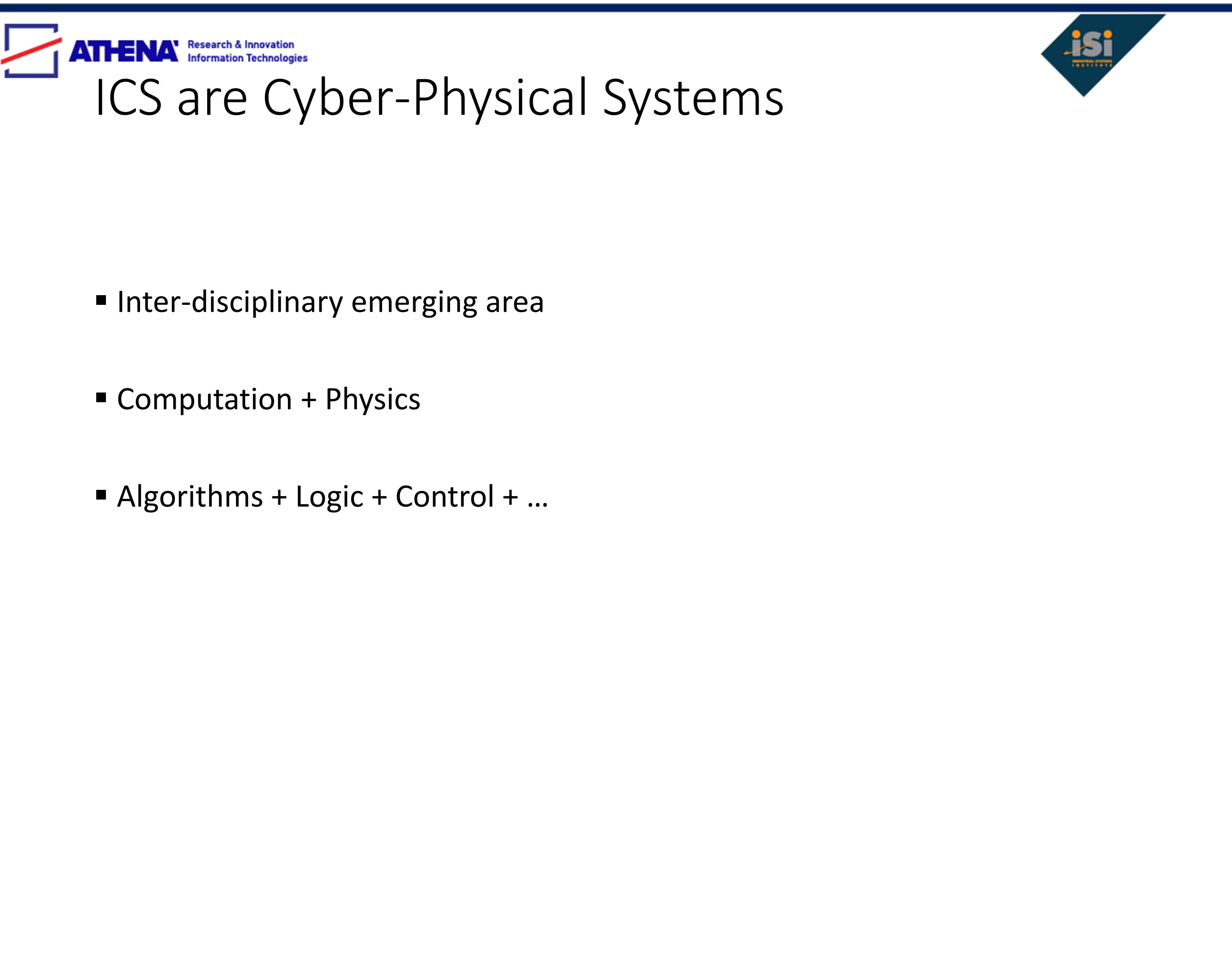
ATHENA Research & Innovation Information Technologies

Industrial Control Systems (ICS)


CAN
Controller Area Network
Collision Detection System
MOST
Media Oriented Systems Transport
Ethernet AVB
Ethernet
FlexRay
Brake-by-Wire System
LIN
Local Interconnect Network
Multifunction Keyless System

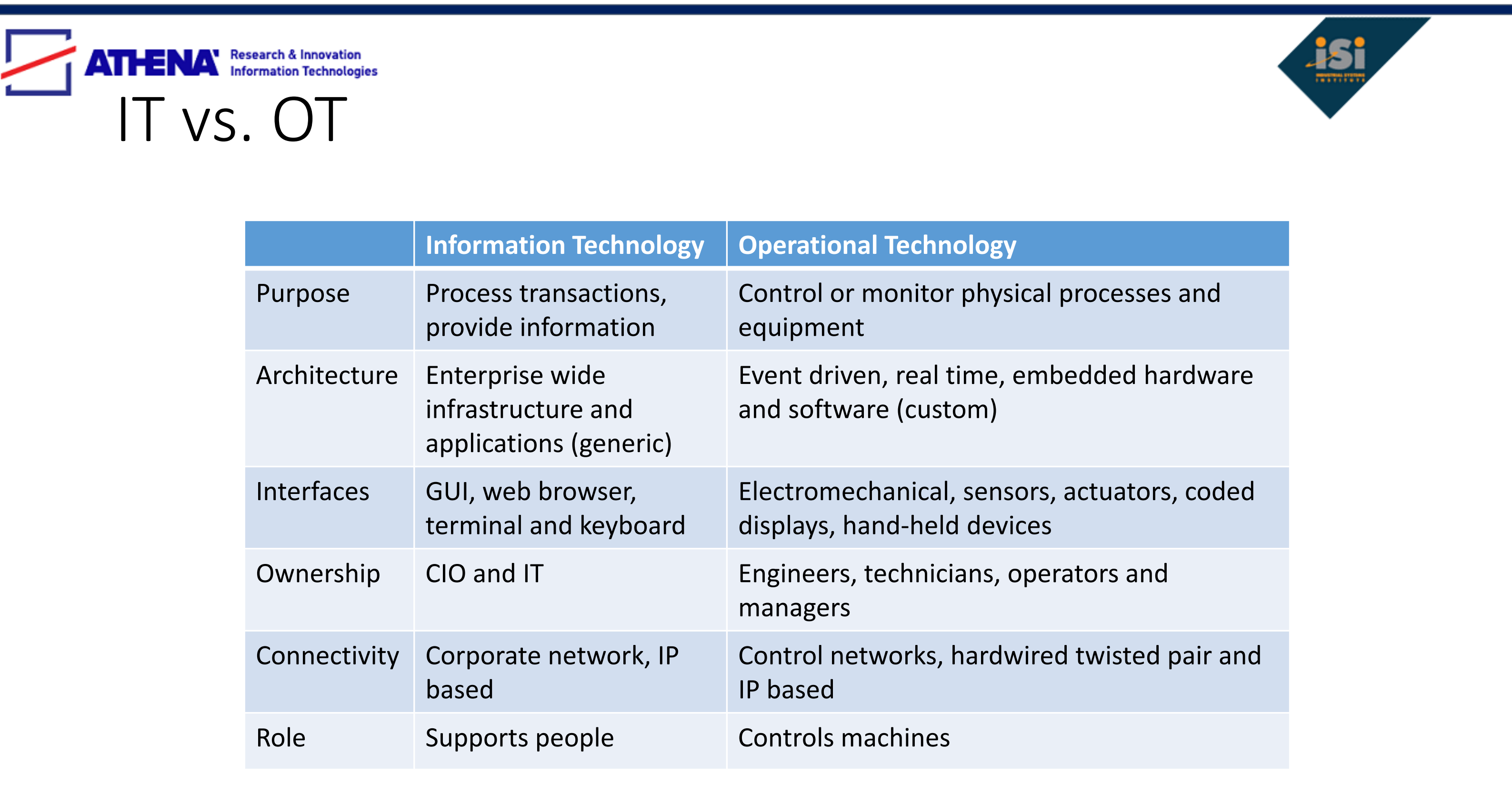






ICS are Cyber-Physical Systems

- Inter-disciplinary emerging area
- Computation + Physics
- Algorithms + Logic + Control + …

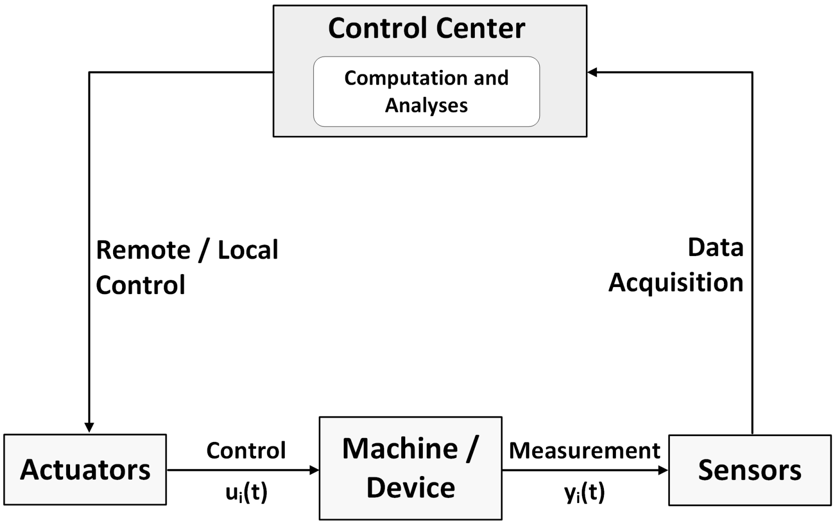


IT vs. OT

	Information Technology	Operational Technology
Purpose	Process transactions, provide information	Control or monitor physical processes and equipment
Architecture	Enterprise wide infrastructure and applications (generic)	Event driven, real time, embedded hardware and software (custom)
Interfaces	GUI, web browser, terminal and keyboard	Electromechanical, sensors, actuators, coded displays, hand-held devices
Ownership	CIO and IT	Engineers, technicians, operators and managers
Connectivity	Corporate network, IP based	Control networks, hardwired twisted pair and IP based
Role	Supports people	Controls machines

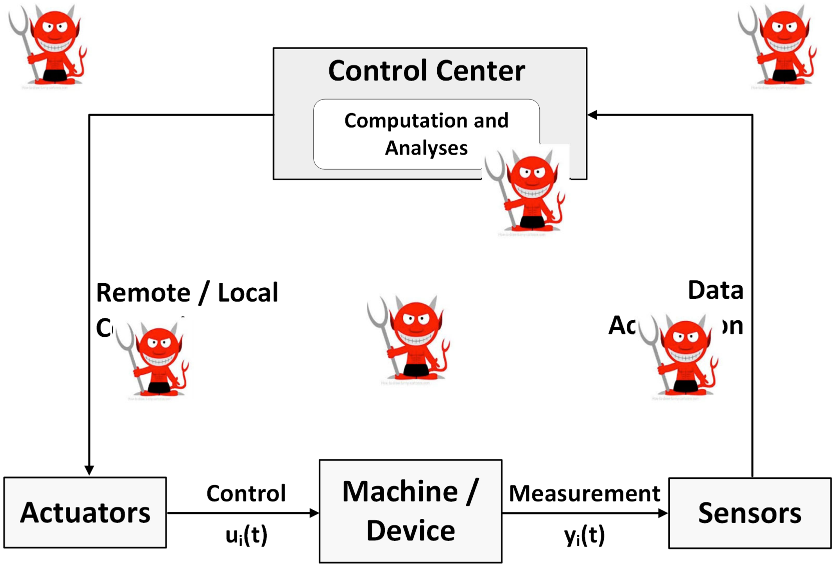
ATHENA Research & Innovation Information Technologies

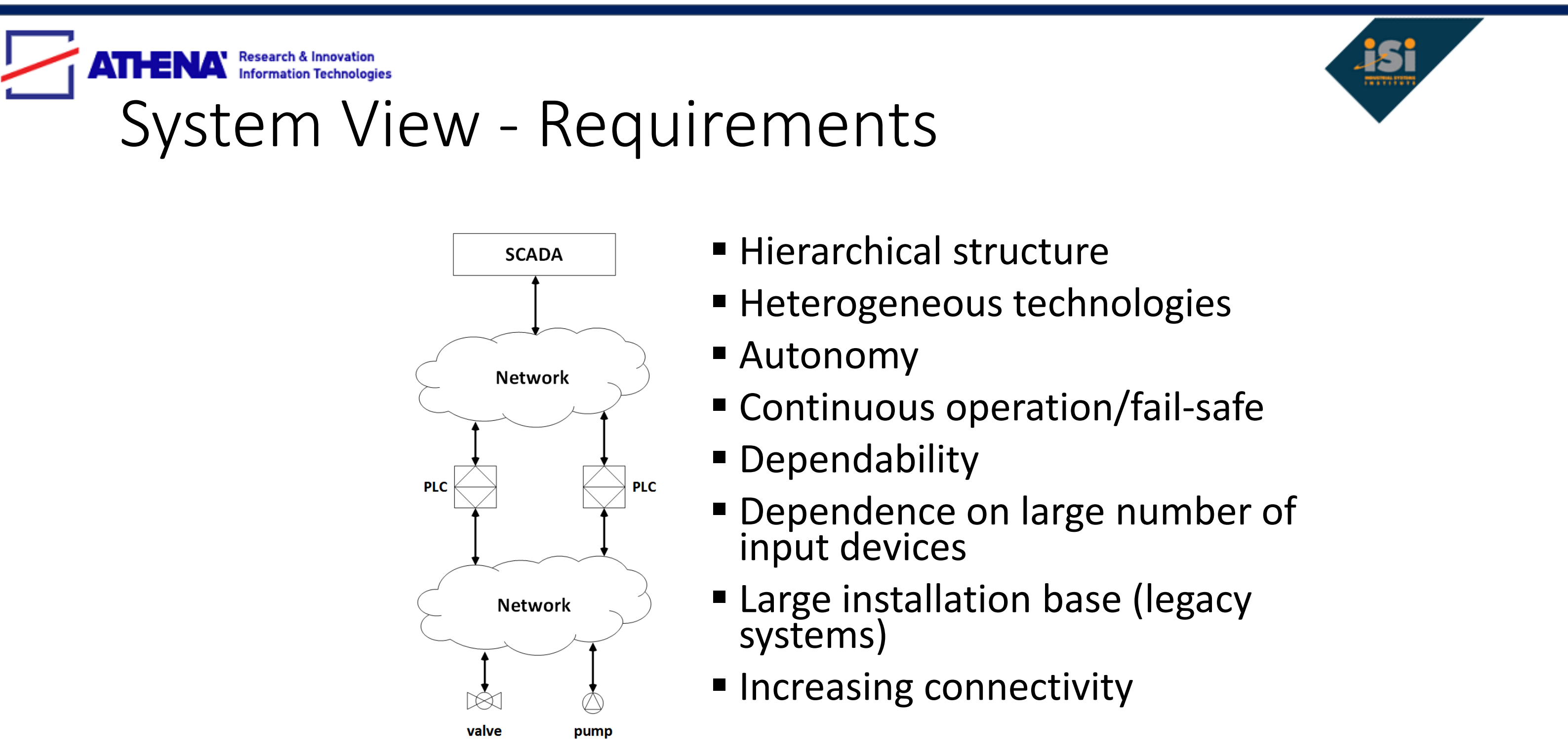
ICS Control Loop



ATHENA Research & Innovation Information Technologies

ICS Control Loop Attack

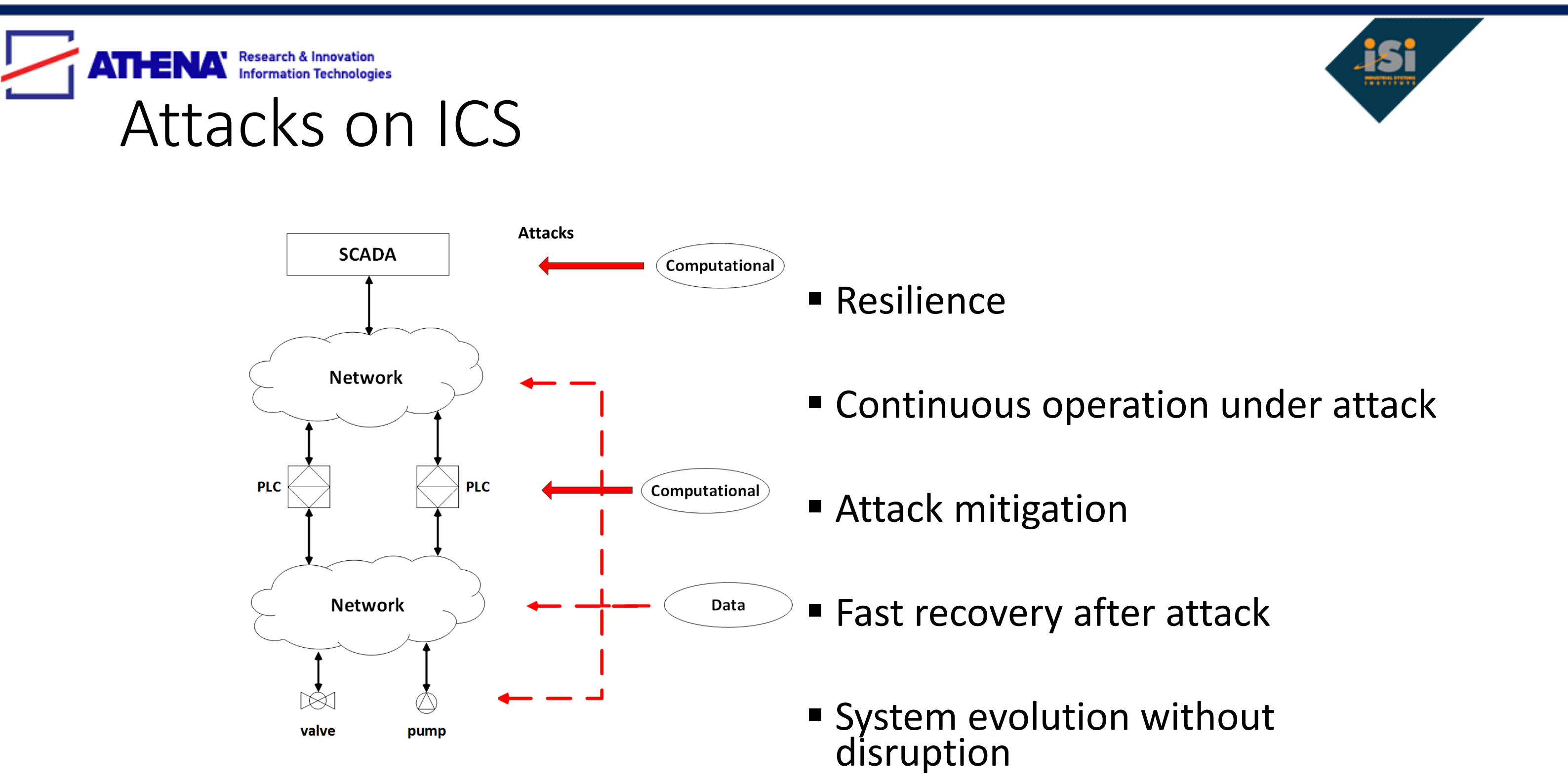




ATHENA Research & Innovation Information Technologies

System View - Requirements

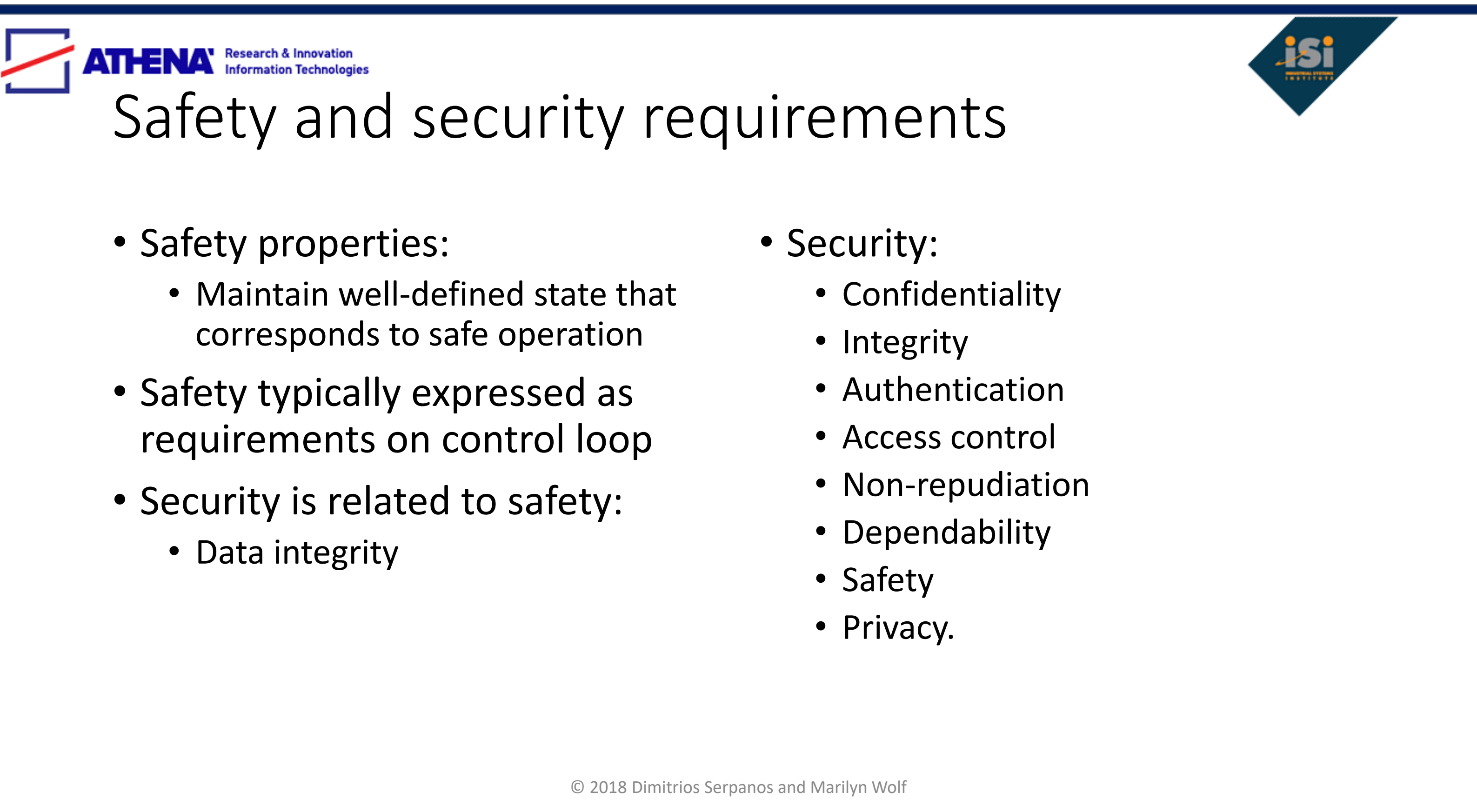
- Hierarchical structure
- Heterogeneous technologies
- Autonomy
- Continuous operation/fail-safe
- Dependability
- Dependence on large number of input devices
- Large installation base (legacy systems)
- Increasing connectivity



Attacks on ICS

- Resilience
- Continuous operation under attack
- Attack mitigation
- Fast recovery after attack
- System evolution without disruption

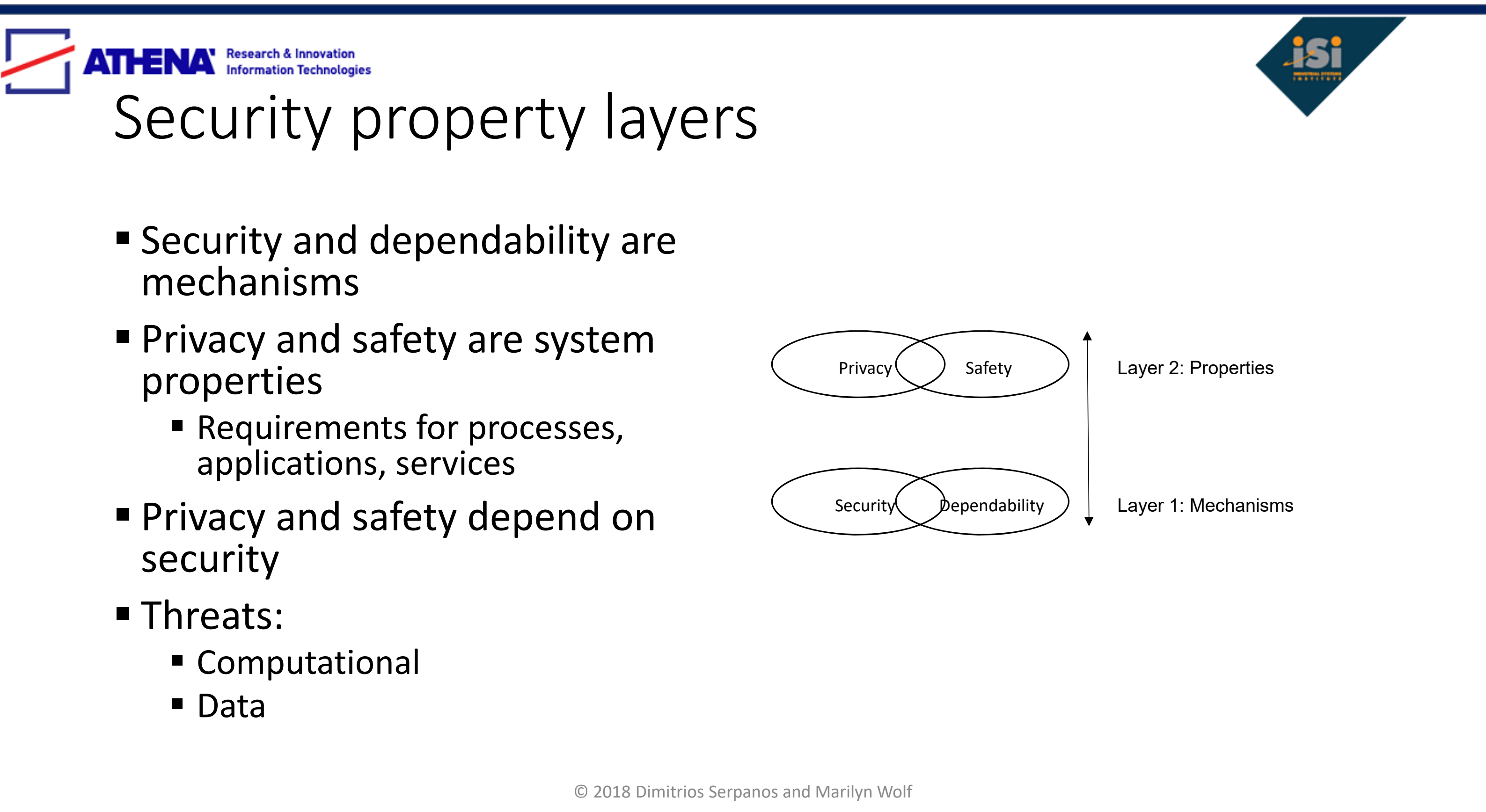
There have been several incidents…



Safety and security requirements

- Safety properties:
  - Maintain well-defined state that corresponds to safe operation
- Safety typically expressed as requirements on control loop
- Security is related to safety:
  - Data integrity

- Security:
  - Confidentiality
  - Integrity
  - Authentication
  - Access control
  - Non-repudiation
  - Dependability
  - Safety
  - Privacy.



Security property layers

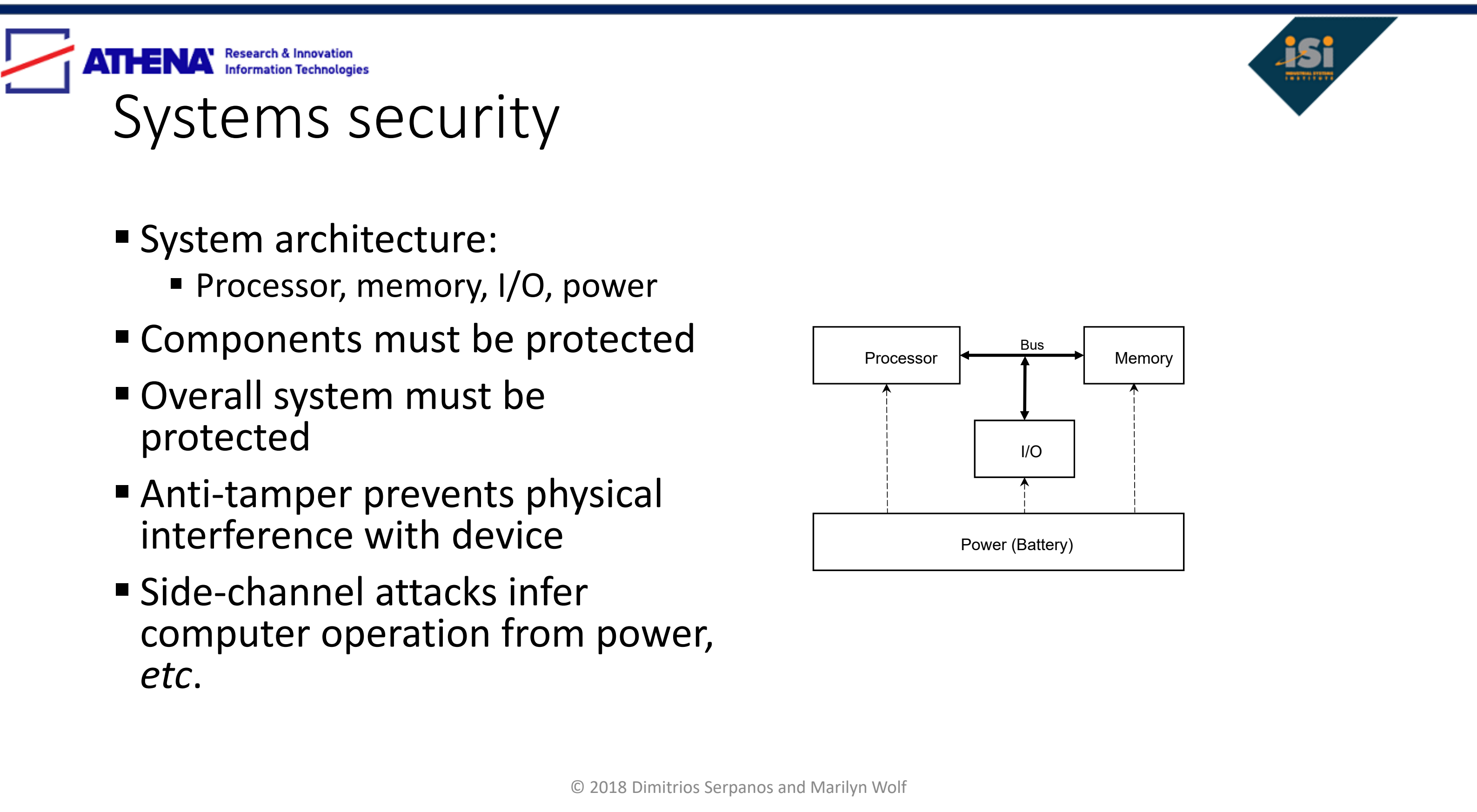
- Security and dependability are mechanisms
- Privacy and safety are system properties
  - Requirements for processes, applications, services
- Privacy and safety depend on security
- Threats:
  - Computational
  - Data

Privacy Safety

Layer 2: Properties

Security Dependability

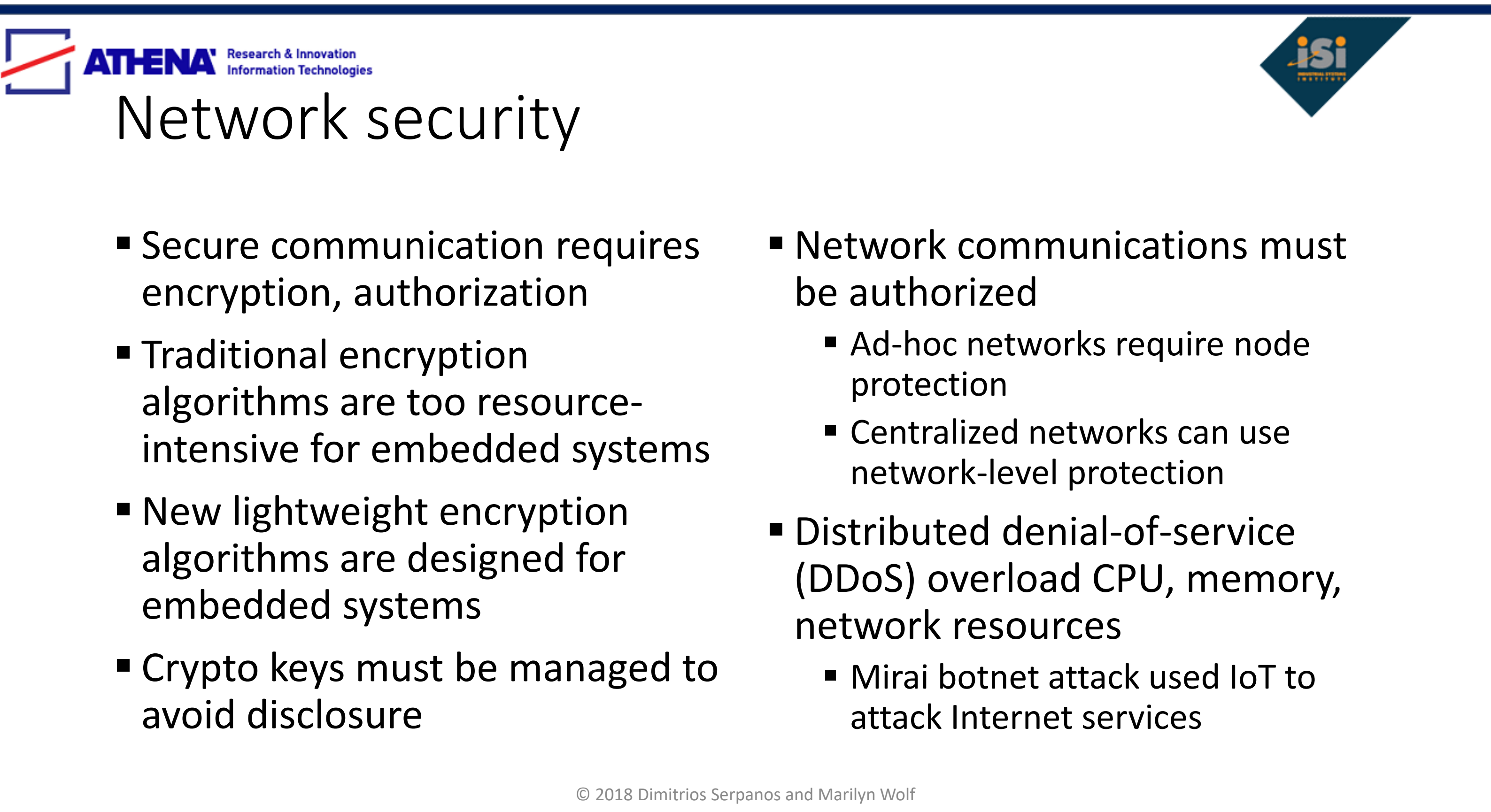
Layer 1: Mechanisms



Systems security

- System architecture:
  - Processor, memory, I/O, power
- Components must be protected
- Overall system must be protected
- Anti-tamper prevents physical interference with device
- Side-channel attacks infer computer operation from power, *etc*.

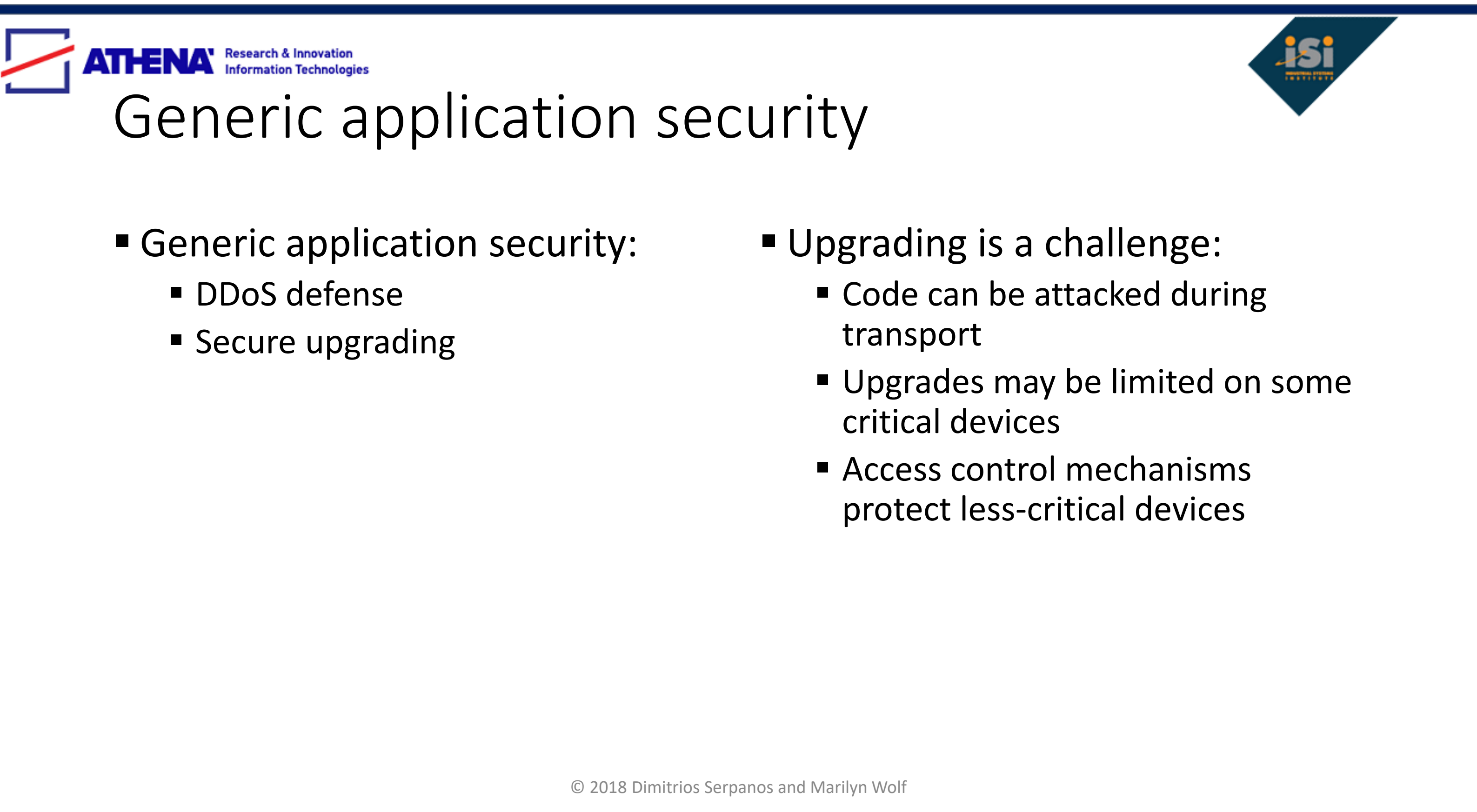
Processor
Bus
Memory
I/O
Power (Battery)



ATHENA Research & Innovation Information Technologies

Network security

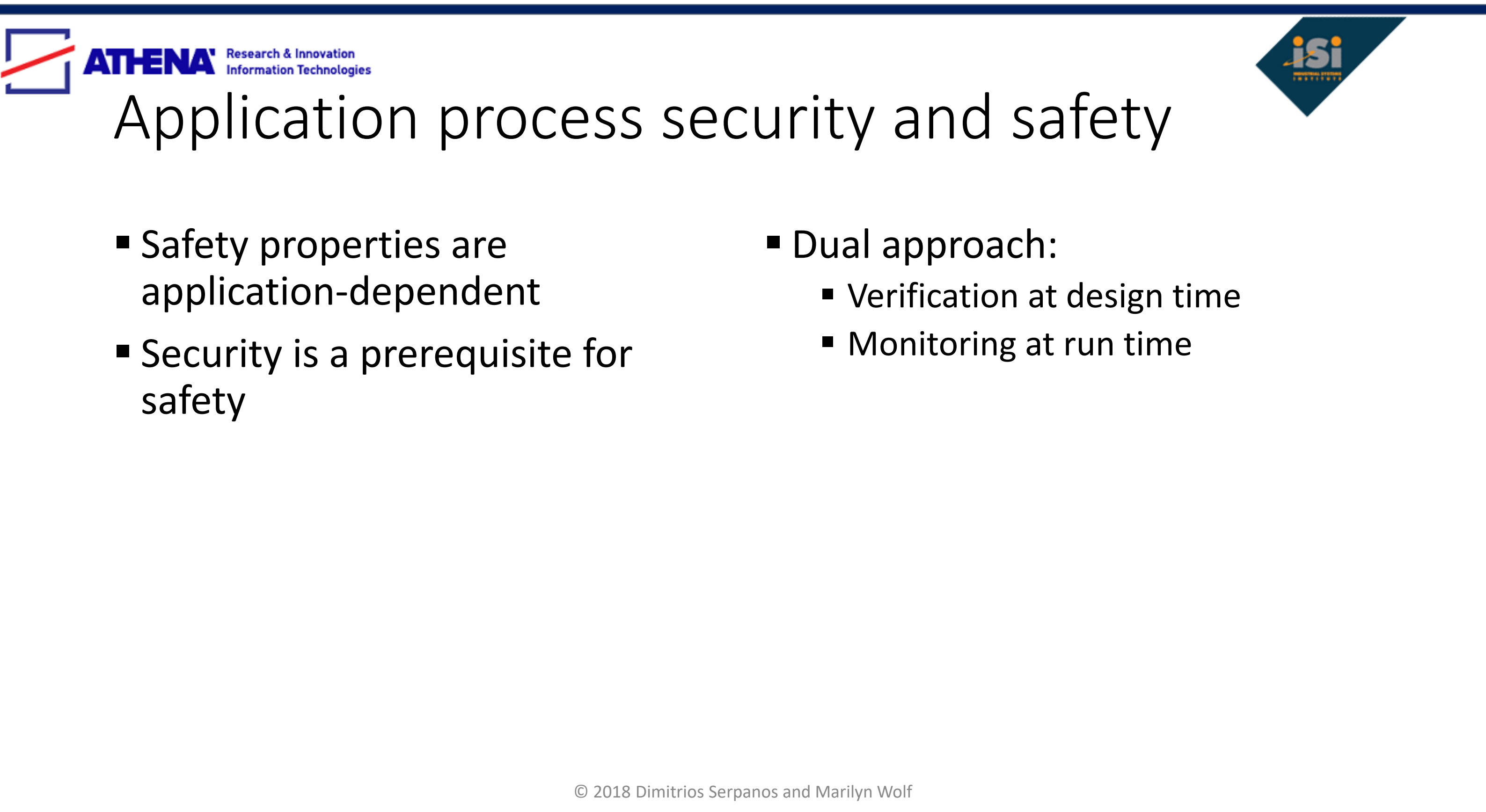
- Secure communication requires encryption, authorization
- Traditional encryption algorithms are too resource-intensive for embedded systems
- New lightweight encryption algorithms are designed for embedded systems
- Crypto keys must be managed to avoid disclosure
- Network communications must be authorized
  - Ad-hoc networks require node protection
  - Centralized networks can use network-level protection
- Distributed denial-of-service (DDoS) overload CPU, memory, network resources
  - Mirai botnet attack used IoT to attack Internet services



Generic application security

- Generic application security:
  - DDoS defense
  - Secure upgrading
- Upgrading is a challenge:
  - Code can be attacked during transport
  - Upgrades may be limited on some critical devices
  - Access control mechanisms protect less-critical devices

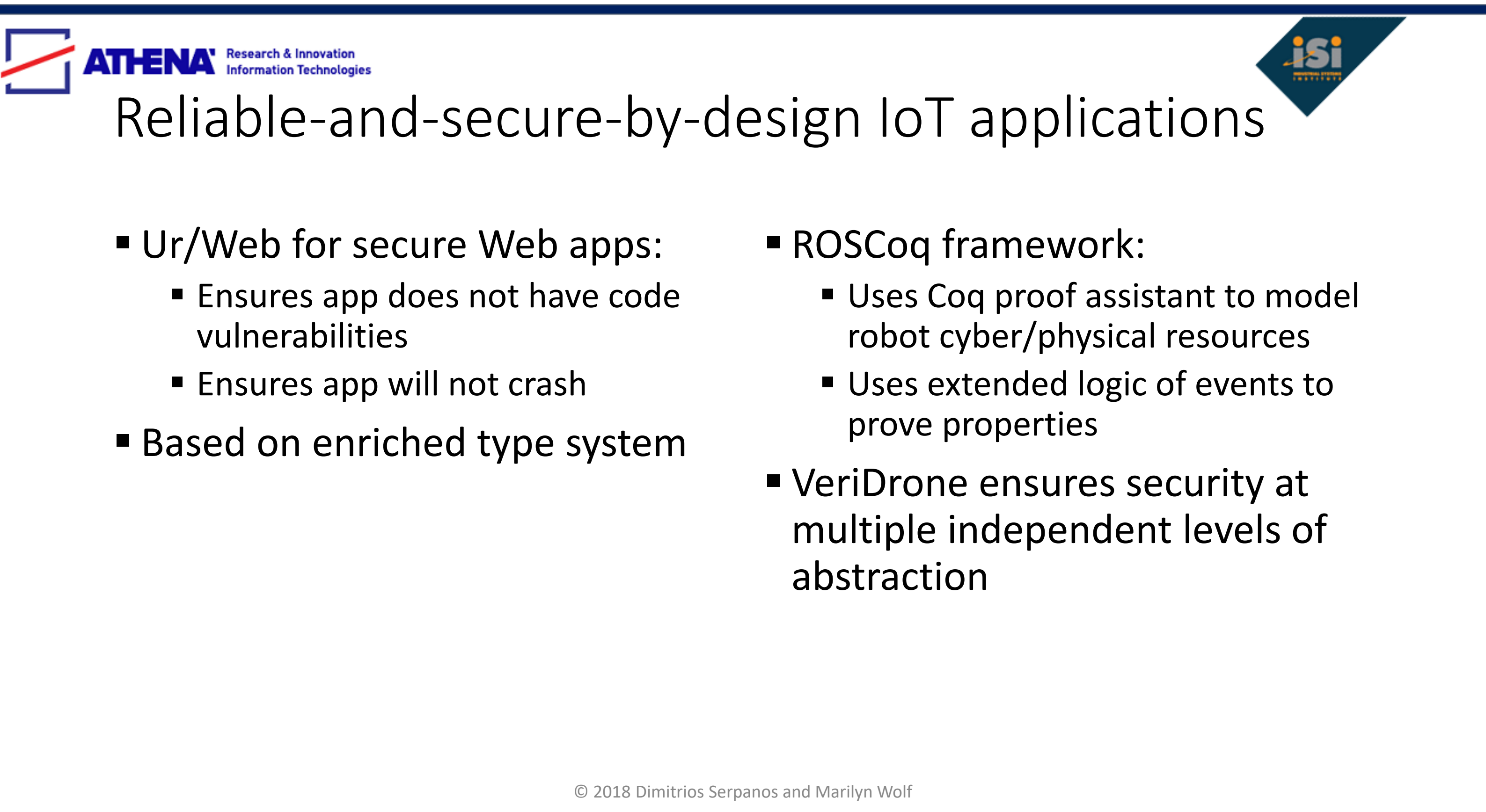
© 2018 Dimitrios Serpanos and Marilyn Wolf



Application process security and safety

- Safety properties are application-dependent
- Security is a prerequisite for safety

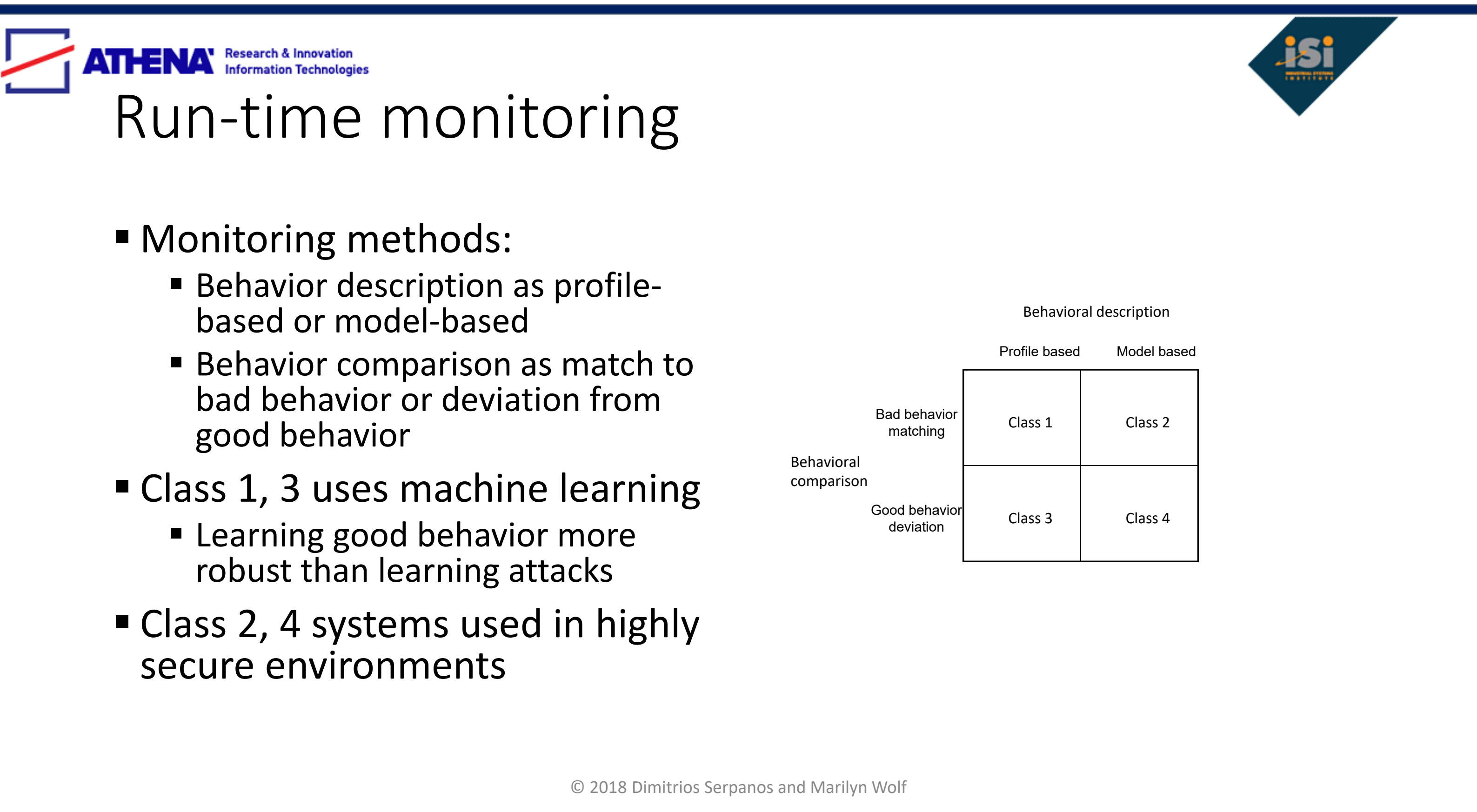
- Dual approach:
  - Verification at design time
  - Monitoring at run time



Reliable-and-secure-by-design IoT applications

- Ur/Web for secure Web apps:
  - Ensures app does not have code vulnerabilities
  - Ensures app will not crash
- Based on enriched type system

- ROSCoq framework:
  - Uses Coq proof assistant to model robot cyber/physical resources
  - Uses extended logic of events to prove properties
- VeriDrone ensures security at multiple independent levels of abstraction

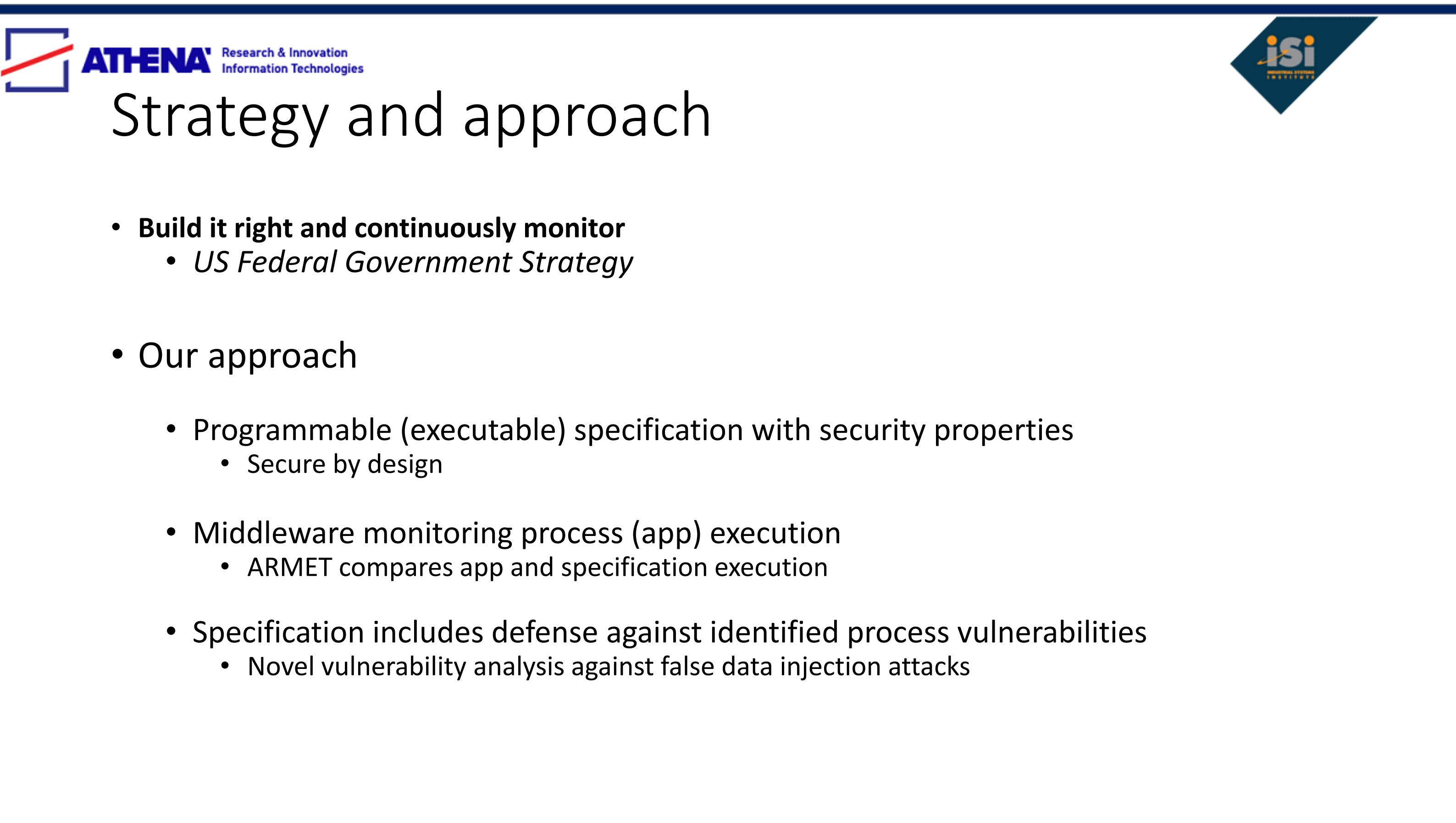


Run-time monitoring

- Monitoring methods:
  - Behavior description as profile-based or model-based
  - Behavior comparison as match to bad behavior or deviation from good behavior
- Class 1, 3 uses machine learning
  - Learning good behavior more robust than learning attacks
- Class 2, 4 systems used in highly secure environments

Behavioral description

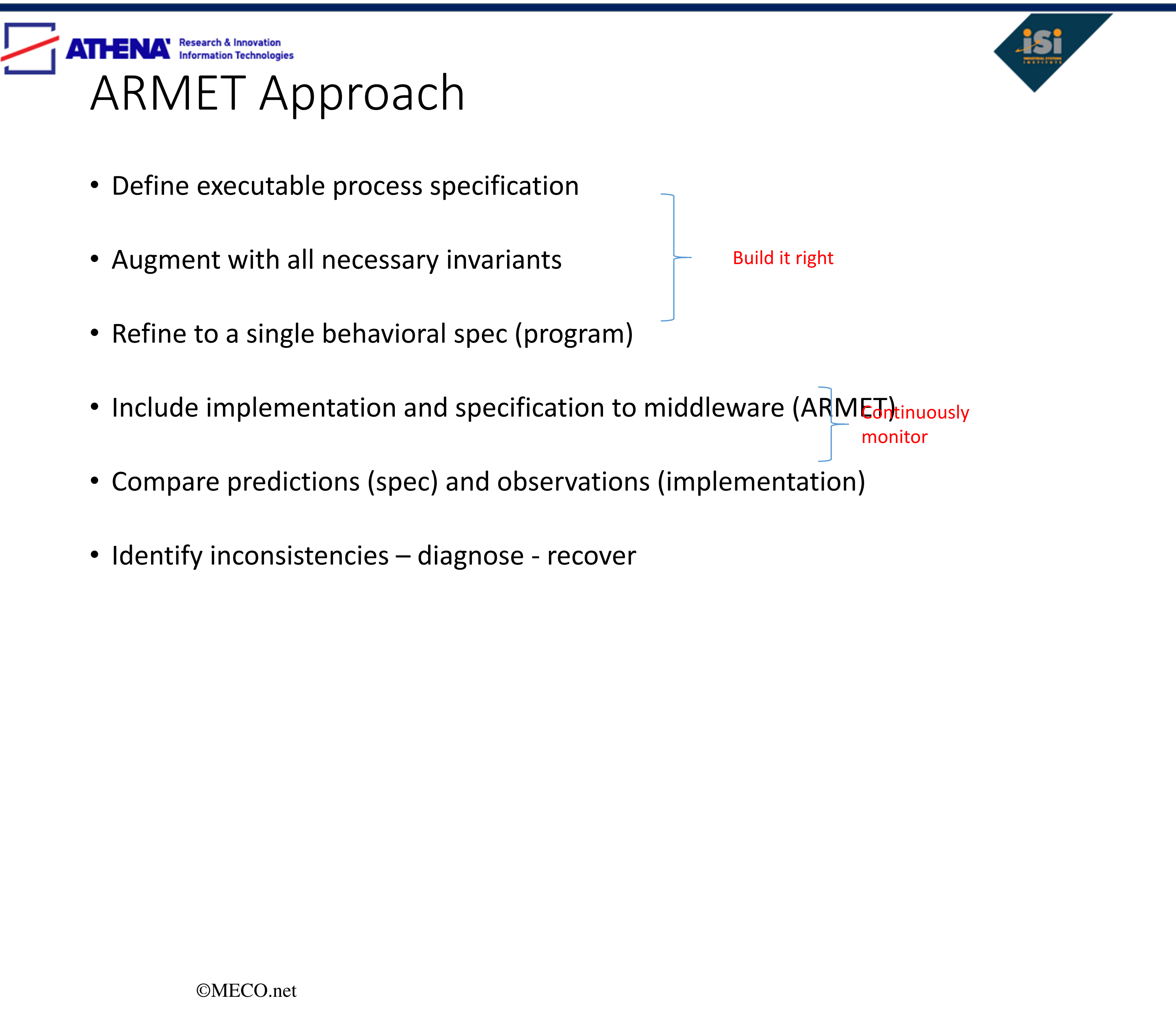
		Profile based	Model based
Behavioral comparison	Bad behavior matching	Class 1	Class 2
	Good behavior deviation	Class 3	Class 4



Strategy and approach

- **Build it right and continuously monitor**
  - *US Federal Government Strategy*

- Our approach
  - Programmable (executable) specification with security properties
    - Secure by design
  - Middleware monitoring process (app) execution
    - ARMET compares app and specification execution
  - Specification includes defense against identified process vulnerabilities
    - Novel vulnerability analysis against false data injection attacks


ATHENA Research & Innovation Information Technologies
isi

ARMET Approach

- Define executable process specification
- Augment with all necessary invariants
- Refine to a single behavioral spec (program)
- Include implementation and specification to middleware (ARMET)
- Compare predictions (spec) and observations (implementation)
- Identify inconsistencies – diagnose - recover

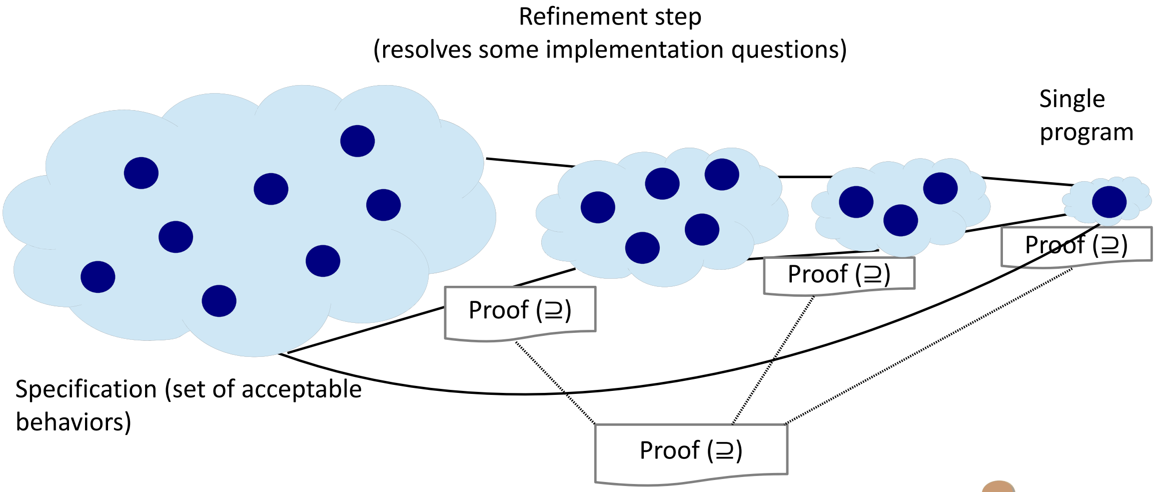
Build it right

Continuously monitor

©MECO.net

ATHENA Research & Innovation Information Technologies

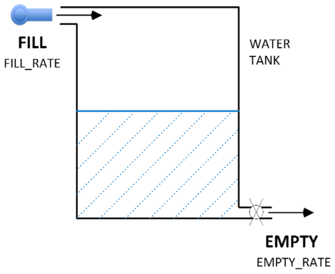
Program derivation by stepwise refinement

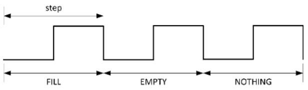

Refinement step
(resolves some implementation questions)
Single program
Proof (⊒)
Proof (⊒)
Proof (⊒)
Proof (⊒)
Specification (set of acceptable behaviors)

Proofs constructed & checked with **Coq**, a general-purpose logic platform

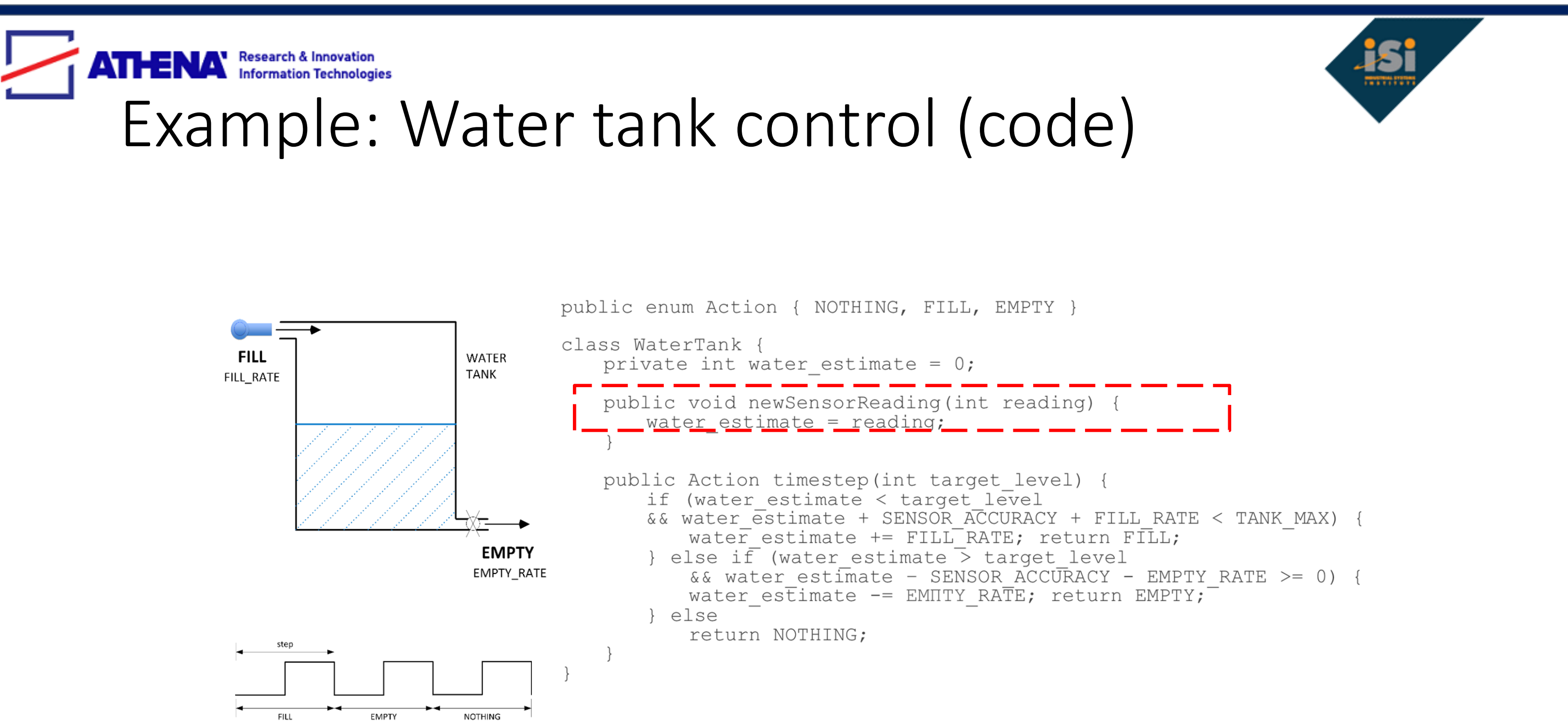
©MECO.net

Example: Water tank control (spec)





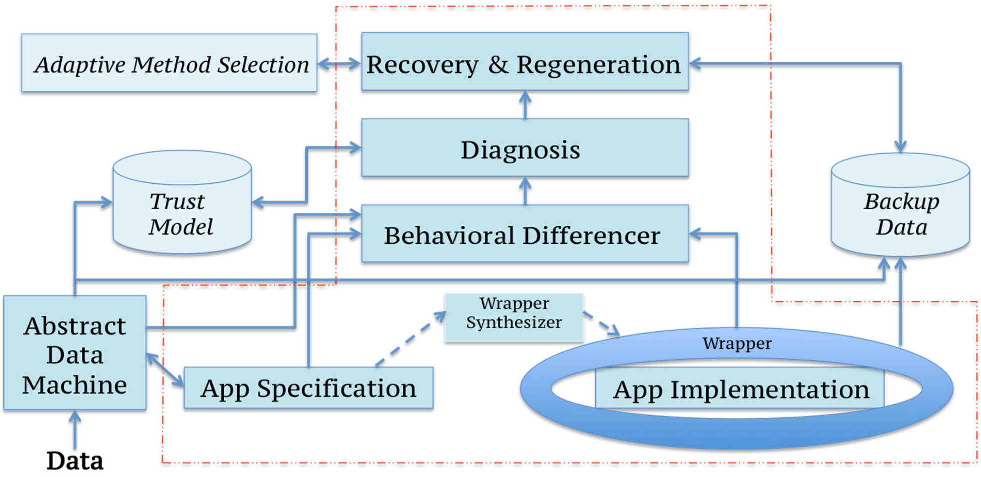
```
public enum Action { NOTHING, FILL, EMPTY }

class WaterTankSpec {
   private int water_level = 0;

   public void newSensorReading(int reading) {
      if (abs(reading - water_level) > SENSOR_ACCURACY)
         water_level = {n | True};
   }

   public Action timestep(int target_level) {
      Action act = {a | (a = FILL → water_level + FILL_RATE ≤ TANK_MAX)
             ∧ (a = EMPTY → water_level - EMPTY_RATE ≥ 0)};
      if (act == FILL)
         water_level += FILL_RATE;
      else if (act == EMPTY)
         water_level -= EMPTY_RATE;
      return act;
   }
}
```

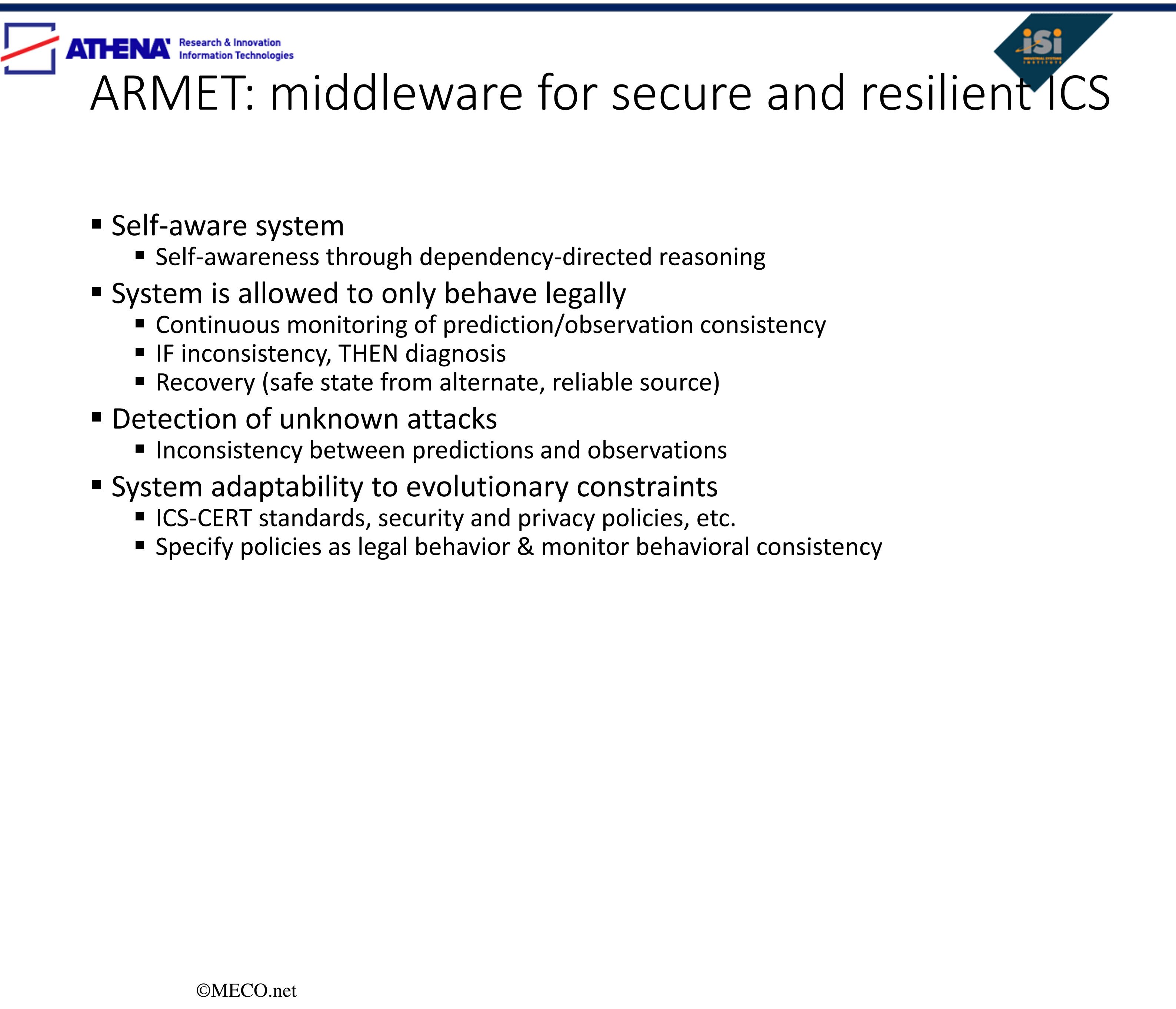


Example: Water tank control (code)

```
public enum Action { NOTHING, FILL, EMPTY }

class WaterTank {
    private int water_estimate = 0;

    public void newSensorReading(int reading) {
        water_estimate = reading;
    }

    public Action timestep(int target_level) {
        if (water_estimate < target_level
        && water_estimate + SENSOR_ACCURACY + FILL_RATE < TANK_MAX) {
            water_estimate += FILL_RATE; return FILL;
        } else if (water_estimate > target_level
            && water_estimate - SENSOR_ACCURACY - EMPTY_RATE >= 0) {
            water_estimate -= EMΠTY_RATE; return EMPTY;
        } else
            return NOTHING;
    }
}
```

ARMET: Organization

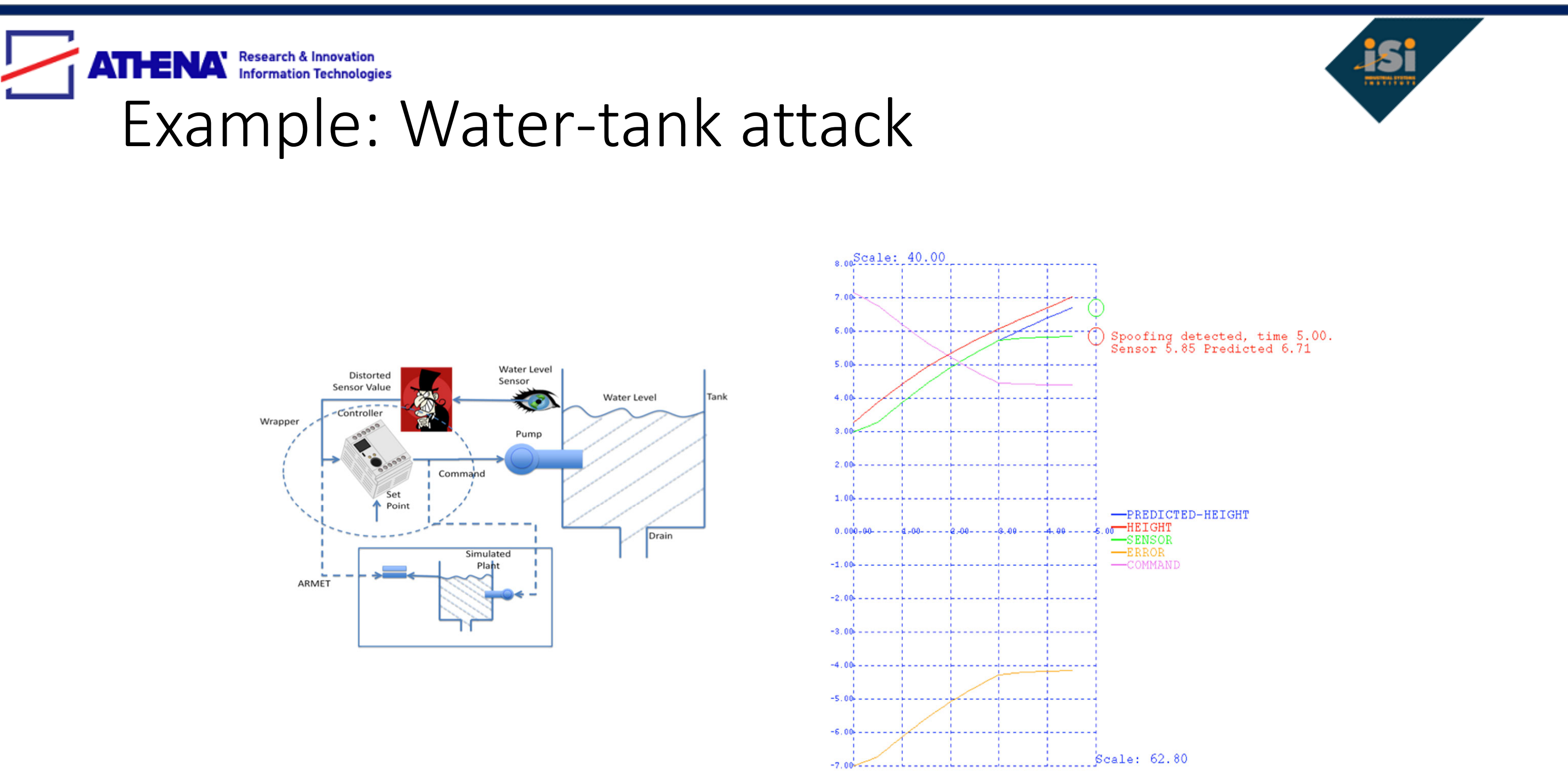




ATHENA Research & Innovation Information Technologies

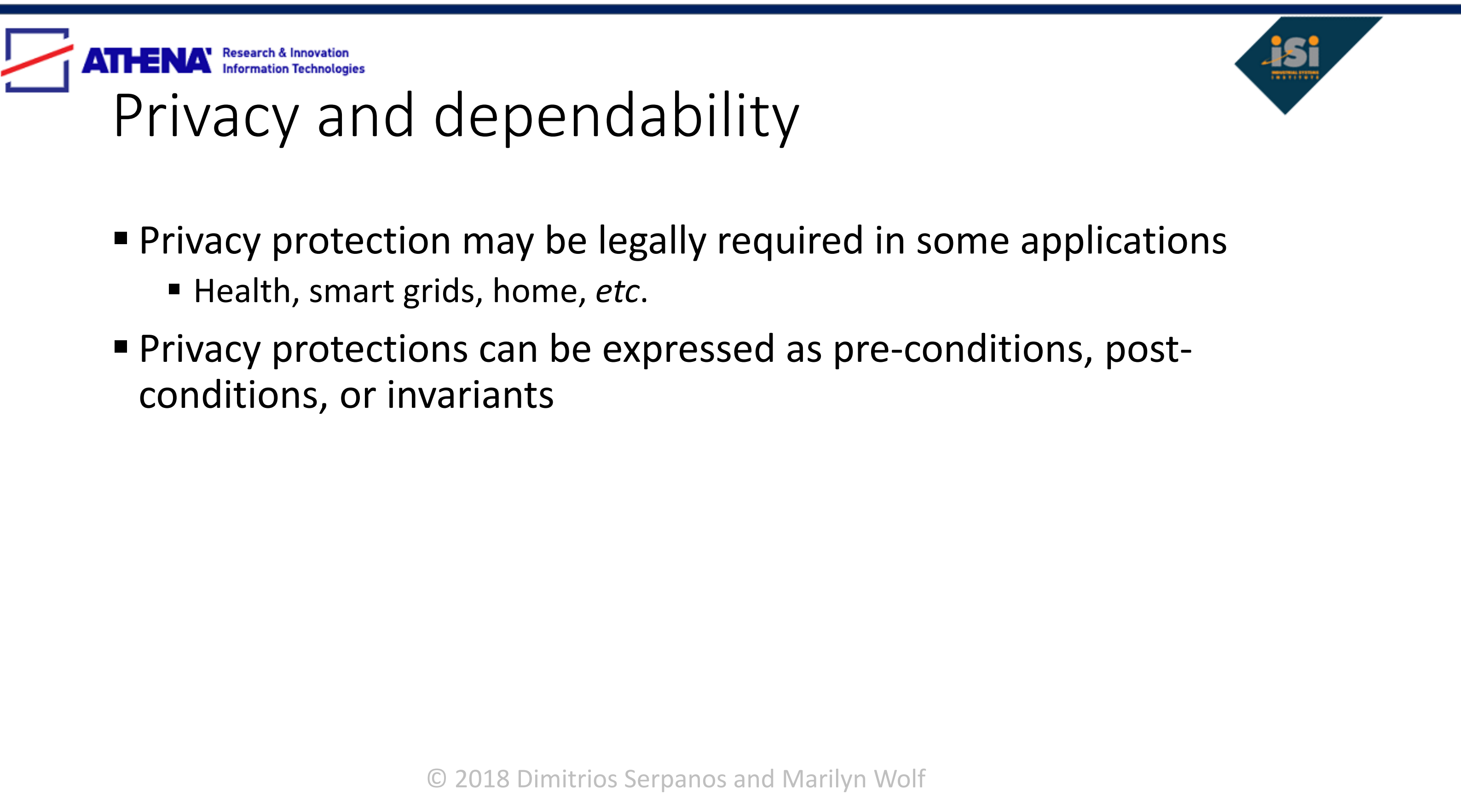
ARMET: middleware for secure and resilient ICS

- Self-aware system
  - Self-awareness through dependency-directed reasoning
- System is allowed to only behave legally
  - Continuous monitoring of prediction/observation consistency
  - IF inconsistency, THEN diagnosis
  - Recovery (safe state from alternate, reliable source)
- Detection of unknown attacks
  - Inconsistency between predictions and observations
- System adaptability to evolutionary constraints
  - ICS-CERT standards, security and privacy policies, etc.
  - Specify policies as legal behavior & monitor behavioral consistency



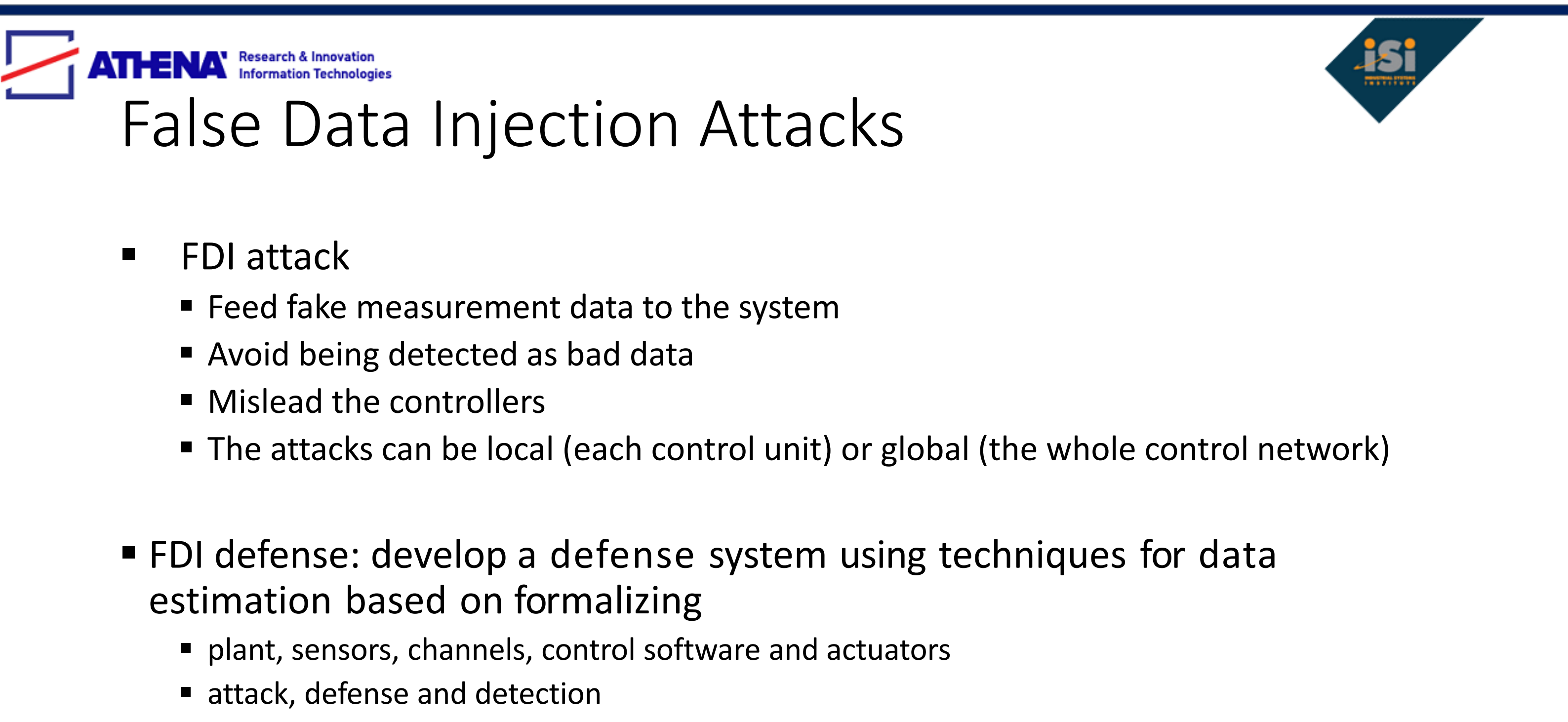
Example: Water-tank attack

Spoofing detected, time 5.00.
Sensor 5.85 Predicted 6.71



Privacy and dependability

- Privacy protection may be legally required in some applications
  - Health, smart grids, home, *etc*.
- Privacy protections can be expressed as pre-conditions, post-conditions, or invariants



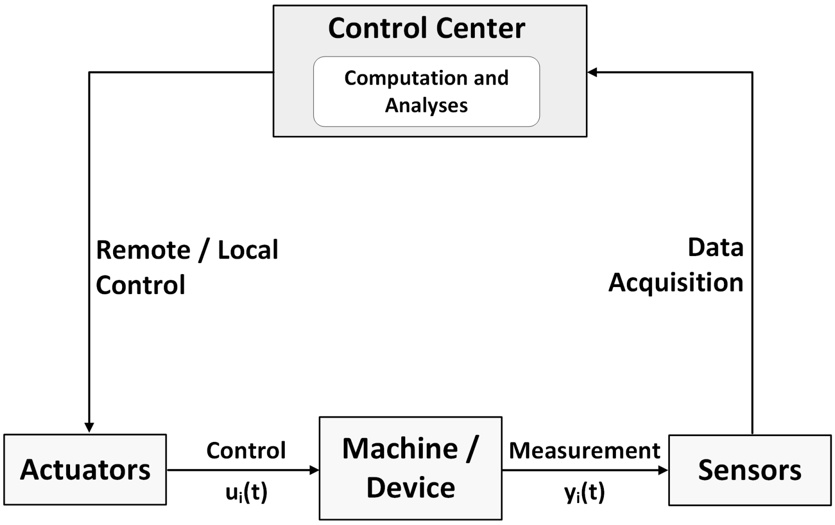
ATHENA Research & Innovation Information Technologies

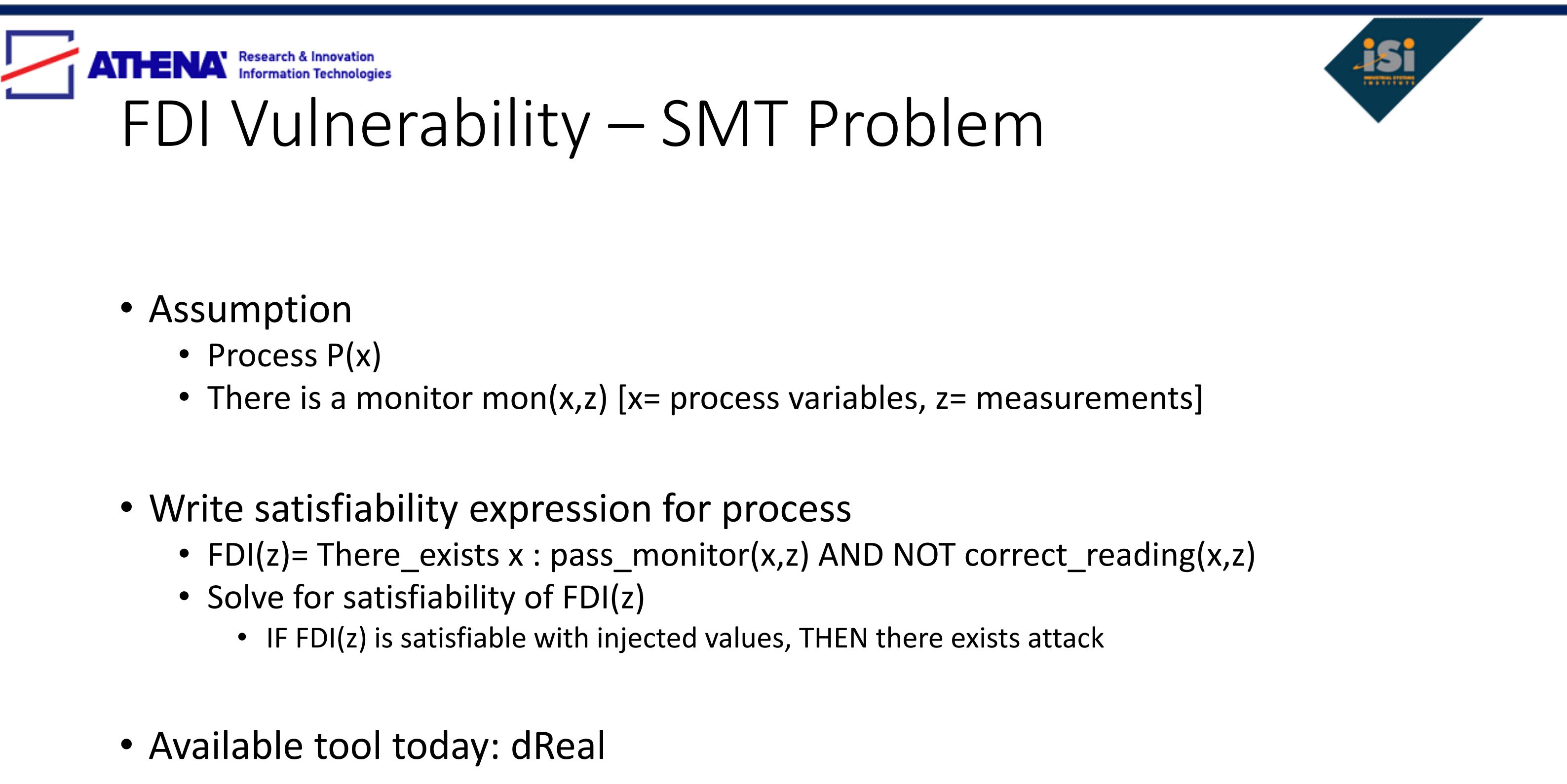
False Data Injection Attacks

- FDI attack
  - Feed fake measurement data to the system
  - Avoid being detected as bad data
  - Mislead the controllers
  - The attacks can be local (each control unit) or global (the whole control network)
- FDI defense: develop a defense system using techniques for data estimation based on formalizing
  - plant, sensors, channels, control software and actuators
  - attack, defense and detection

ATHENA Research & Innovation Information Technologies

ICS Control Loop





FDI Vulnerability – SMT Problem

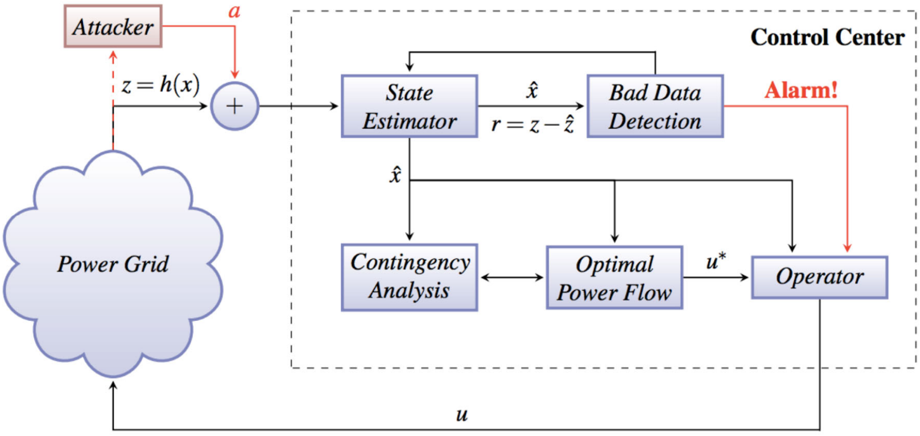
- Assumption
  - Process P(x)
  - There is a monitor mon(x,z) [x= process variables, z= measurements]

- Write satisfiability expression for process
  - FDI(z)= There_exists x : pass_monitor(x,z) AND NOT correct_reading(x,z)
  - Solve for satisfiability of FDI(z)
    - IF FDI(z) is satisfiable with injected values, THEN there exists attack

- Available tool today: dReal

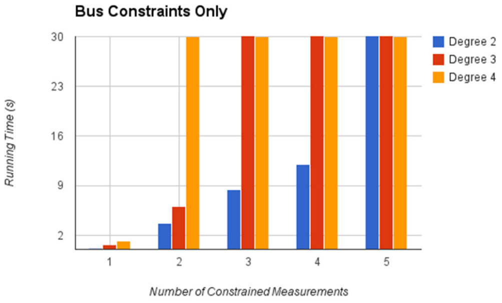
ATHENA Research & Innovation Information Technologies

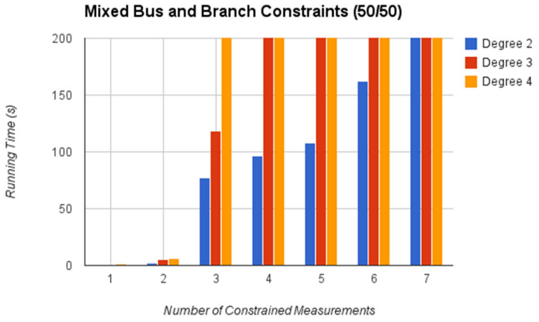
Example: FDI Attack for State Estimation

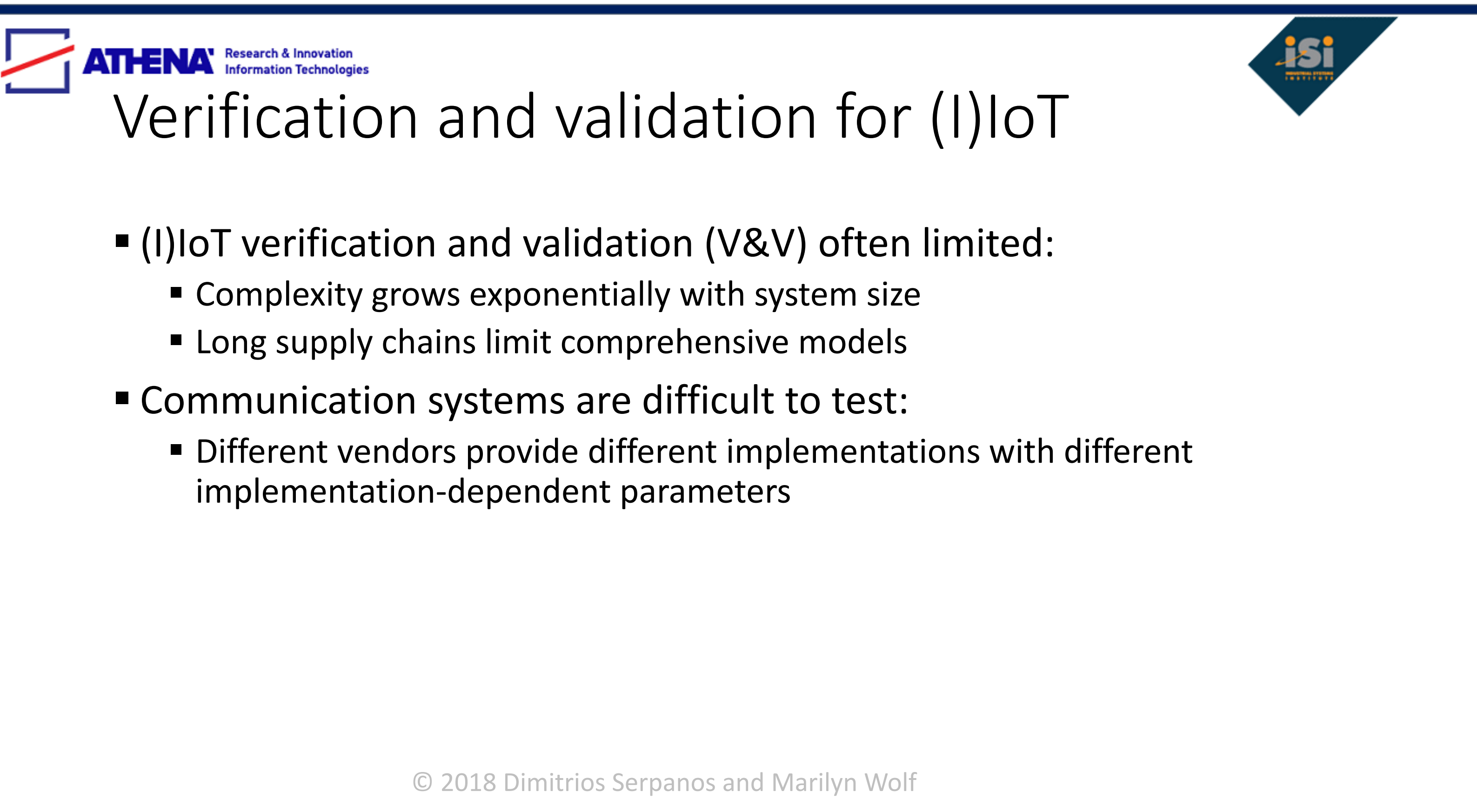


ATHENA Research & Innovation Information Technologies

Analysis of benchmarks



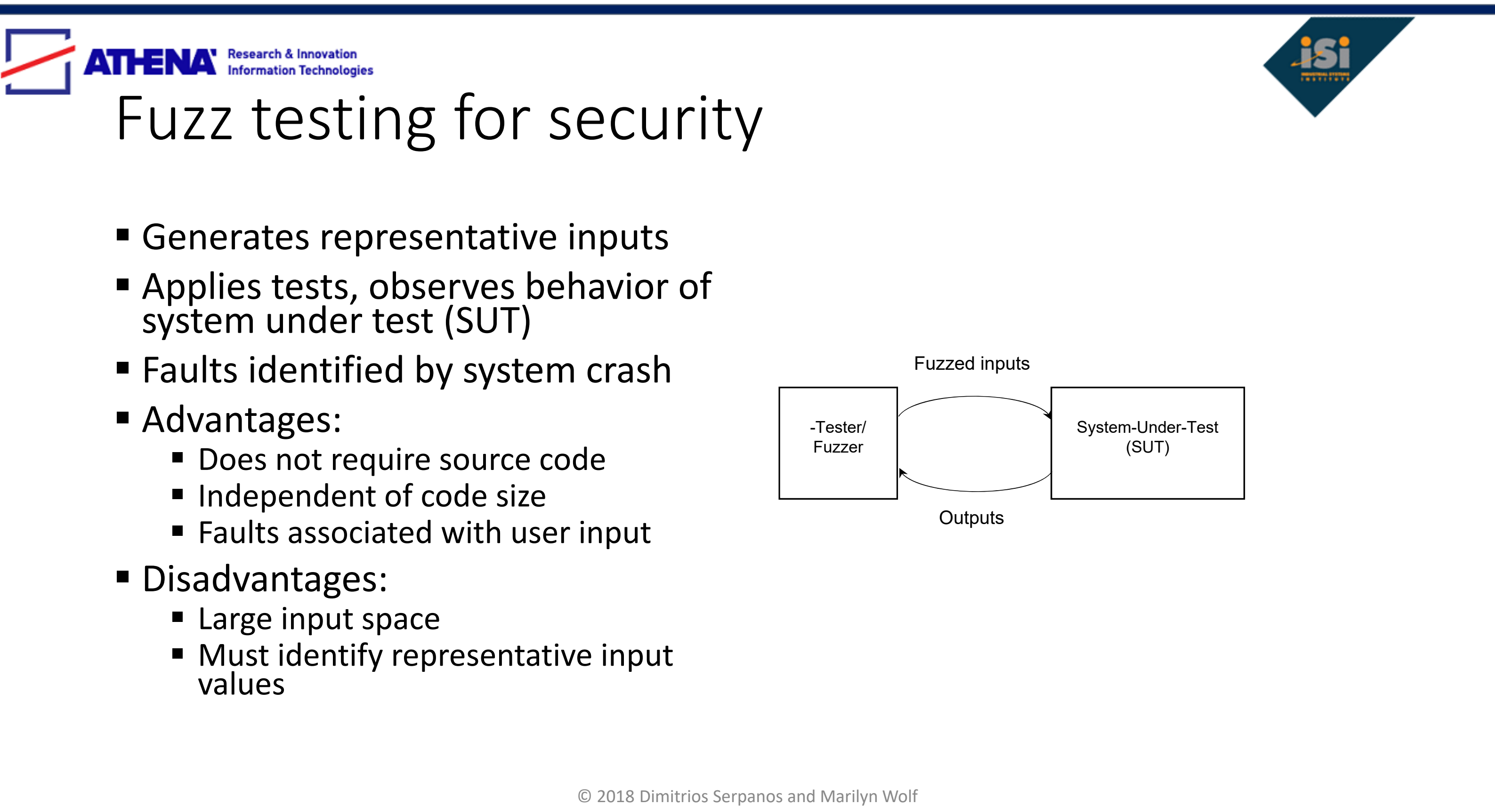




ATHENA Research & Innovation Information Technologies

Verification and validation for (I)IoT

- (I)IoT verification and validation (V&V) often limited:
  - Complexity grows exponentially with system size
  - Long supply chains limit comprehensive models
- Communication systems are difficult to test:
  - Different vendors provide different implementations with different implementation-dependent parameters



ATHENA Research & Innovation Information Technologies

Fuzz testing for security

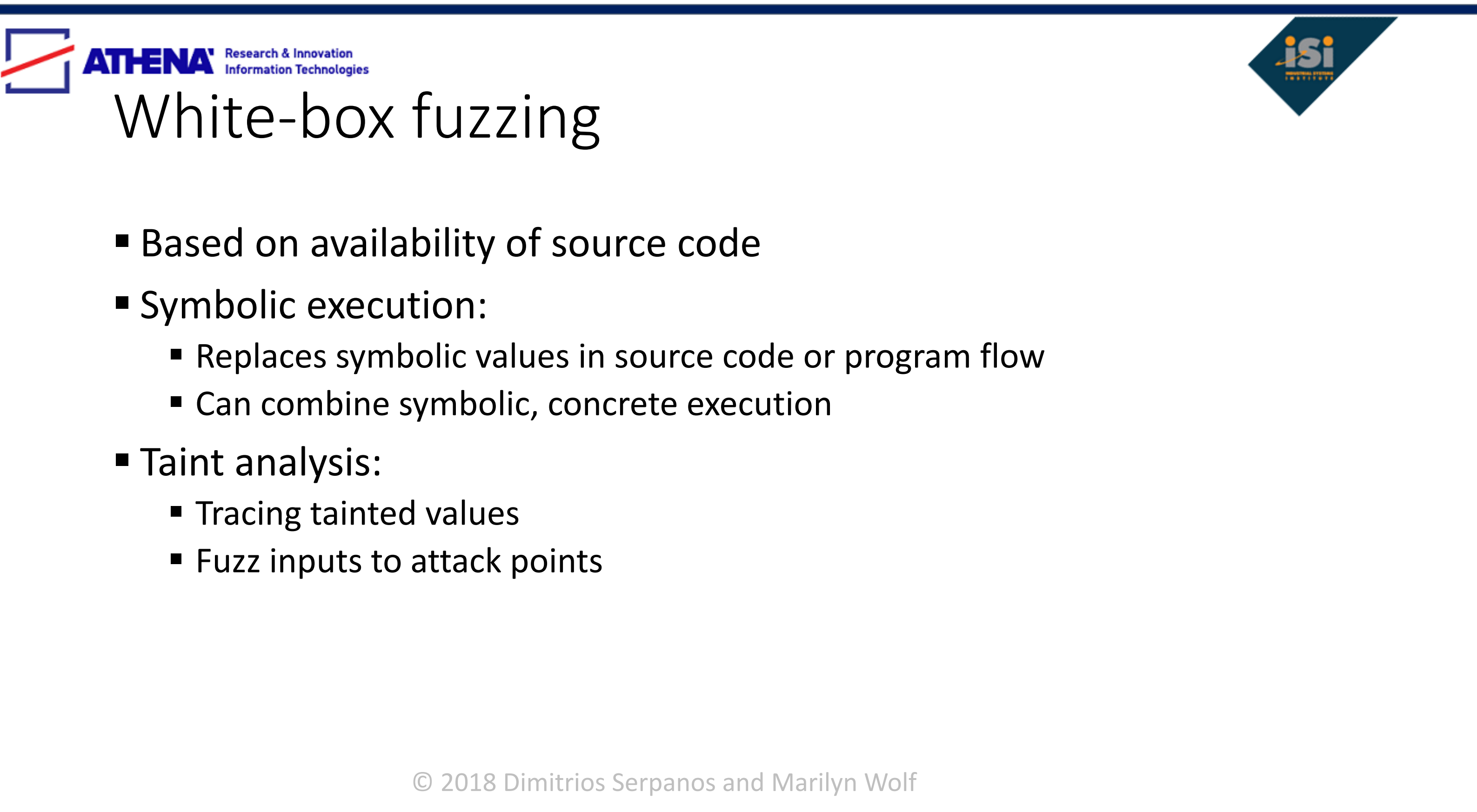
- Generates representative inputs
- Applies tests, observes behavior of system under test (SUT)
- Faults identified by system crash
- Advantages:
  - Does not require source code
  - Independent of code size
  - Faults associated with user input
- Disadvantages:
  - Large input space
  - Must identify representative input values

Fuzzed inputs

-Tester/ Fuzzer

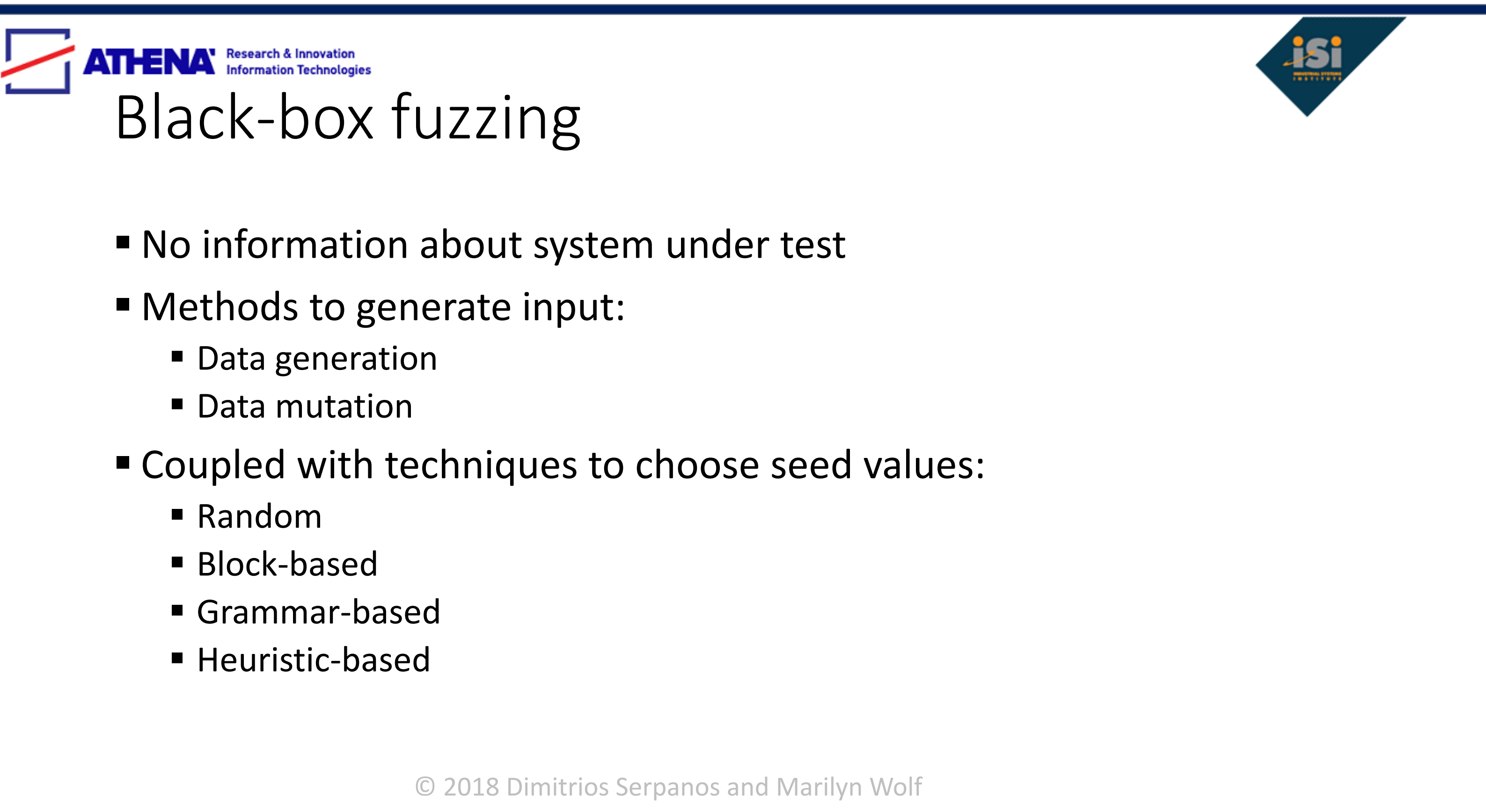
System-Under-Test (SUT)

Outputs



White-box fuzzing

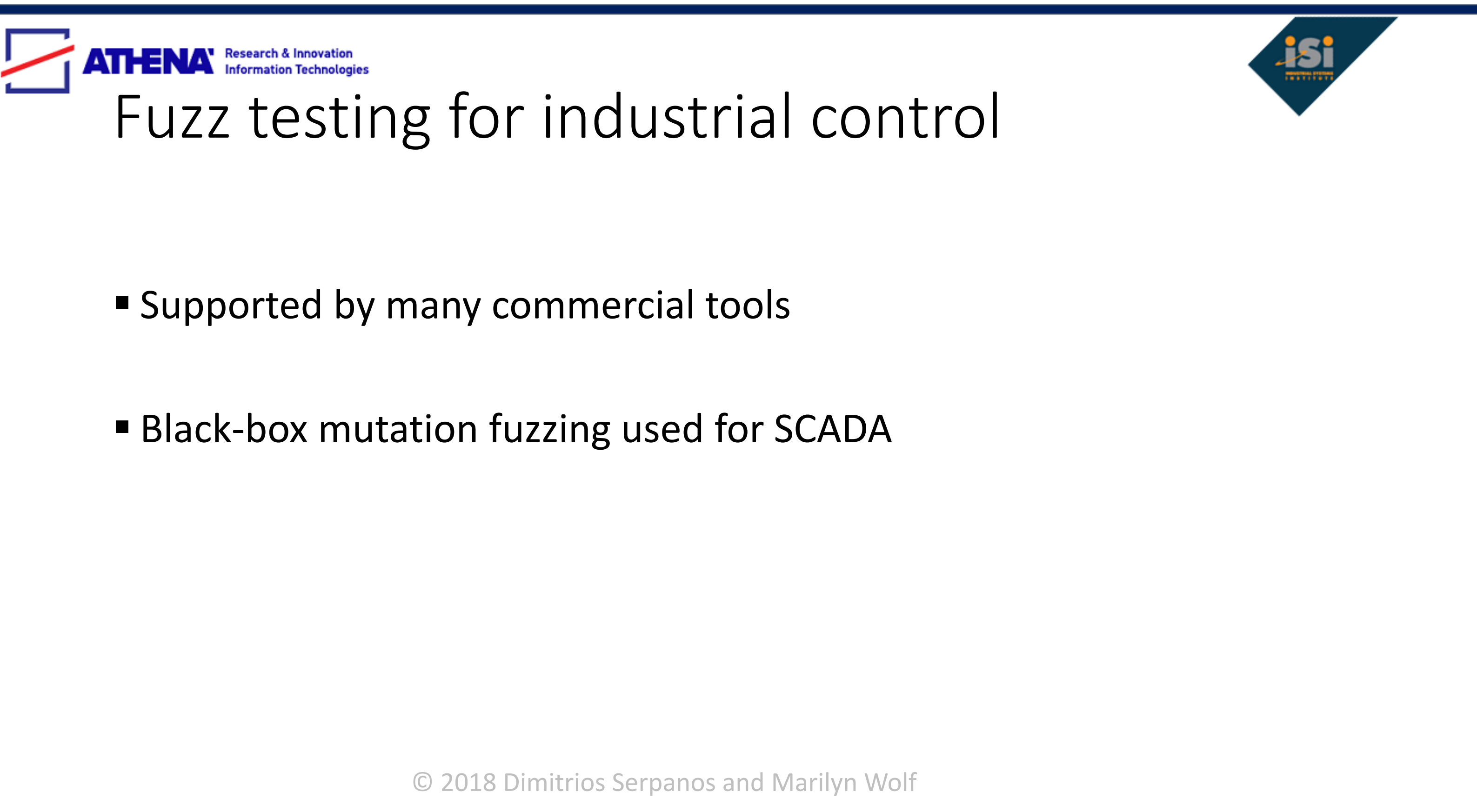
- Based on availability of source code
- Symbolic execution:
  - Replaces symbolic values in source code or program flow
  - Can combine symbolic, concrete execution
- Taint analysis:
  - Tracing tainted values
  - Fuzz inputs to attack points



ATHENA Research & Innovation Information Technologies
isi

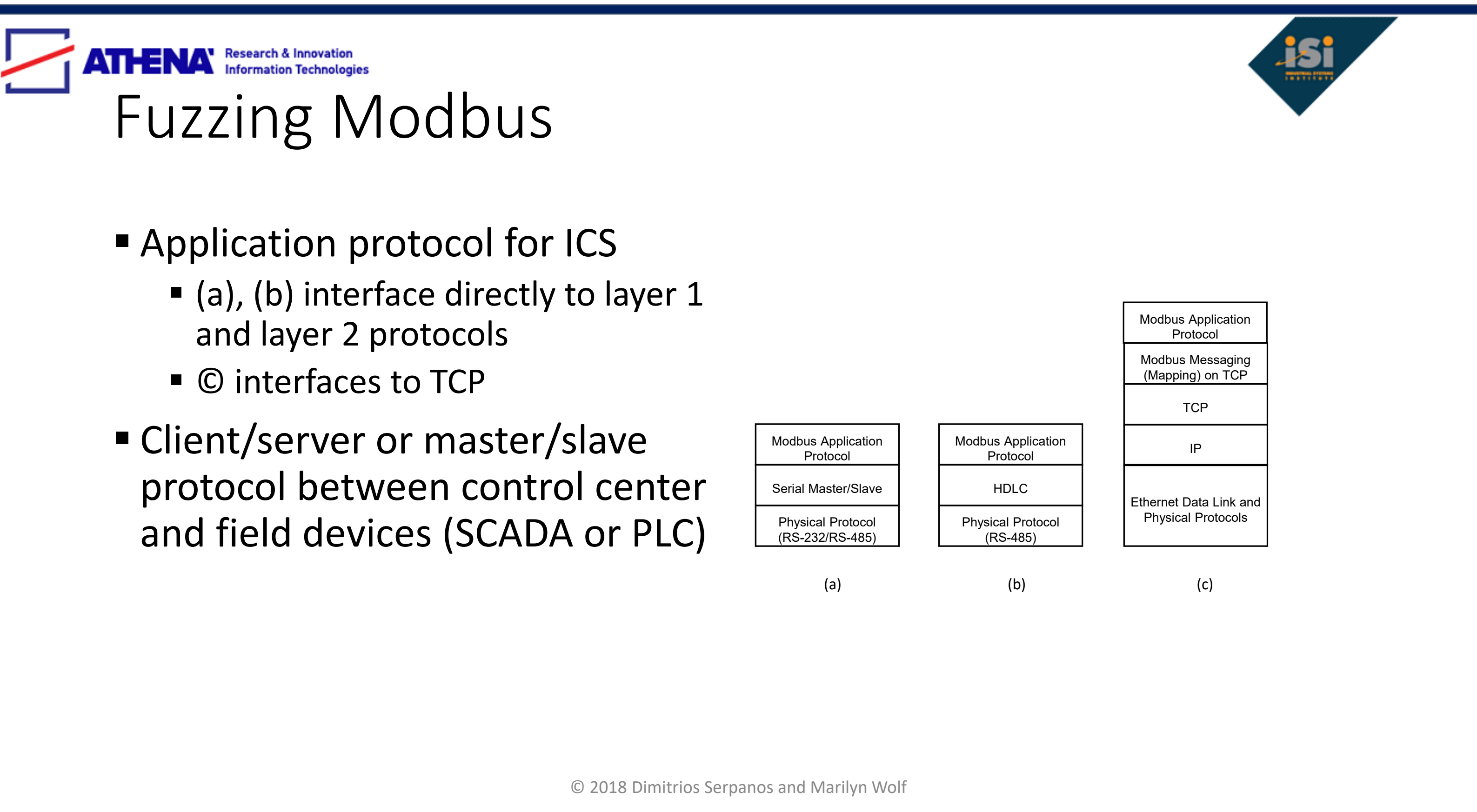
Black-box fuzzing

- No information about system under test
- Methods to generate input:
  - Data generation
  - Data mutation
- Coupled with techniques to choose seed values:
  - Random
  - Block-based
  - Grammar-based
  - Heuristic-based



Fuzz testing for industrial control

- Supported by many commercial tools
- Black-box mutation fuzzing used for SCADA



Fuzzing Modbus

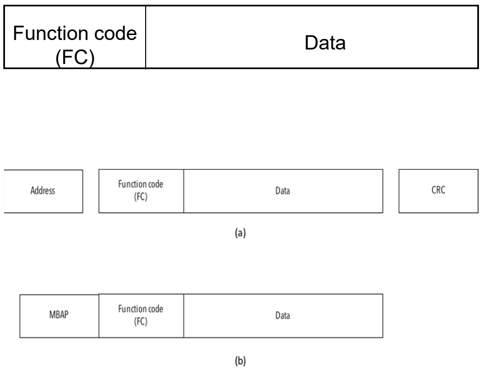
- Application protocol for ICS
  - (a), (b) interface directly to layer 1 and layer 2 protocols
  - © interfaces to TCP
- Client/server or master/slave protocol between control center and field devices (SCADA or PLC)

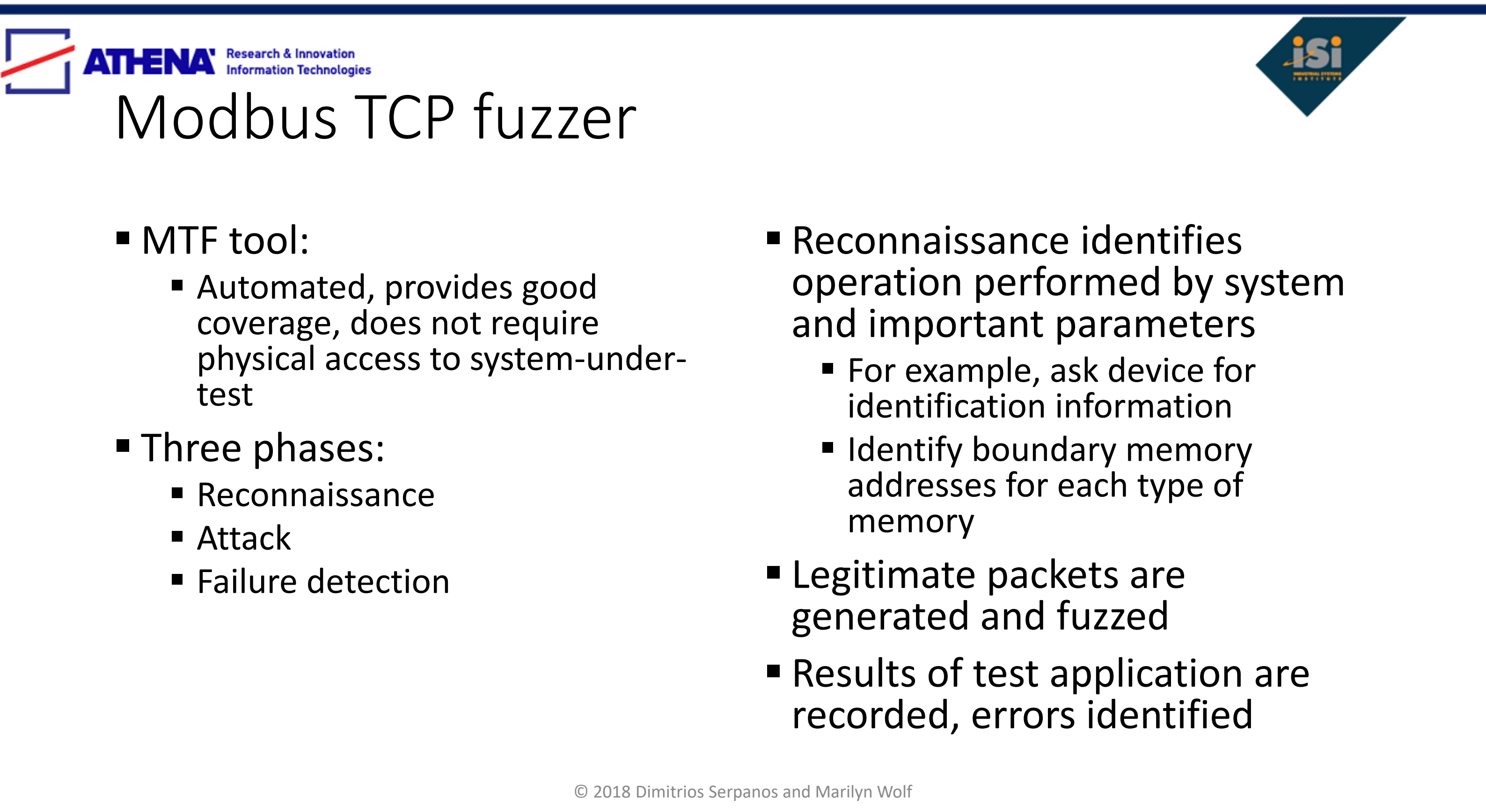
Modbus Application Protocol
Serial Master/Slave
Physical Protocol (RS-232/RS-485)
(a)
Modbus Application Protocol
HDLC
Physical Protocol (RS-485)
(b)
Modbus Application Protocol
Modbus Messaging (Mapping) on TCP
TCP
IP
Ethernet Data Link and Physical Protocols
(c)

ATHENA Research & Innovation Information Technologies

Modbus application packet

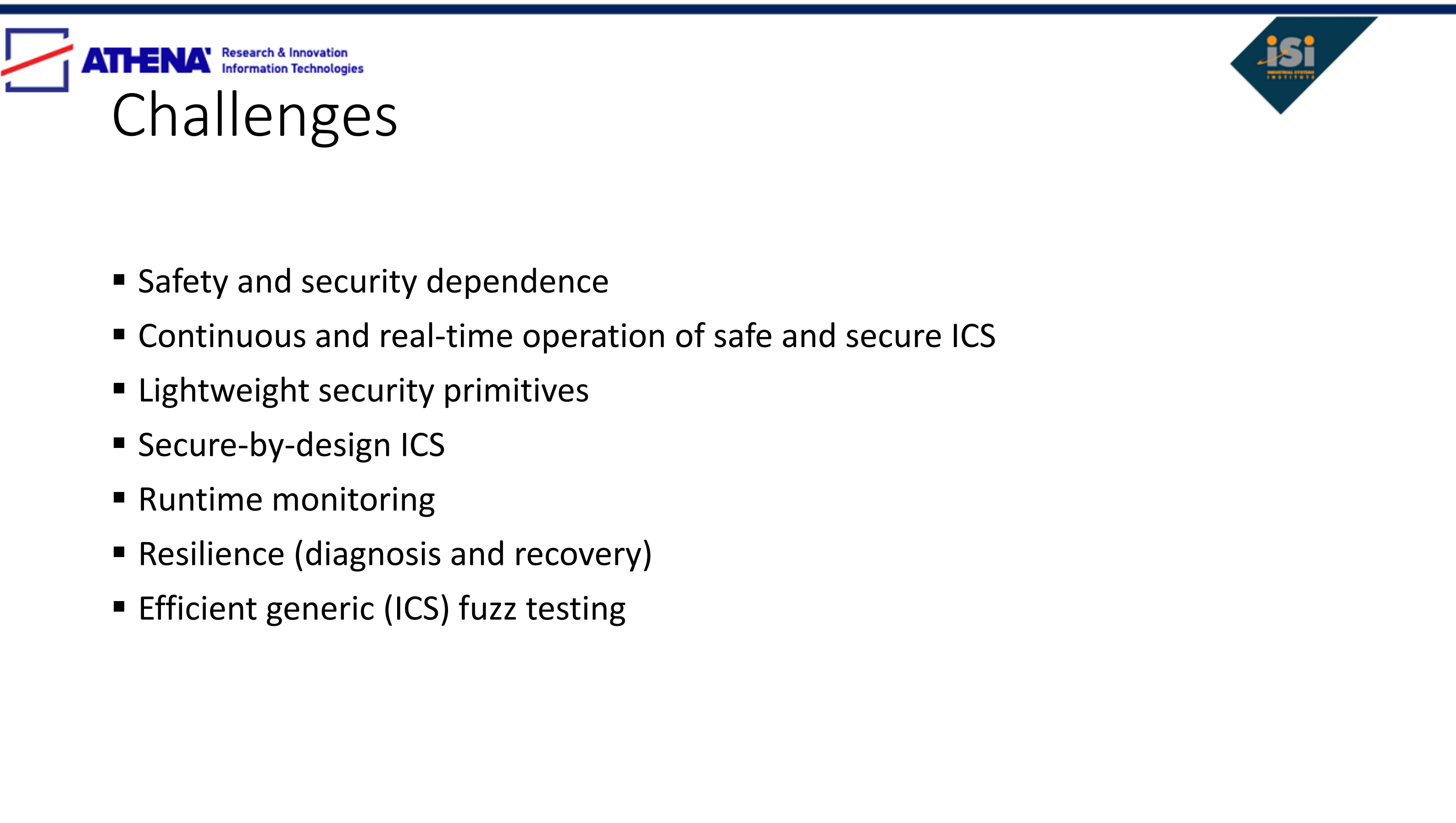
- Requests send function code to execute and related data
- Client responds with function code executed and related data
- Three classes of function codes:
  - Public
  - User-defined
  - Reserved
- Application packets are encapsulated in lower-layer protocol packets





Modbus TCP fuzzer

- MTF tool:
  - Automated, provides good coverage, does not require physical access to system-under-test
- Three phases:
  - Reconnaissance
  - Attack
  - Failure detection
- Reconnaissance identifies operation performed by system and important parameters
  - For example, ask device for identification information
  - Identify boundary memory addresses for each type of memory
- Legitimate packets are generated and fuzzed
- Results of test application are recorded, errors identified



Challenges

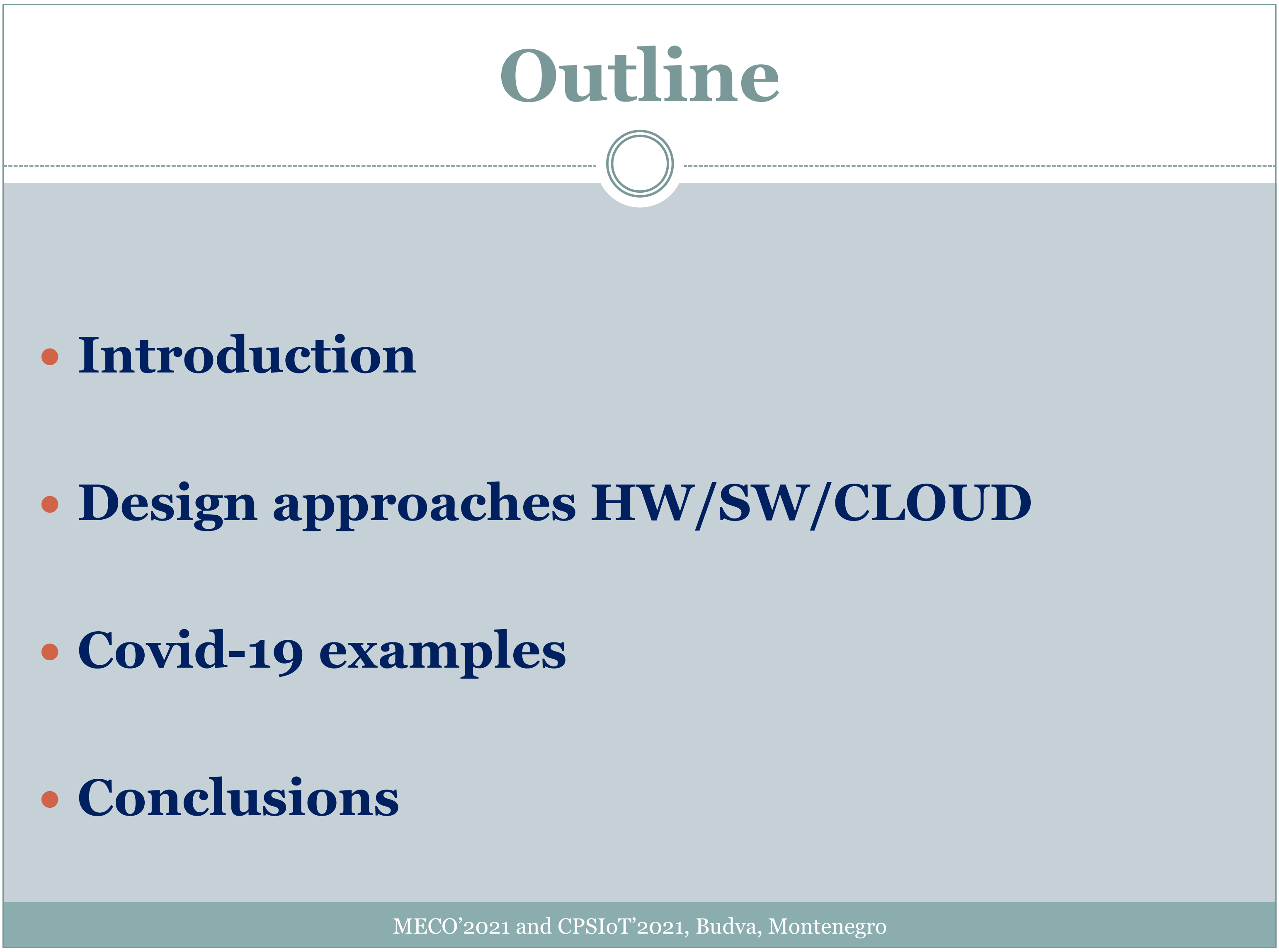
- Safety and security dependence
- Continuous and real-time operation of safe and secure ICS
- Lightweight security primitives
- Secure-by-design ICS
- Runtime monitoring
- Resilience (diagnosis and recovery)
- Efficient generic (ICS) fuzz testing

THANK YOU !

Challenging issues in cost effective wearable and IoT medical devices with example to Covid19

RADOVAN STOJANOVIĆ
UNIVERSITY OF MONTENEGRO AND MECONET
MONTENEGRO

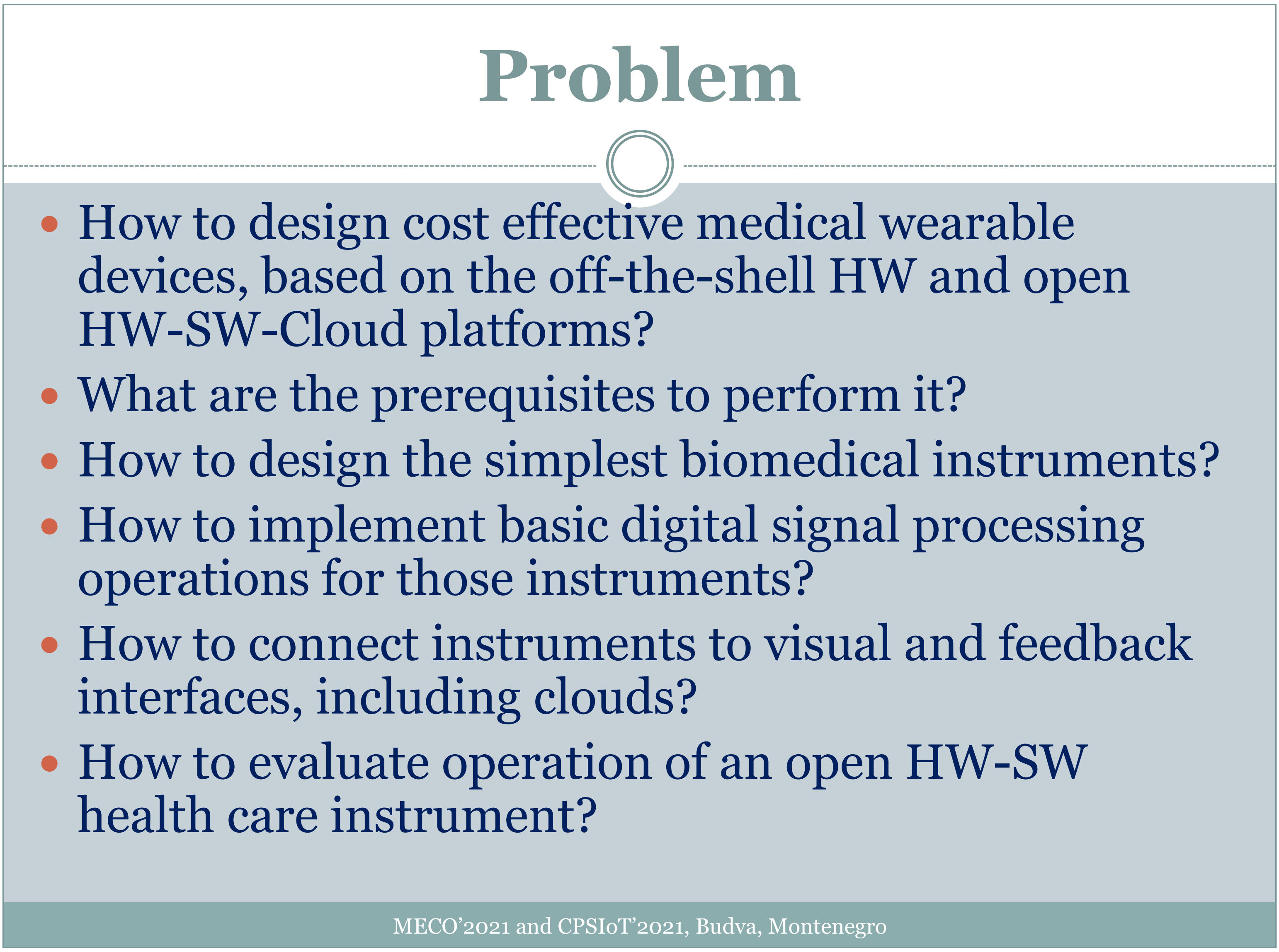
Presented at 2nd Summer Scholl on CPSIoT'2021, Budva, Montenegro
www.embeddedcomputing.me



Outline

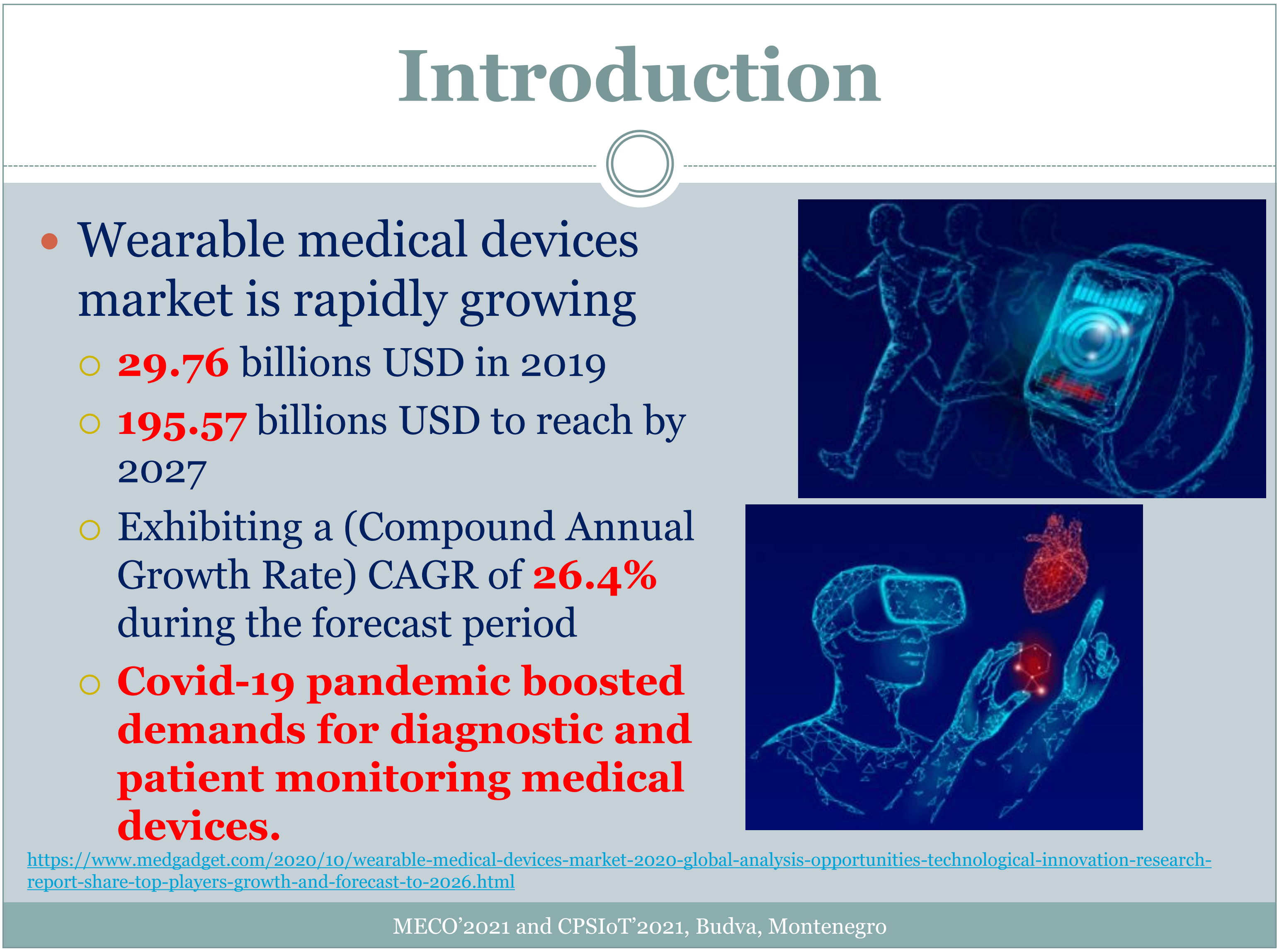
- Introduction
- Design approaches HW/SW/CLOUD
- Covid-19 examples
- Conclusions

MECO'2021 and CPSIoT'2021, Budva, Montenegro



Problem

- How to design cost effective medical wearable devices, based on the off-the-shell HW and open HW-SW-Cloud platforms?
- What are the prerequisites to perform it?
- How to design the simplest biomedical instruments?
- How to implement basic digital signal processing operations for those instruments?
- How to connect instruments to visual and feedback interfaces, including clouds?
- How to evaluate operation of an open HW-SW health care instrument?

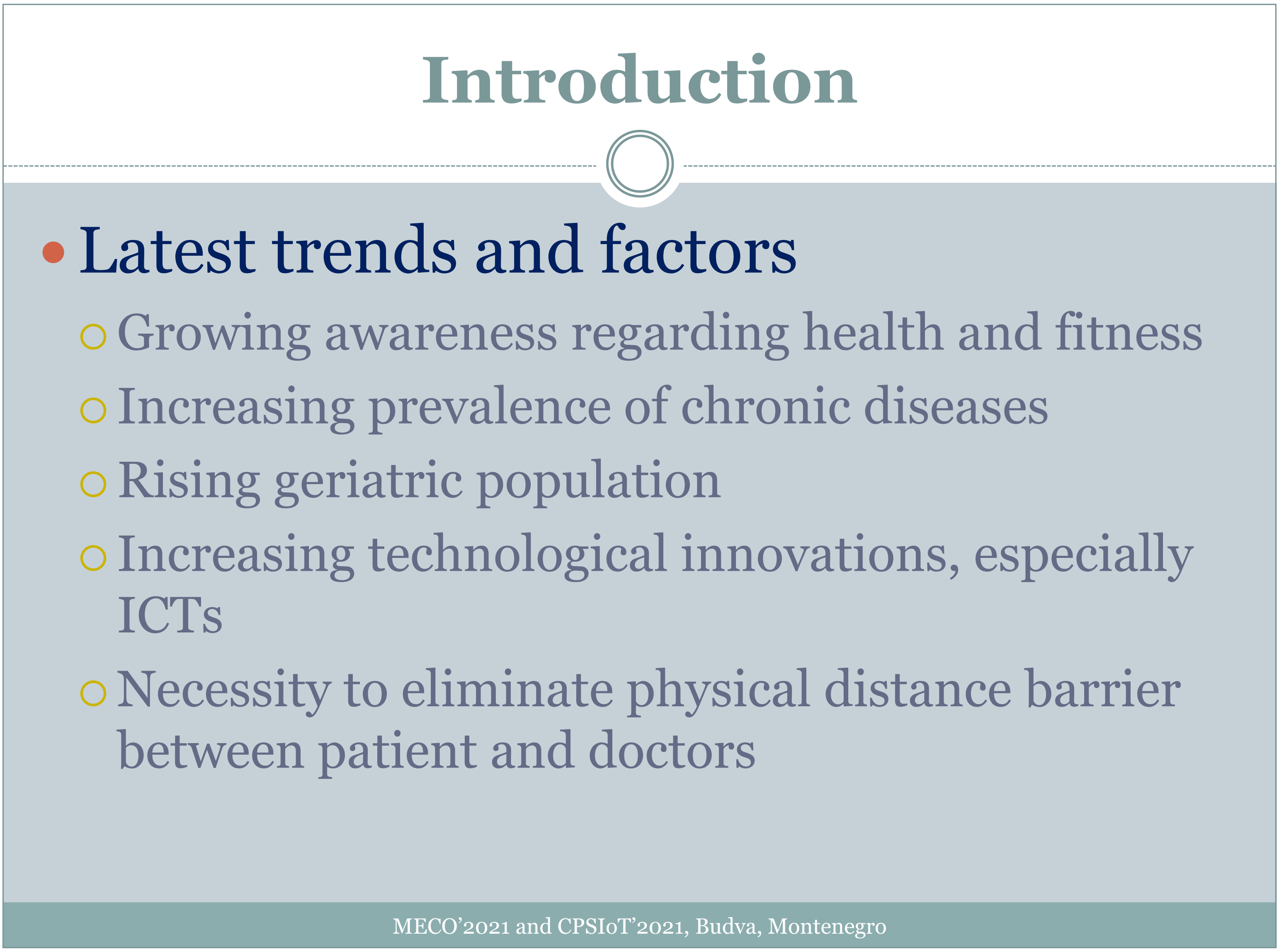


Introduction

- Wearable medical devices market is rapidly growing
  - **29.76** billions USD in 2019
  - **195.57** billions USD to reach by 2027
  - Exhibiting a (Compound Annual Growth Rate) CAGR of **26.4%** during the forecast period
  - **Covid-19 pandemic boosted demands for diagnostic and patient monitoring medical devices.**

https://www.medgadget.com/2020/10/wearable-medical-devices-market-2020-global-analysis-opportunities-technological-innovation-research-report-share-top-players-growth-and-forecast-to-2026.html

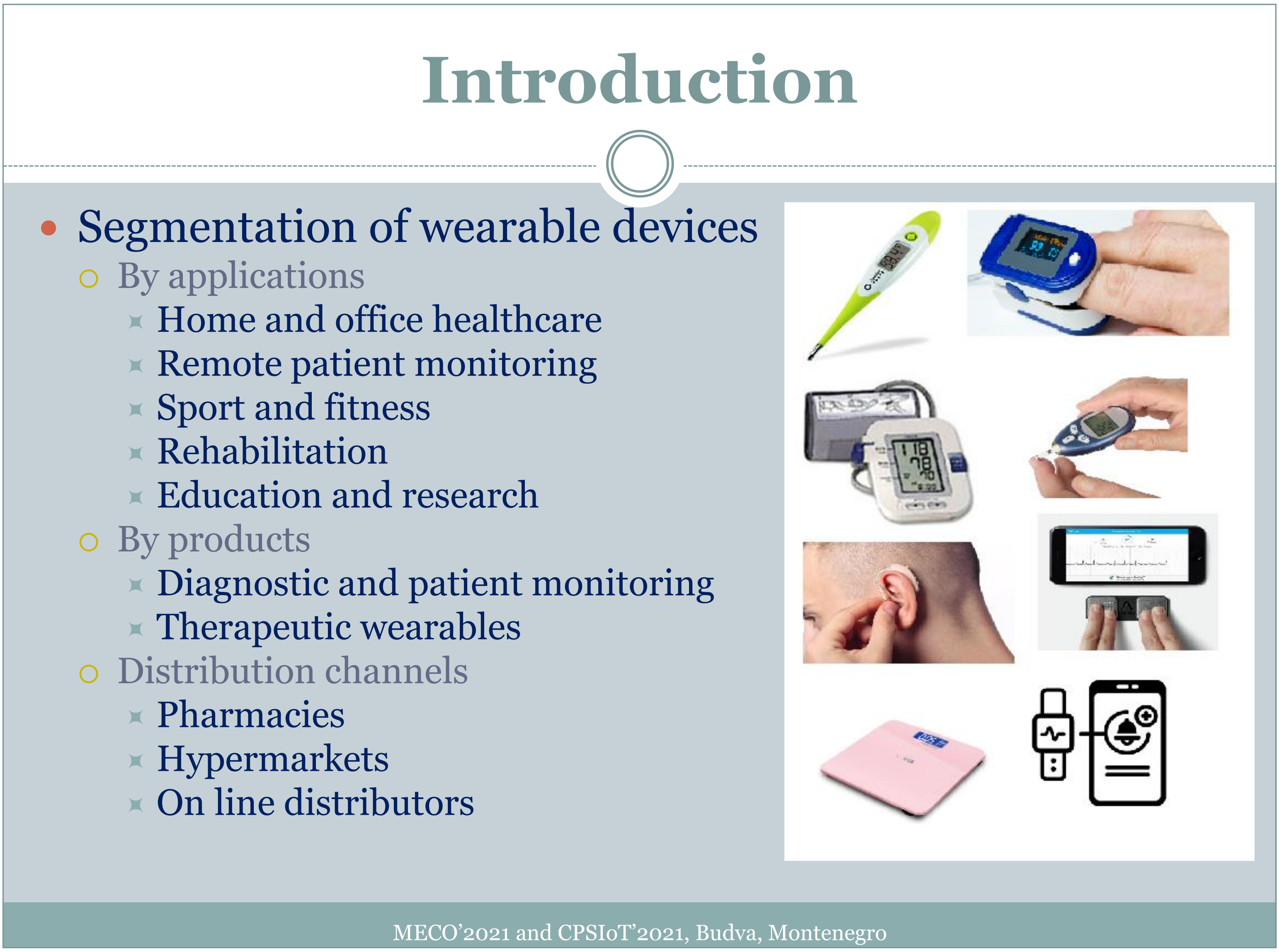
MECO'2021 and CPSIoT'2021, Budva, Montenegro



Introduction

- Latest trends and factors
  - Growing awareness regarding health and fitness
  - Increasing prevalence of chronic diseases
  - Rising geriatric population
  - Increasing technological innovations, especially ICTs
  - Necessity to eliminate physical distance barrier between patient and doctors

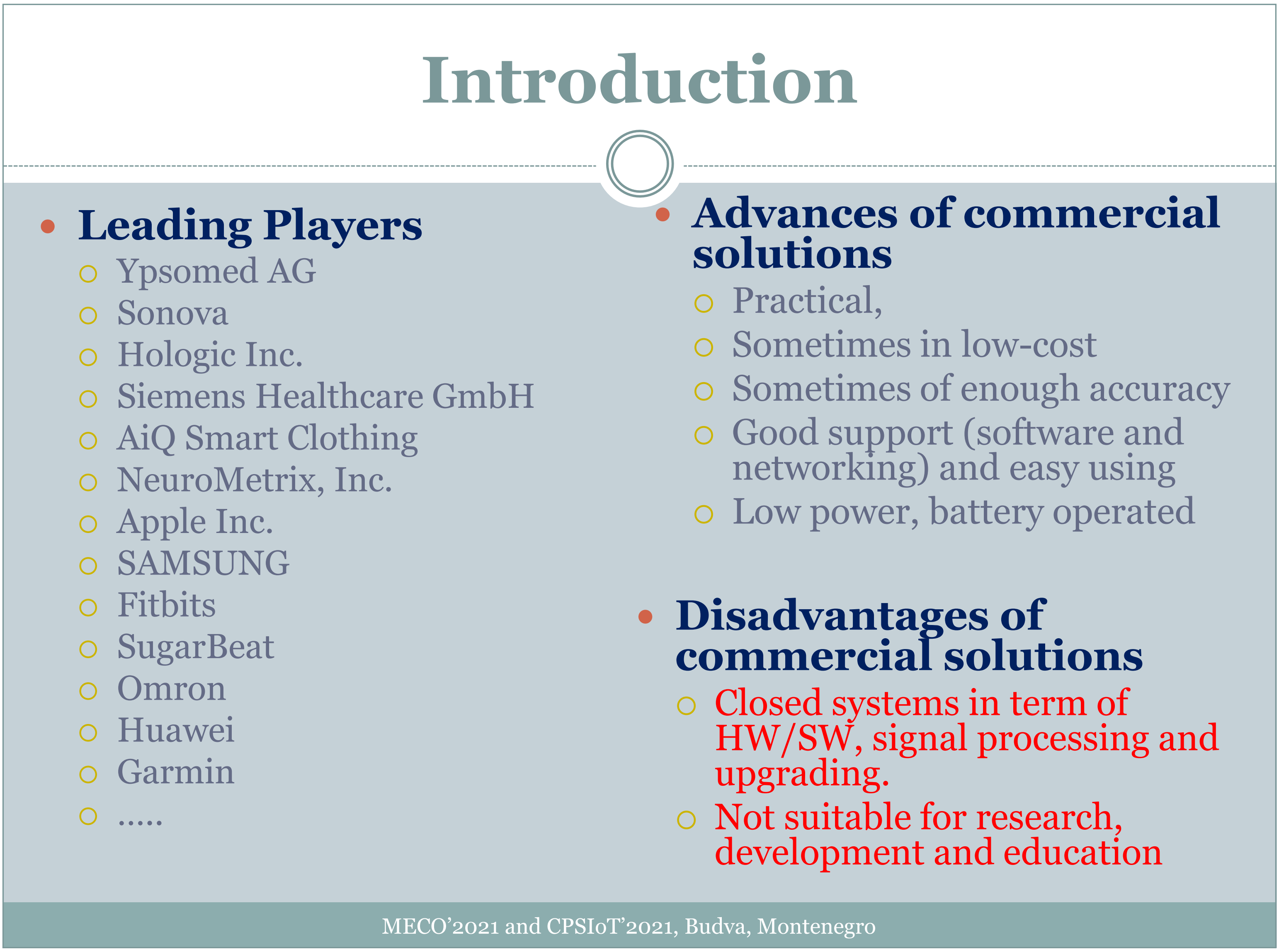
MECO'2021 and CPSIoT'2021, Budva, Montenegro



Introduction

- Segmentation of wearable devices
  - By applications
    - Home and office healthcare
    - Remote patient monitoring
    - Sport and fitness
    - Rehabilitation
    - Education and research
  - By products
    - Diagnostic and patient monitoring
    - Therapeutic wearables
  - Distribution channels
    - Pharmacies
    - Hypermarkets
    - On line distributors

MECO'2021 and CPSIoT'2021, Budva, Montenegro

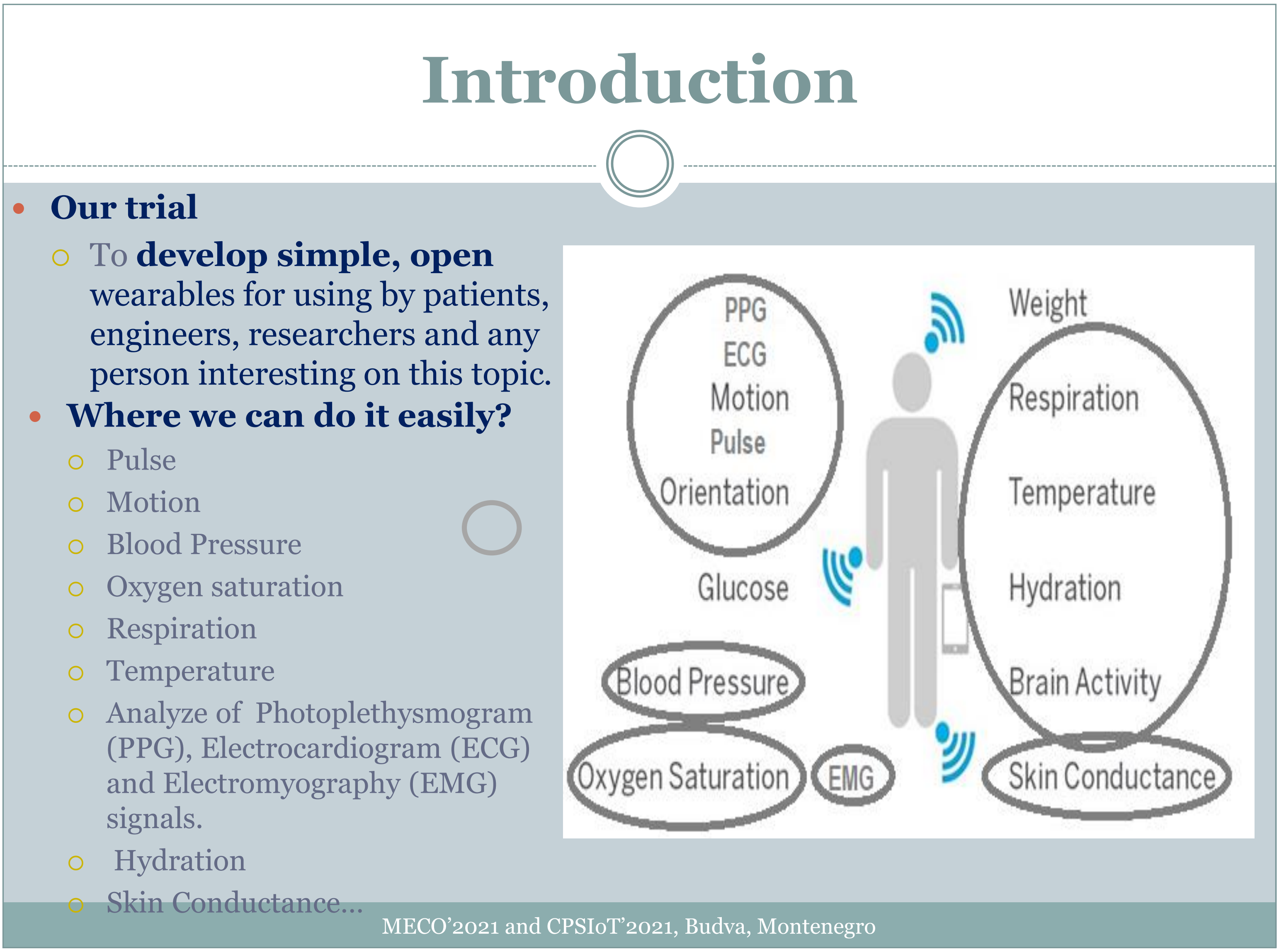


Introduction

- **Leading Players**
  - Ypsomed AG
  - Sonova
  - Hologic Inc.
  - Siemens Healthcare GmbH
  - AiQ Smart Clothing
  - NeuroMetrix, Inc.
  - Apple Inc.
  - SAMSUNG
  - Fitbits
  - SugarBeat
  - Omron
  - Huawei
  - Garmin
  - …..

- **Advances of commercial solutions**
  - Practical,
  - Sometimes in low-cost
  - Sometimes of enough accuracy
  - Good support (software and networking) and easy using
  - Low power, battery operated

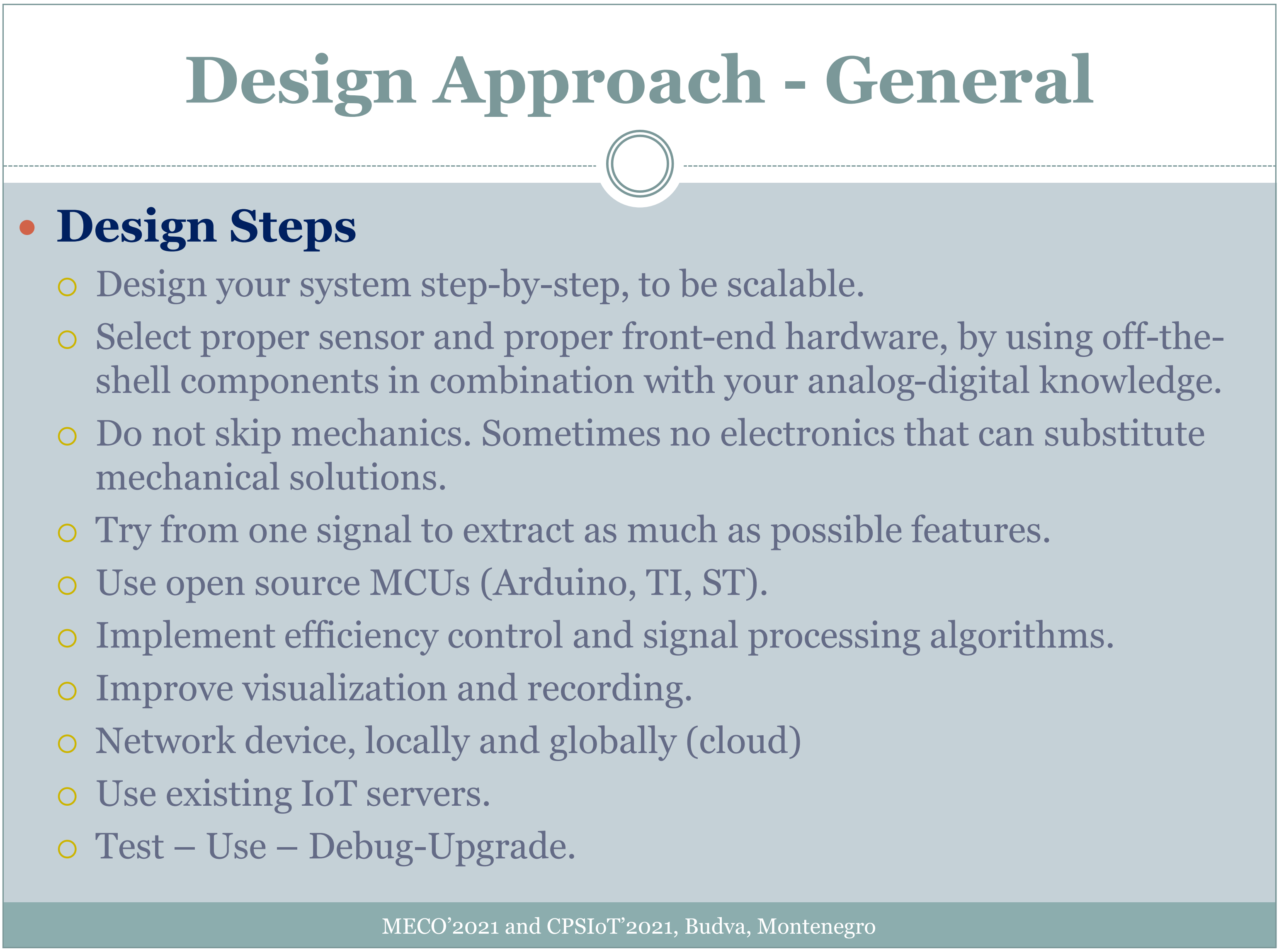
- **Disadvantages of commercial solutions**
  - Closed systems in term of HW/SW, signal processing and upgrading.
  - Not suitable for research, development and education



Introduction

- **Our trial**
  - To **develop simple, open** wearables for using by patients, engineers, researchers and any person interesting on this topic.
- **Where we can do it easily?**
  - Pulse
  - Motion
  - Blood Pressure
  - Oxygen saturation
  - Respiration
  - Temperature
  - Analyze of Photoplethysmogram (PPG), Electrocardiogram (ECG) and Electromyography (EMG) signals.
  - Hydration
  - Skin Conductance...

MECO'2021 and CPSIoT'2021, Budva, Montenegro



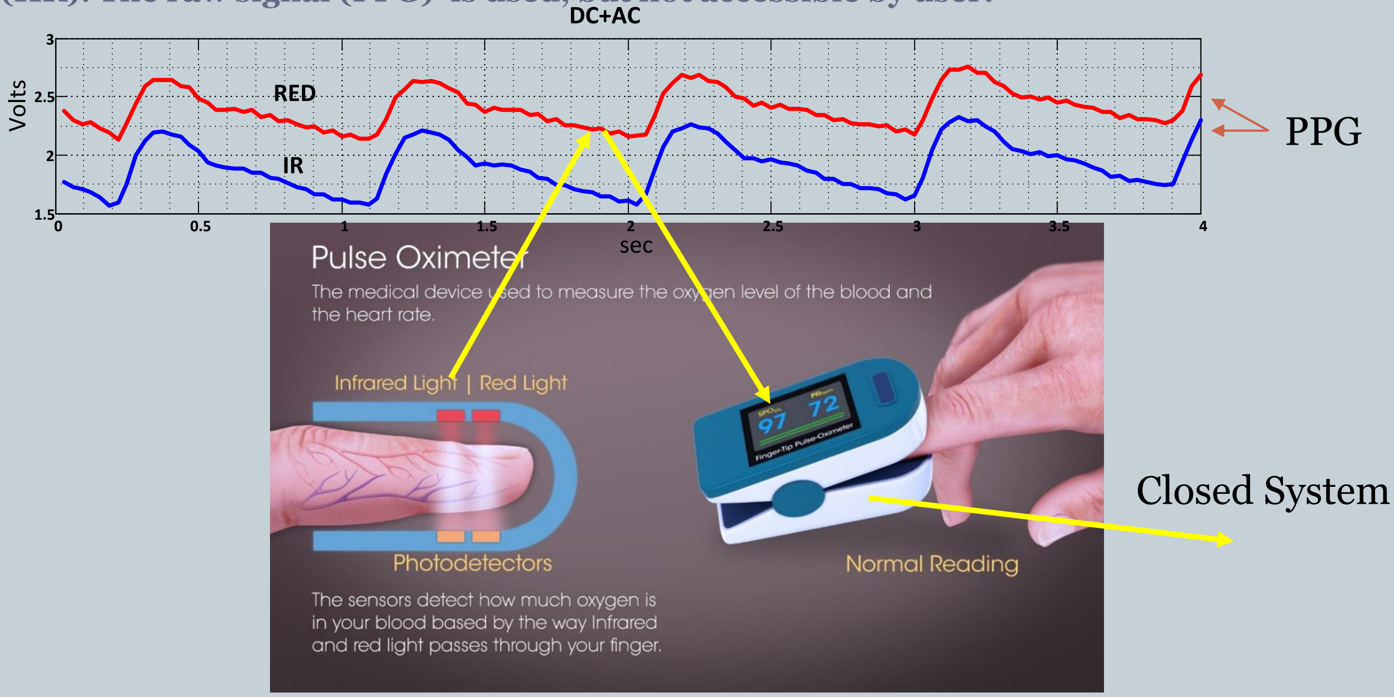
Design Approach - General

- **Design Steps**
  - Design your system step-by-step, to be scalable.
  - Select proper sensor and proper front-end hardware, by using off-the-shell components in combination with your analog-digital knowledge.
  - Do not skip mechanics. Sometimes no electronics that can substitute mechanical solutions.
  - Try from one signal to extract as much as possible features.
  - Use open source MCUs (Arduino, TI, ST).
  - Implement efficiency control and signal processing algorithms.
  - Improve visualization and recording.
  - Network device, locally and globally (cloud)
  - Use existing IoT servers.
  - Test – Use – Debug-Upgrade.

MECO'2021 and CPSIoT'2021, Budva, Montenegro

Design Approach - General

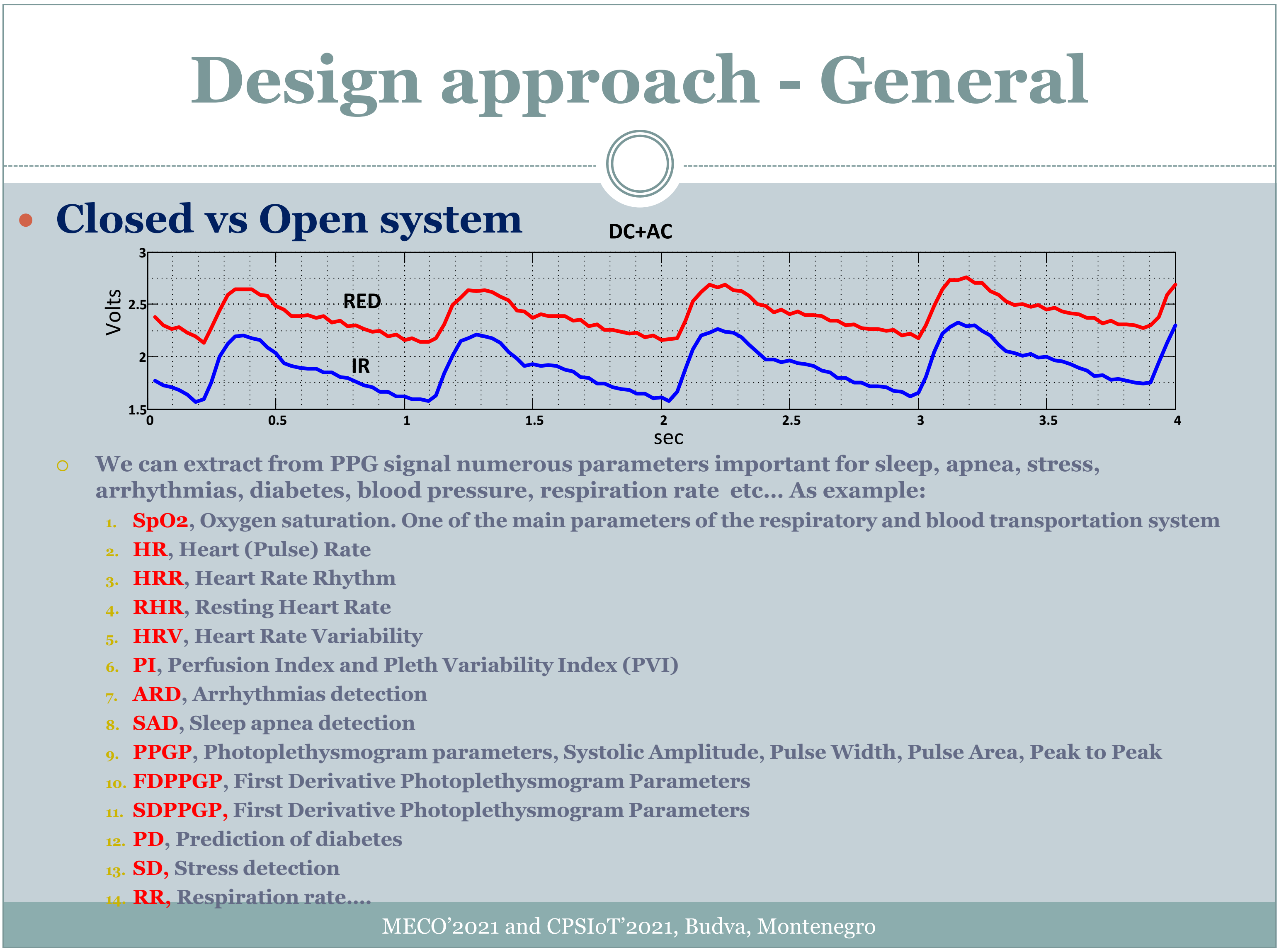
- **Example. Pulse oximetry from PPG - closed system**
  - **Commercial wearable, acquires and displays Oxygen Saturation (SpO2) and Pulse (HR). The raw signal (PPG) is used, but not accessible by user.**



The medical device used to measure the oxygen level of the blood and the heart rate.

The sensors detect how much oxygen is in your blood based by the way Infrared and red light passes through your finger.

https://www.scientificanimations.com/pulse-oximetry-mechanism-history-use-sources/



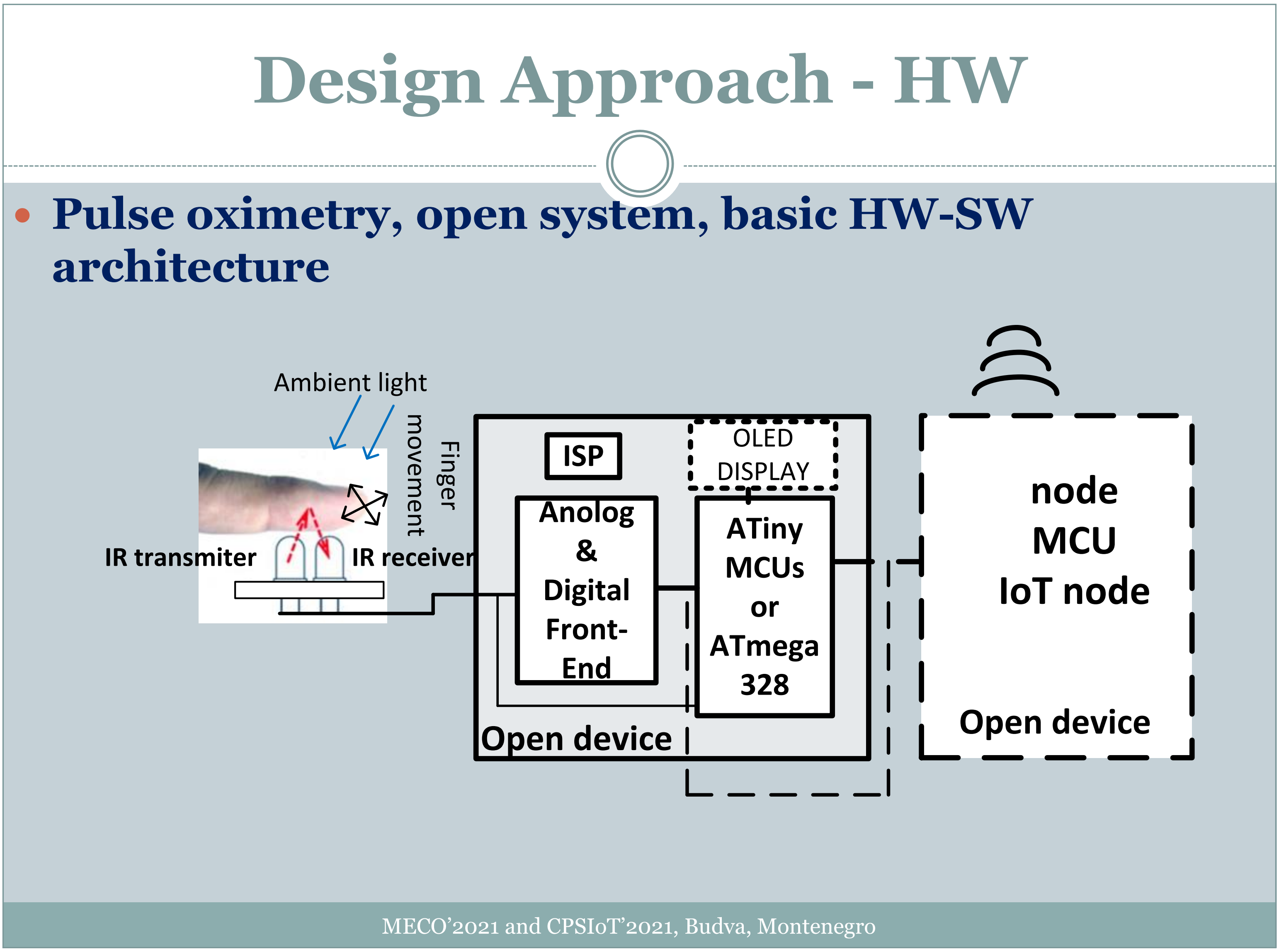
Design approach - General

- **Closed vs Open system**

DC+AC
Volts
3
2.5
2
1.5
RED
IR
0
0.5
1
1.5
2
2.5
3
3.5
4
sec

- We can extract from PPG signal numerous parameters important for sleep, apnea, stress, arrhythmias, diabetes, blood pressure, respiration rate etc… As example:
  1. **SpO2**, Oxygen saturation. One of the main parameters of the respiratory and blood transportation system
  2. **HR**, Heart (Pulse) Rate
  3. **HRR**, Heart Rate Rhythm
  4. **RHR**, Resting Heart Rate
  5. **HRV**, Heart Rate Variability
  6. **PI**, Perfusion Index and Pleth Variability Index (PVI)
  7. **ARD**, Arrhythmias detection
  8. **SAD**, Sleep apnea detection
  9. **PPGP**, Photoplethysmogram parameters, Systolic Amplitude, Pulse Width, Pulse Area, Peak to Peak
  10. **FDPPGP**, First Derivative Photoplethysmogram Parameters
  11. **SDPPGP**, First Derivative Photoplethysmogram Parameters
  12. **PD**, Prediction of diabetes
  13. **SD,** Stress detection
  14. **RR,** Respiration rate….

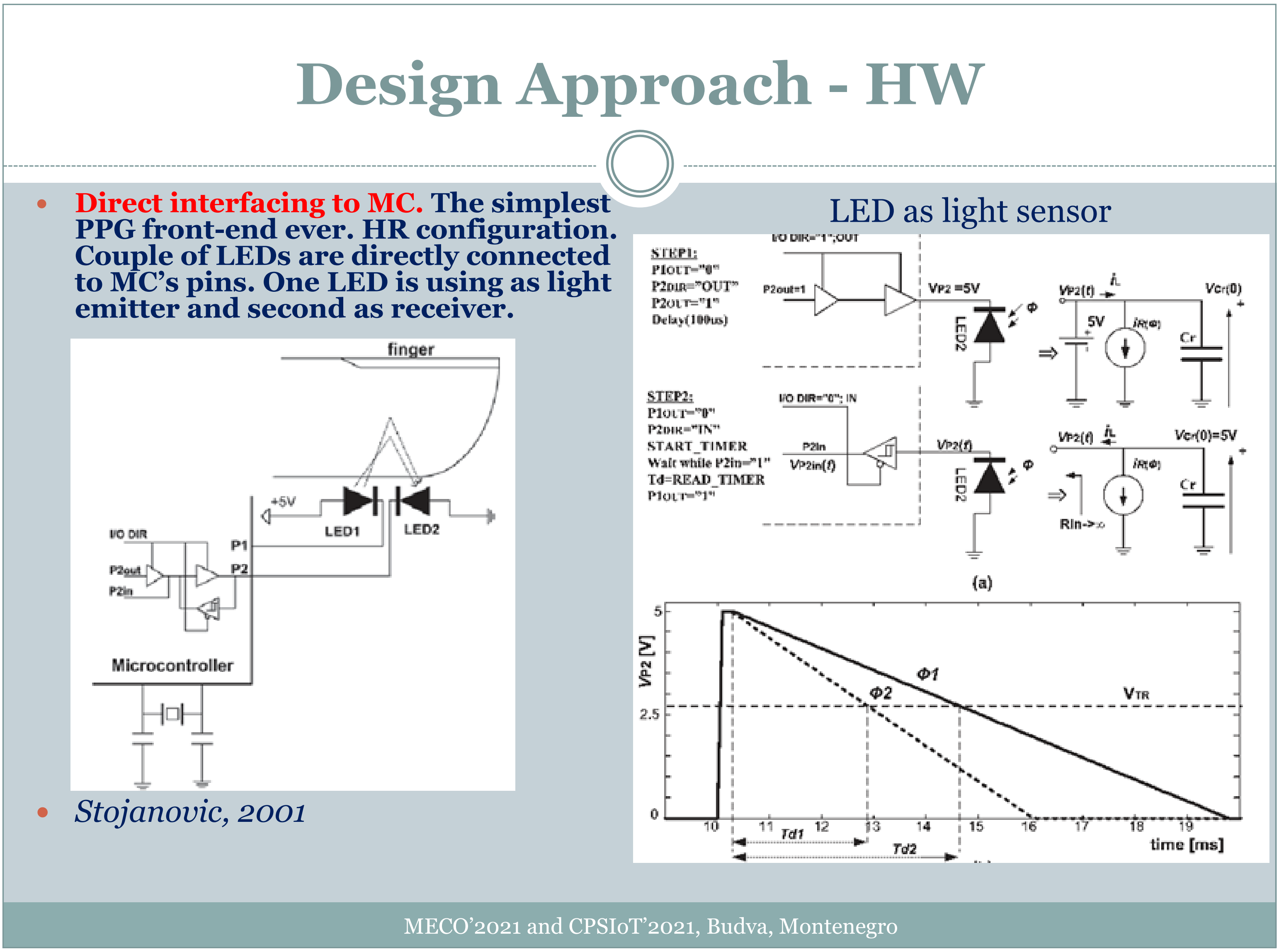
MECO'2021 and CPSIoT'2021, Budva, Montenegro



Design Approach - HW

- **Pulse oximetry, open system, basic HW-SW architecture**

MECO'2021 and CPSIoT'2021, Budva, Montenegro



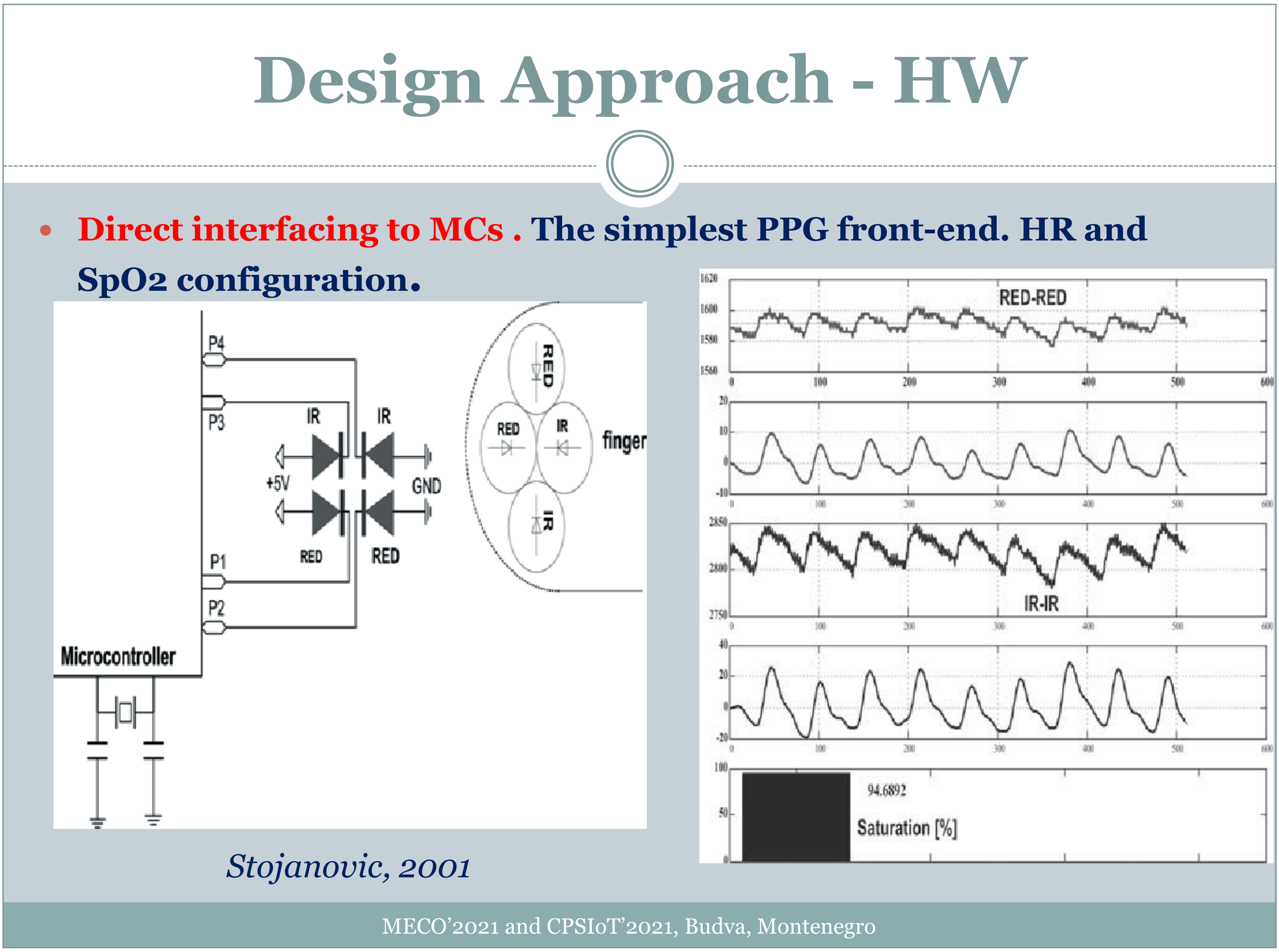
Design Approach - HW

- **Direct interfacing to MC. The simplest PPG front-end ever. HR configuration. Couple of LEDs are directly connected to MC's pins. One LED is using as light emitter and second as receiver.**

LED as light sensor

- *Stojanovic, 2001*

MECO'2021 and CPSIoT'2021, Budva, Montenegro



Design Approach - HW

- **Direct interfacing to MCs . The simplest PPG front-end. HR and SpO2 configuration.**

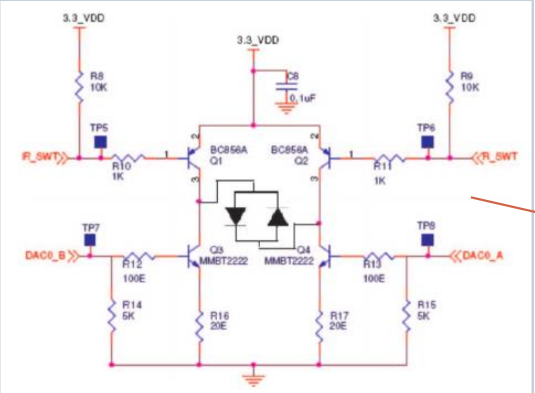
P4
P3
P1
P2
IR
IR
+5V
GND
RED
RED
Microcontroller
RED
RED
IR
IR
finger
RED-RED
IR-IR
1620
1600
1580
1560
20
10
0
-10
2850
2800
2750
40
20
0
-20
100
50
0
100
200
300
400
500
600
94.6892
Saturation [%]

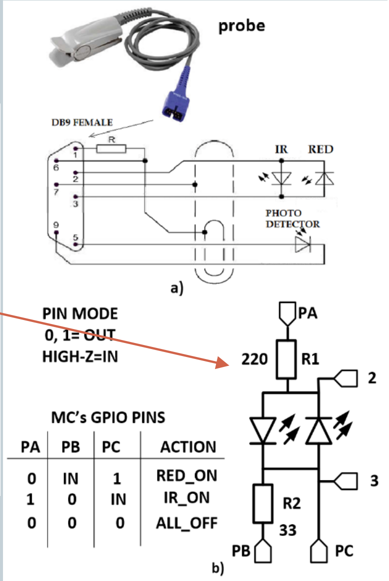
Stojanovic, 2001

MECO'2021 and CPSIoT'2021, Budva, Montenegro

Design Approach - HW

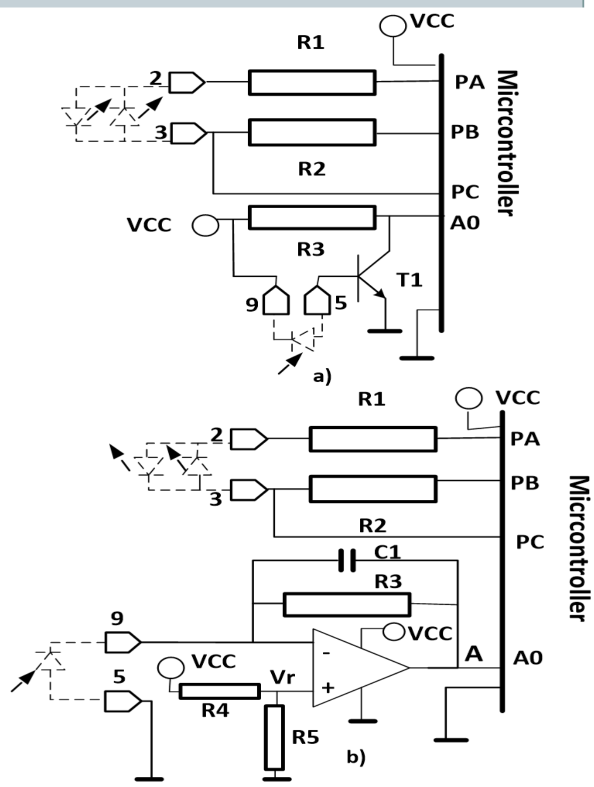
- **Minimal interfacing. HR, SpO2 sensing by factory probe and MC**. Classical LED driving implemented by transistor bridge and intensity control, implemented by DACs are replaced by 3 MC pins and 2 resistors. As receiver, one transistor amplifier and one OA are used. *Stojanovic and Skraba 2020*

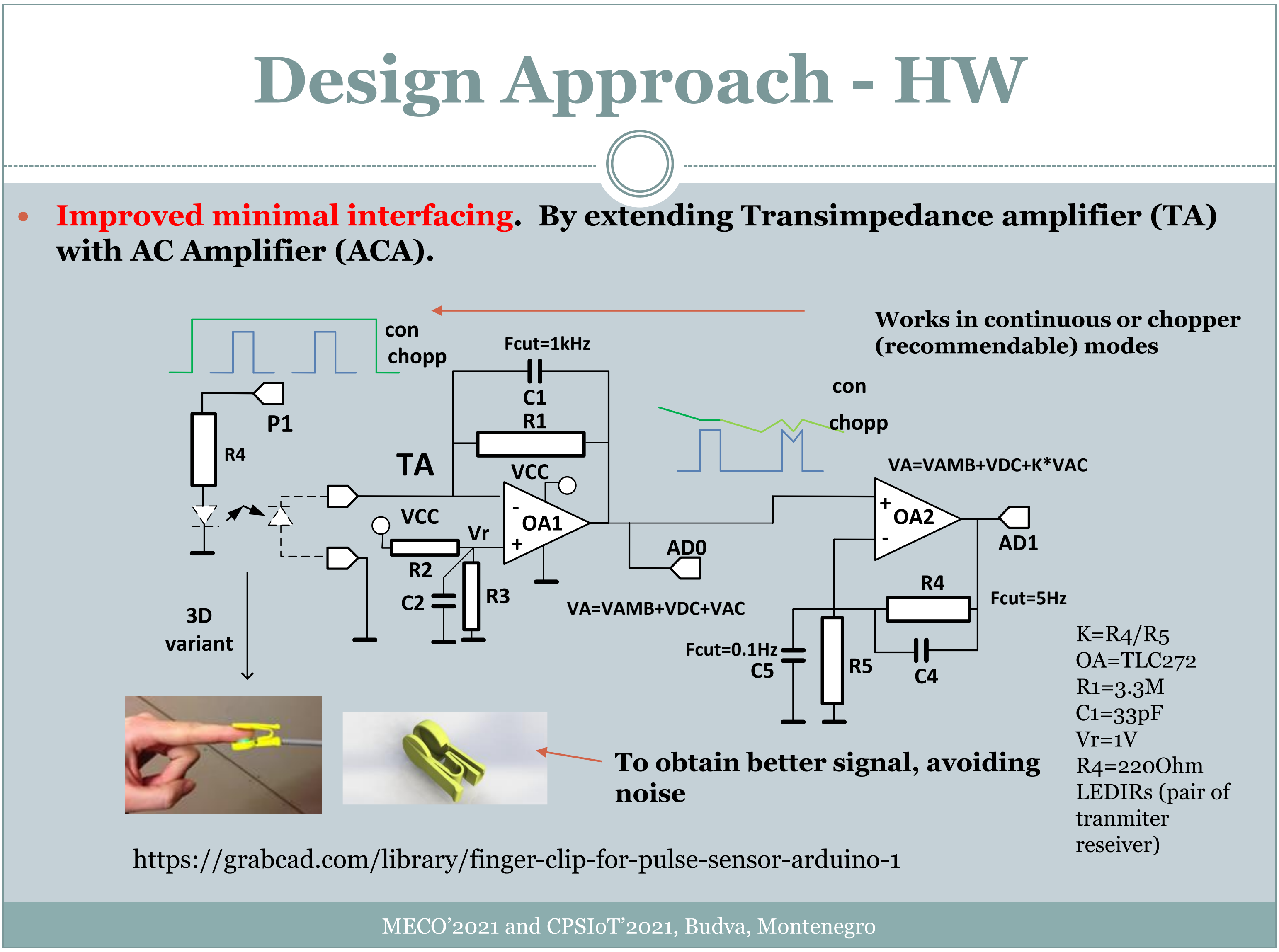




MC's GPIO PINS

PA	PB	PC	ACTION
0	IN	1	RED_ON
1	0	IN	IR_ON
0	0	0	ALL_OFF





Design Approach - HW

- Improved minimal interfacing. By extending Transimpedance amplifier (TA) with AC Amplifier (ACA).

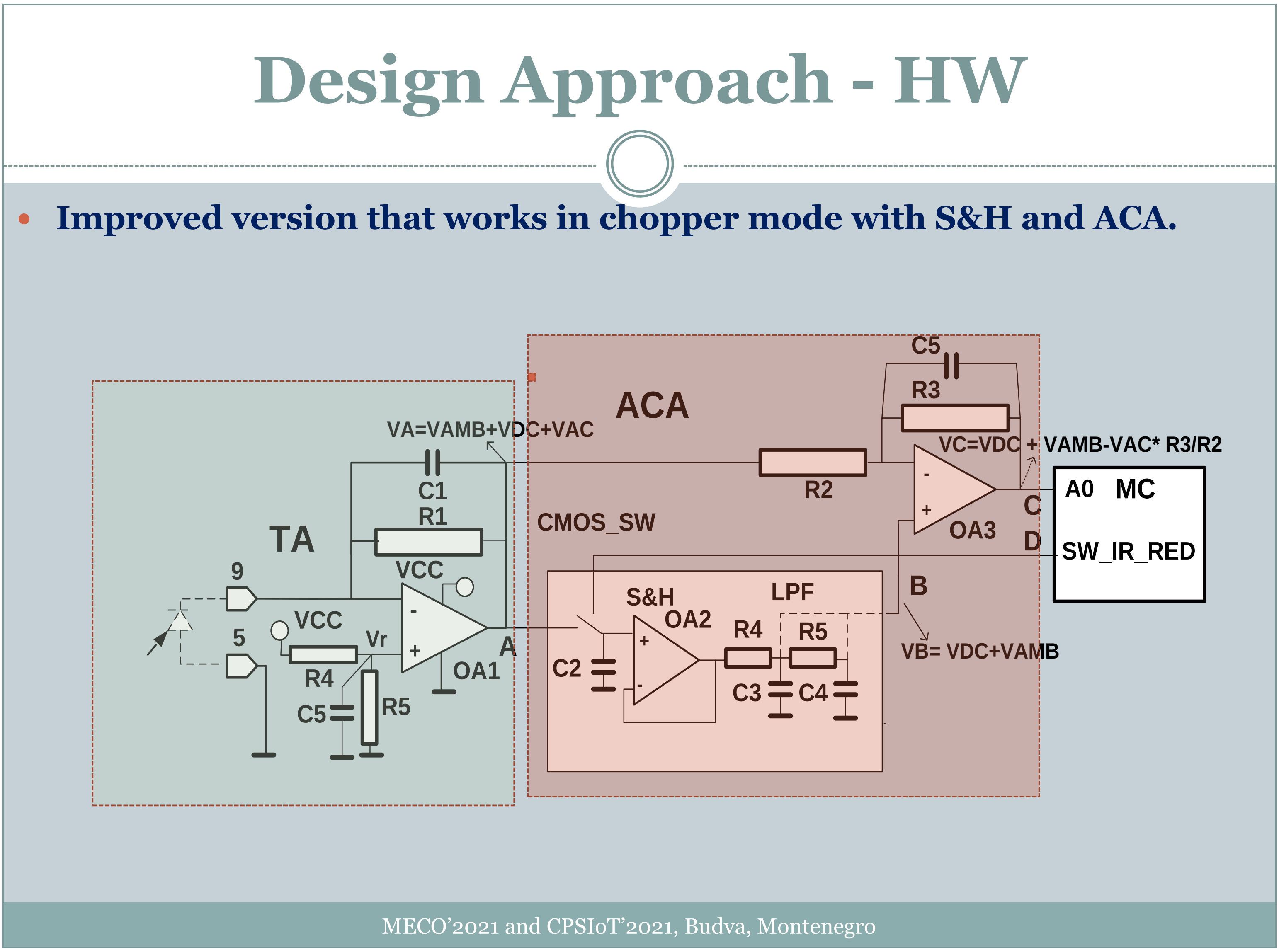
Works in continuous or chopper (recommendable) modes

To obtain better signal, avoiding noise

K=R4/R5
OA=TLC272
R1=3.3M
C1=33pF
Vr=1V
R4=220Ohm
LEDIRs (pair of tranmiter reseiver)

https://grabcad.com/library/finger-clip-for-pulse-sensor-arduino-1

MECO'2021 and CPSIoT'2021, Budva, Montenegro



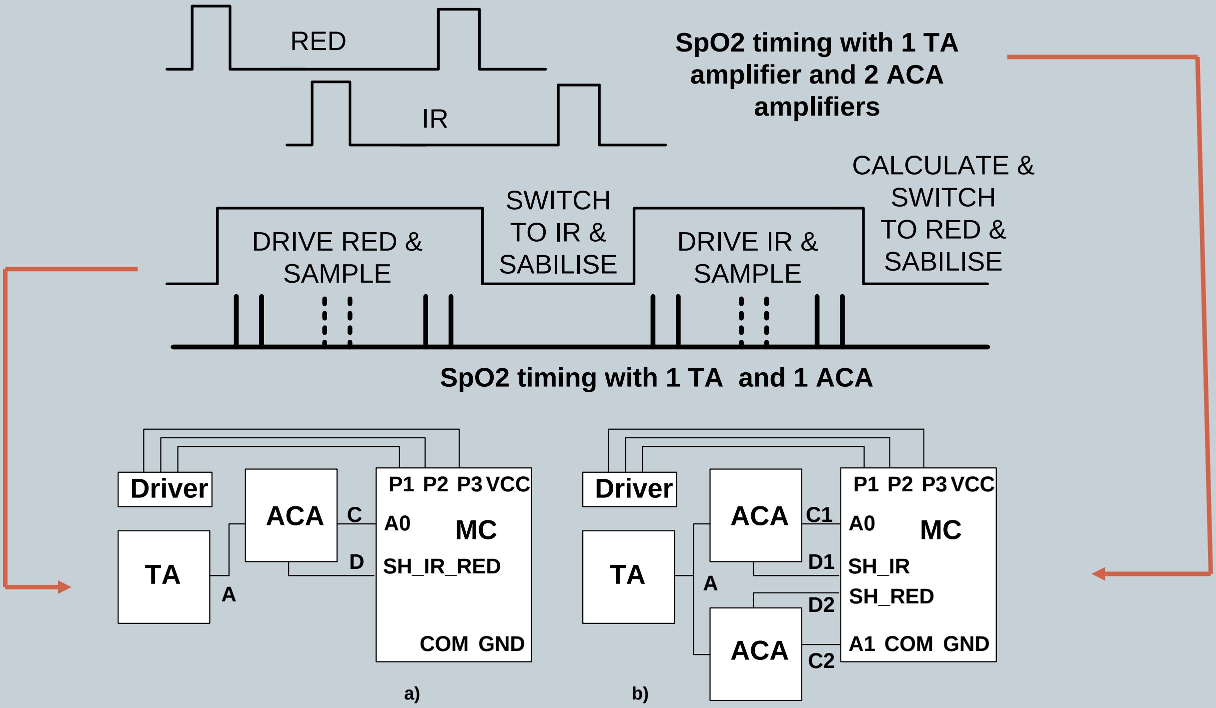
Design Approach - HW

- **Improved version that works in chopper mode with S&H and ACA.**

MECO'2021 and CPSIoT'2021, Budva, Montenegro

Design Approach - HW

- By proper timing one TA and one ACA can be used for acquiring both IR and RED channels, or it can be done by one TA and two ACAs.

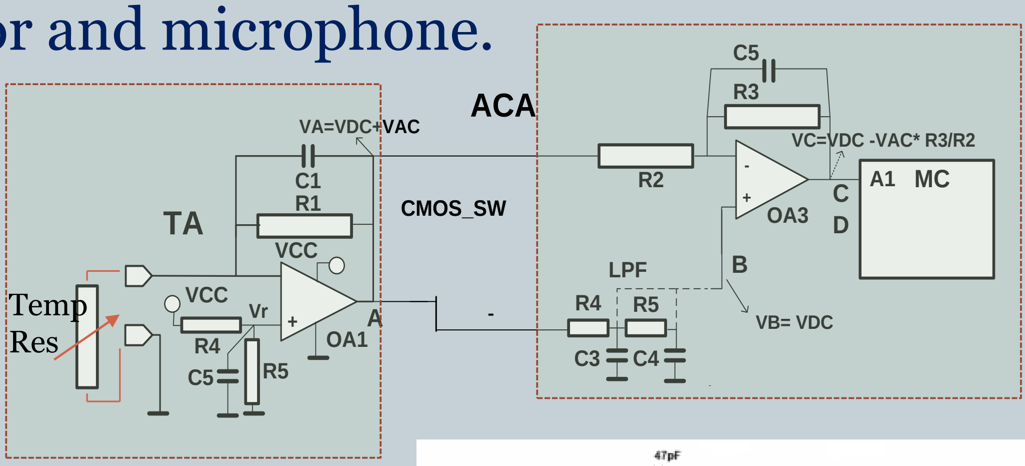


MECO'2021 and CPSIoT'2021, Budva, Montenegro

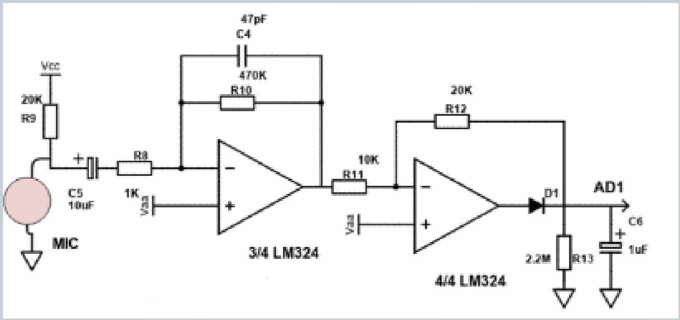
Design Approach - HW

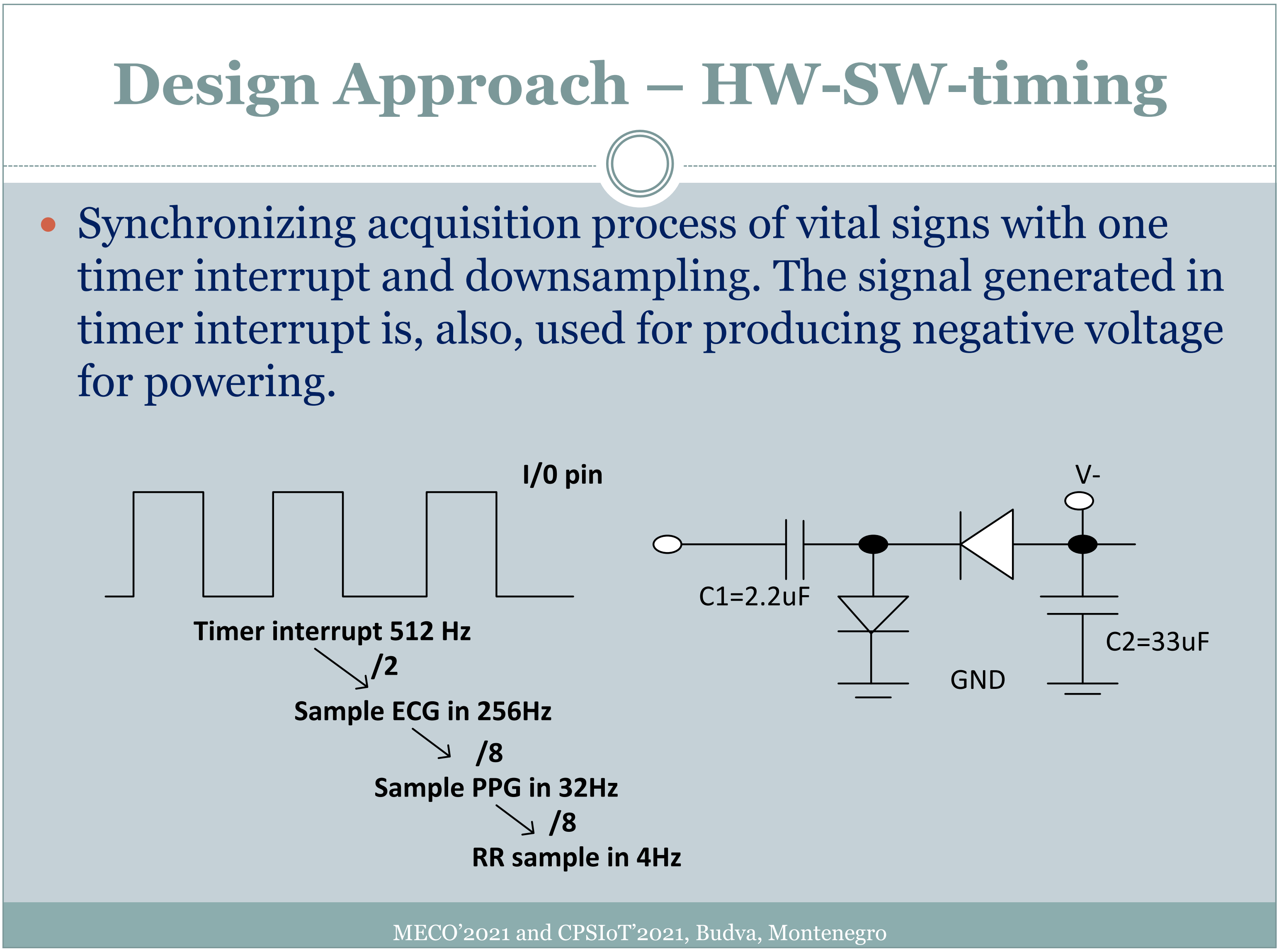
- Respiration ration (RR) amplifier based on thermistor and microphone.

inhale
exhale



inhale
exhale





Design Approach – HW-SW-timing

- Synchronizing acquisition process of vital signs with one timer interrupt and downsampling. The signal generated in timer interrupt is, also, used for producing negative voltage for powering.

Timer interrupt 512 Hz

/2

Sample ECG in 256Hz

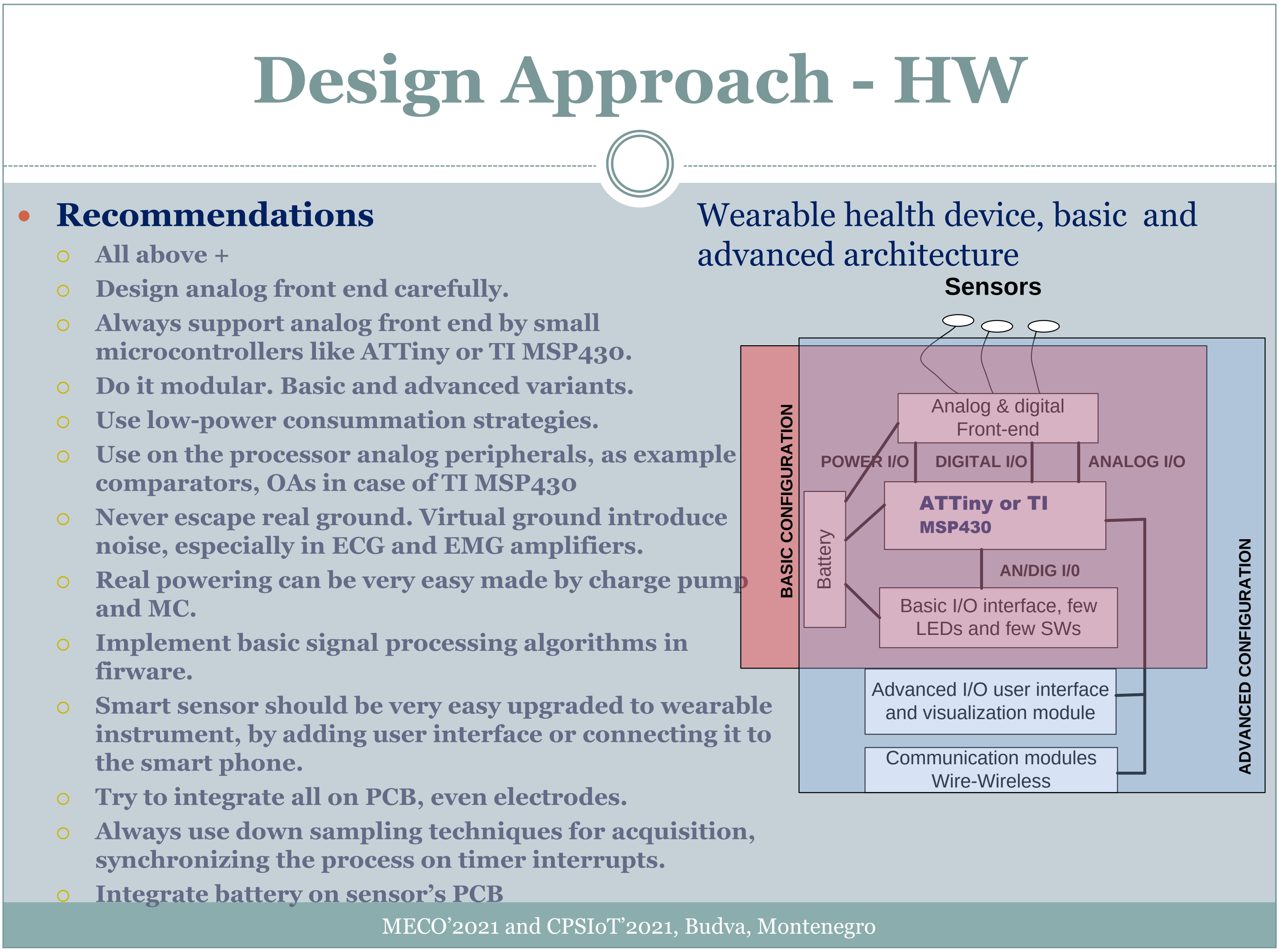
/8

Sample PPG in 32Hz

/8

RR sample in 4Hz

MECO'2021 and CPSIoT'2021, Budva, Montenegro



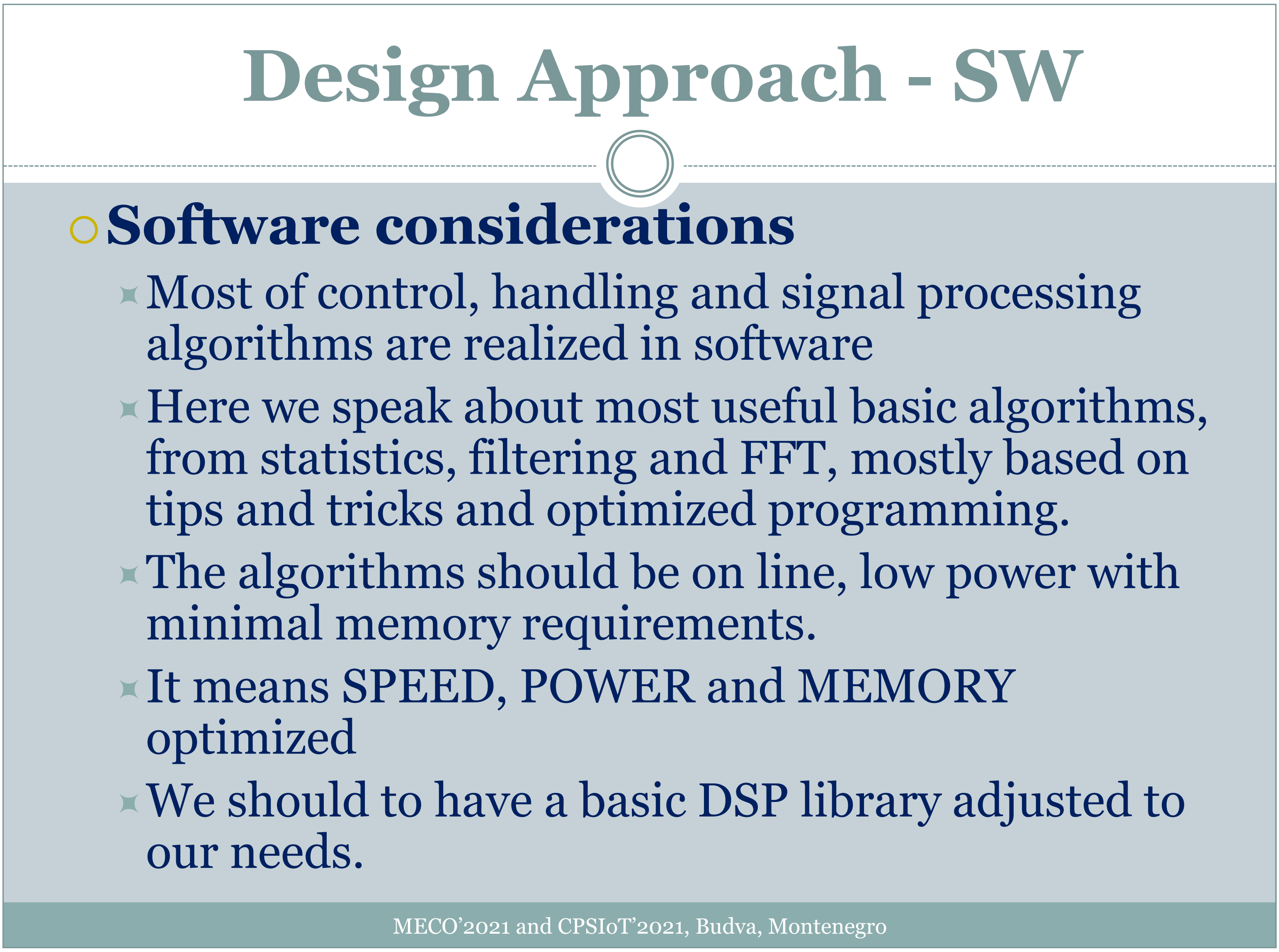
Design Approach - HW

- **Recommendations**
  - All above +
  - Design analog front end carefully.
  - Always support analog front end by small microcontrollers like ATTiny or TI MSP430.
  - Do it modular. Basic and advanced variants.
  - Use low-power consummation strategies.
  - Use on the processor analog peripherals, as example comparators, OAs in case of TI MSP430
  - Never escape real ground. Virtual ground introduce noise, especially in ECG and EMG amplifiers.
  - Real powering can be very easy made by charge pump and MC.
  - Implement basic signal processing algorithms in firware.
  - Smart sensor should be very easy upgraded to wearable instrument, by adding user interface or connecting it to the smart phone.
  - Try to integrate all on PCB, even electrodes.
  - Always use down sampling techniques for acquisition, synchronizing the process on timer interrupts.
  - Integrate battery on sensor's PCB

Wearable health device, basic and advanced architecture

Sensors
BASIC CONFIGURATION
Analog & digital Front-end
POWER I/O
DIGITAL I/O
ANALOG I/O
Battery
ATTiny or TI MSP430
AN/DIG I/0
Basic I/O interface, few LEDs and few SWs
Advanced I/O user interface and visualization module
Communication modules Wire-Wireless
ADVANCED CONFIGURATION

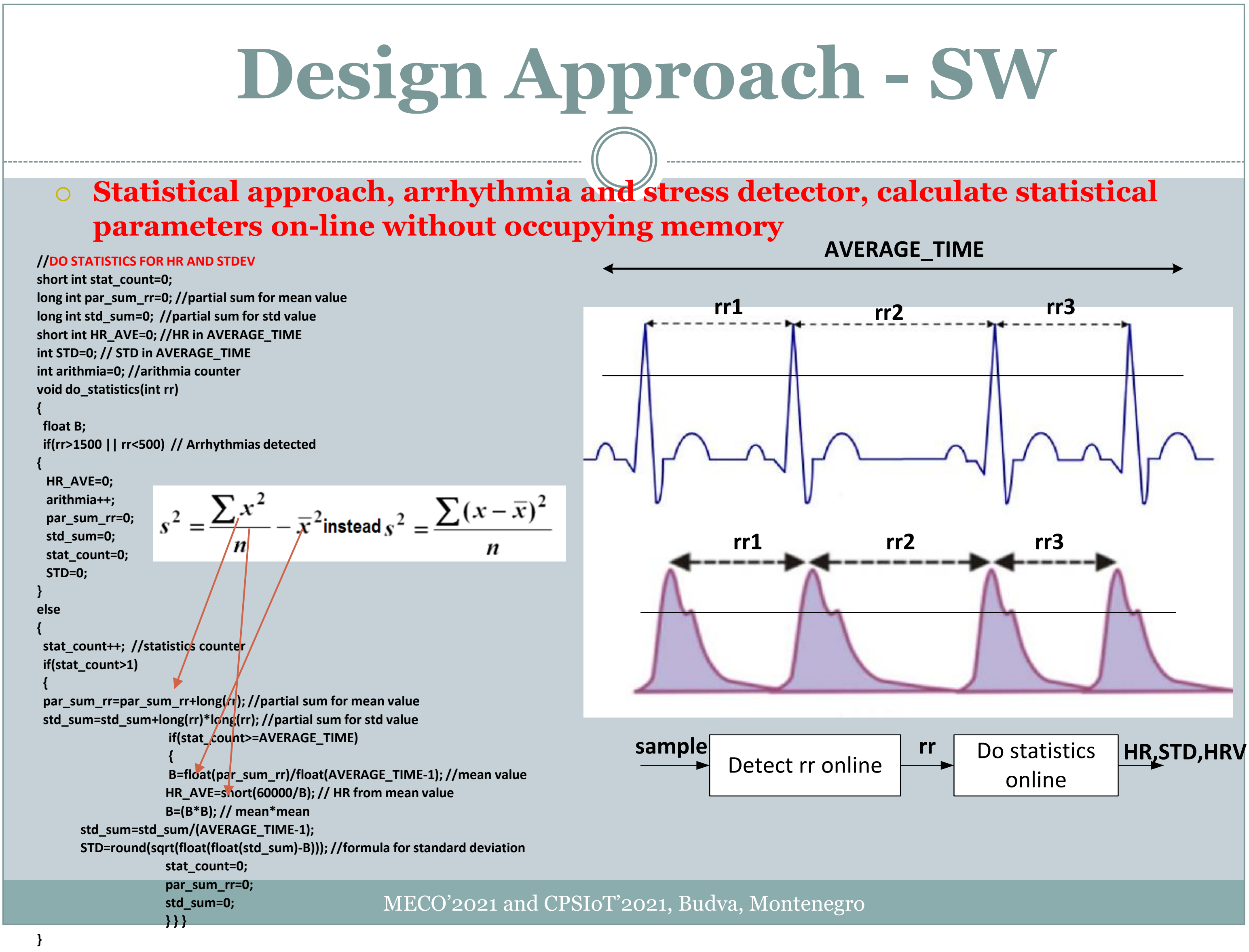
MECO'2021 and CPSIoT'2021, Budva, Montenegro



Design Approach - SW

- **Software considerations**
  - Most of control, handling and signal processing algorithms are realized in software
  - Here we speak about most useful basic algorithms, from statistics, filtering and FFT, mostly based on tips and tricks and optimized programming.
  - The algorithms should be on line, low power with minimal memory requirements.
  - It means SPEED, POWER and MEMORY optimized
  - We should to have a basic DSP library adjusted to our needs.

MECO'2021 and CPSIoT'2021, Budva, Montenegro



Design Approach - SW

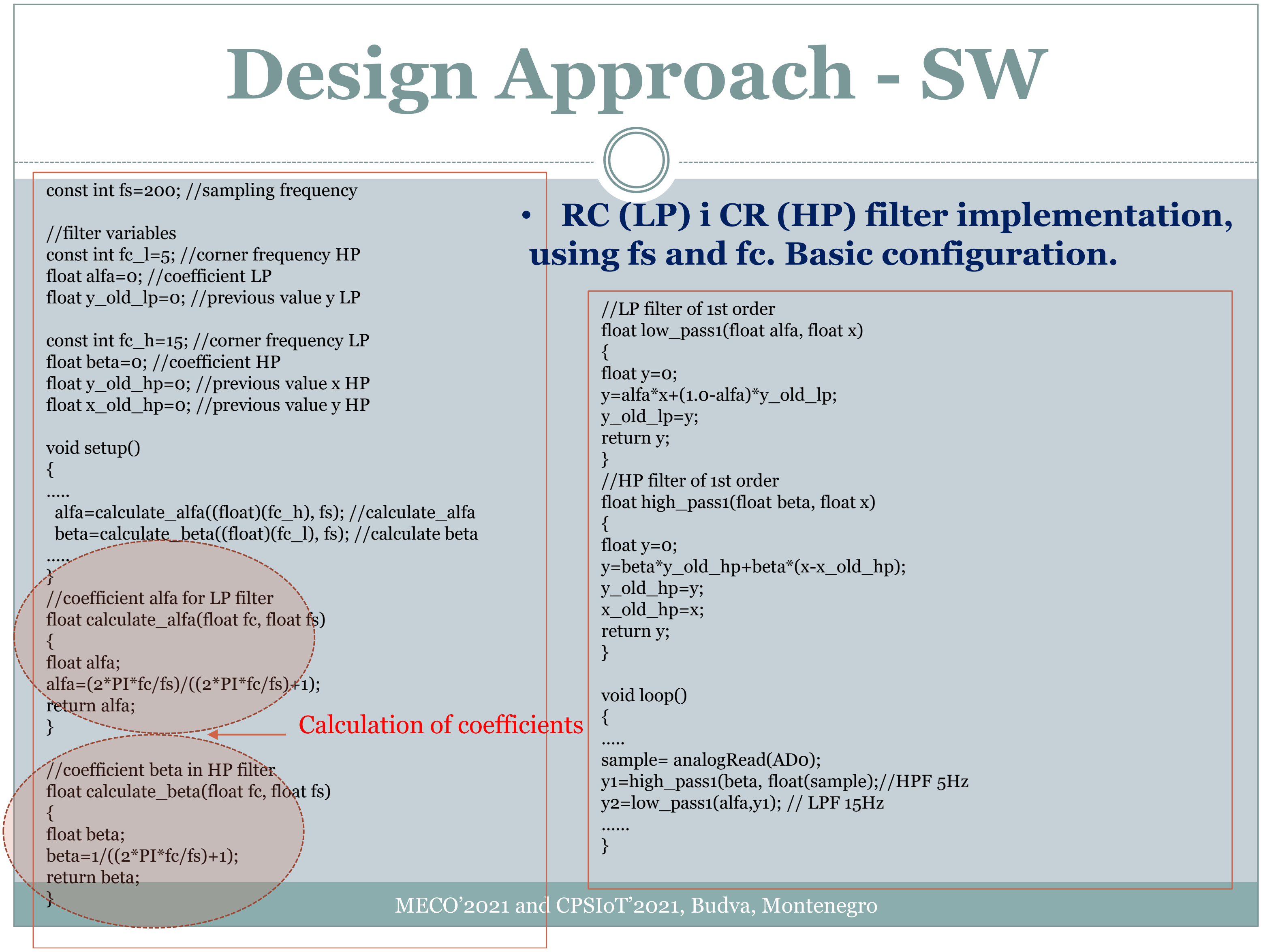
- **Statistical approach, arrhythmia and stress detector, calculate statistical parameters on-line without occupying memory**

```
//DO STATISTICS FOR HR AND STDEV
short int stat_count=0;
long int par_sum_rr=0; //partial sum for mean value
long int std_sum=0;  //partial sum for std value
short int HR_AVE=0; //HR in AVERAGE_TIME
int STD=0; // STD in AVERAGE_TIME
int arithmia=0; //arithmia counter
void do_statistics(int rr)
{
 float B;
 if(rr>1500 || rr<500)  // Arrhythmias detected
{
  HR_AVE=0;
  arithmia++;
  par_sum_rr=0;
  std_sum=0;
  stat_count=0;
  STD=0;
}
else
{
 stat_count++;  //statistics counter
 if(stat_count>1)
 {
 par_sum_rr=par_sum_rr+long(rr); //partial sum for mean value
 std_sum=std_sum+long(rr)*long(rr); //partial sum for std value
                         if(stat_count>=AVERAGE_TIME)
                         {
                         B=float(par_sum_rr)/float(AVERAGE_TIME-1); //mean value
                        HR_AVE=short(60000/B); // HR from mean value
                        B=(B*B); // mean*mean
            std_sum=std_sum/(AVERAGE_TIME-1);
            STD=round(sqrt(float(float(std_sum)-B))); //formula for standard deviation
                        stat_count=0;
                        par_sum_rr=0;
                        std_sum=0;
                        }}}
}
```

$$s^2 = \frac{\sum x^2}{n} - \bar{x}^2 \text{instead } s^2 = \frac{\sum (x-\bar{x})^2}{n}$$

sample → Detect rr online → rr → Do statistics online → HR,STD,HRV

MECO'2021 and CPSIoT'2021, Budva, Montenegro



Design Approach - SW

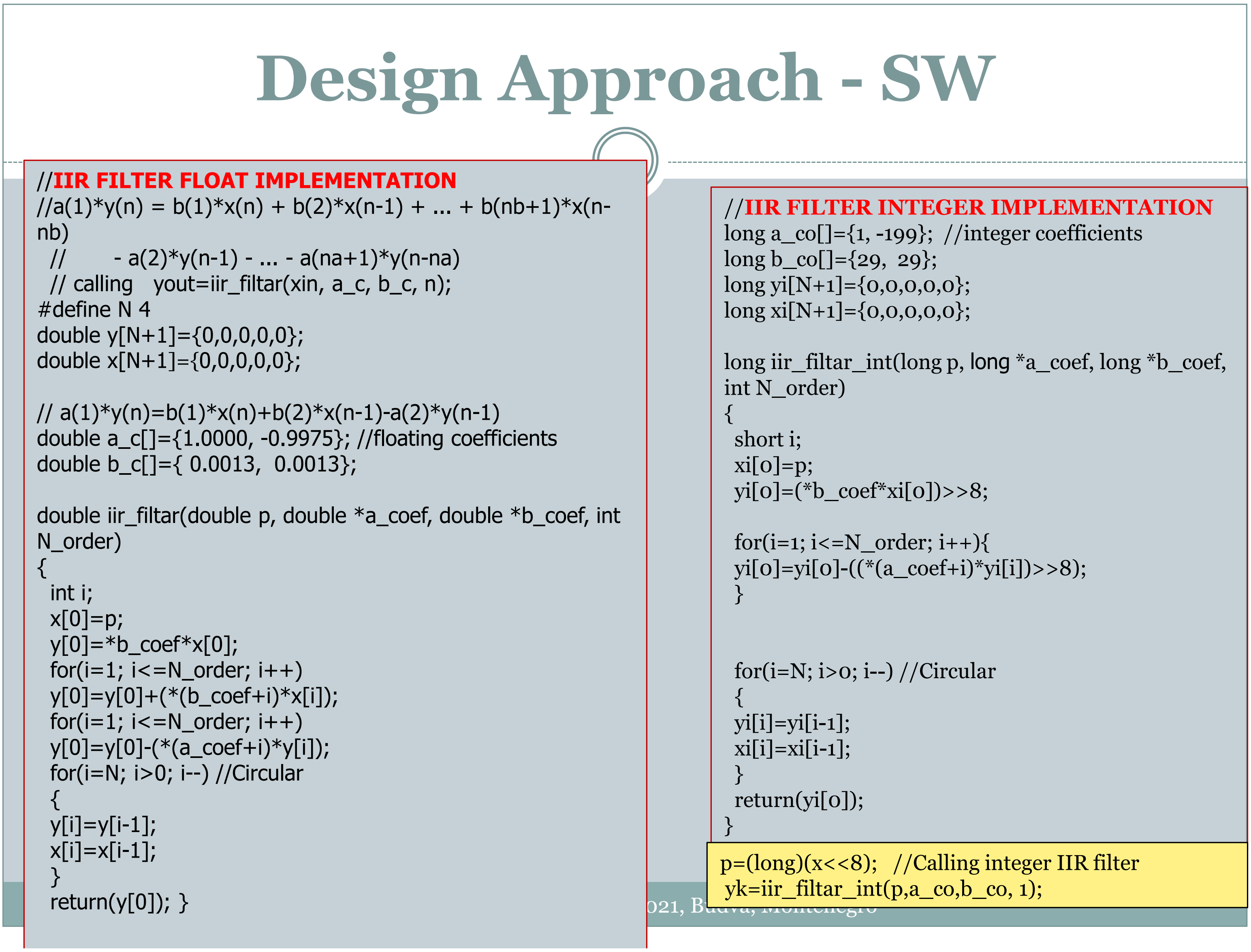
```
const int fs=200; //sampling frequency

//filter variables
const int fc_l=5; //corner frequency HP
float alfa=0; //coefficient LP
float y_old_lp=0; //previous value y LP

const int fc_h=15; //corner frequency LP
float beta=0; //coefficient HP
float y_old_hp=0; //previous value x HP
float x_old_hp=0; //previous value y HP

void setup()
{
.....
 alfa=calculate_alfa((float)(fc_h), fs); //calculate_alfa
 beta=calculate_beta((float)(fc_l), fs); //calculate beta
.....
}
//coefficient alfa for LP filter
float calculate_alfa(float fc, float fs)
{
float alfa;
alfa=(2*PI*fc/fs)/((2*PI*fc/fs)+1);
return alfa;
}
//coefficient beta in HP filter
float calculate_beta(float fc, float fs)
{
float beta;
beta=1/((2*PI*fc/fs)+1);
return beta;
}
```

Calculation of coefficients

- **RC (LP) i CR (HP) filter implementation, using fs and fc. Basic configuration.**

```
//LP filter of 1st order
float low_pass1(float alfa, float x)
{
float y=0;
y=alfa*x+(1.0-alfa)*y_old_lp;
y_old_lp=y;
return y;
}
//HP filter of 1st order
float high_pass1(float beta, float x)
{
float y=0;
y=beta*y_old_hp+beta*(x-x_old_hp);
y_old_hp=y;
x_old_hp=x;
return y;
}

void loop()
{
.....
sample= analogRead(AD0);
y1=high_pass1(beta, float(sample);//HPF 5Hz
y2=low_pass1(alfa,y1); // LPF 15Hz
......
}
```

MECO'2021 and CPSIoT'2021, Budva, Montenegro

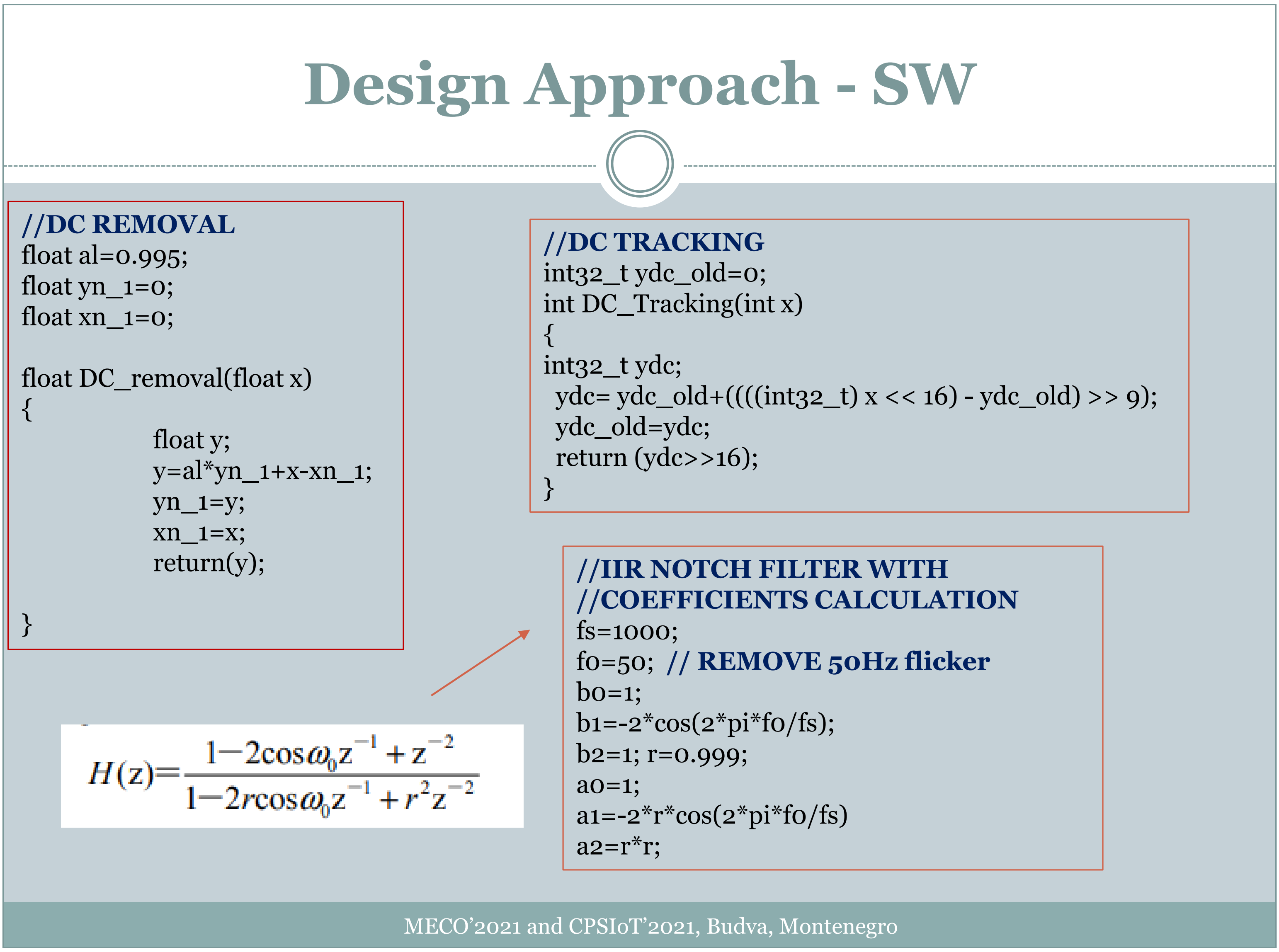


Design Approach - SW

```
//IIR FILTER FLOAT IMPLEMENTATION
//a(1)*y(n) = b(1)*x(n) + b(2)*x(n-1) + ... + b(nb+1)*x(n-nb)
  //       - a(2)*y(n-1) - ... - a(na+1)*y(n-na)
  // calling   yout=iir_filtar(xin, a_c, b_c, n);
#define N 4
double y[N+1]={0,0,0,0,0};
double x[N+1]={0,0,0,0,0};

// a(1)*y(n)=b(1)*x(n)+b(2)*x(n-1)-a(2)*y(n-1)
double a_c[]={1.0000, -0.9975}; //floating coefficients
double b_c[]={ 0.0013,  0.0013};

double iir_filtar(double p, double *a_coef, double *b_coef, int N_order)
{
  int i;
  x[0]=p;
  y[0]=*b_coef*x[0];
  for(i=1; i<=N_order; i++)
  y[0]=y[0]+(*(b_coef+i)*x[i]);
  for(i=1; i<=N_order; i++)
  y[0]=y[0]-(*(a_coef+i)*y[i]);
  for(i=N; i>0; i--) //Circular
  {
  y[i]=y[i-1];
  x[i]=x[i-1];
  }
  return(y[0]); }
```

```
//IIR FILTER INTEGER IMPLEMENTATION
long a_co[]={1, -199};  //integer coefficients
long b_co[]={29,  29};
long yi[N+1]={0,0,0,0,0};
long xi[N+1]={0,0,0,0,0};

long iir_filtar_int(long p, long *a_coef, long *b_coef, int N_order)
{
 short i;
 xi[0]=p;
 yi[0]=(*b_coef*xi[0])>>8;

 for(i=1; i<=N_order; i++){
 yi[0]=yi[0]-((*(a_coef+i)*yi[i])>>8);
 }


 for(i=N; i>0; i--) //Circular
 {
 yi[i]=yi[i-1];
 xi[i]=xi[i-1];
 }
 return(yi[0]);
}
```

```
p=(long)(x<<8);   //Calling integer IIR filter
 yk=iir_filtar_int(p,a_co,b_co, 1);
```



Design Approach - SW

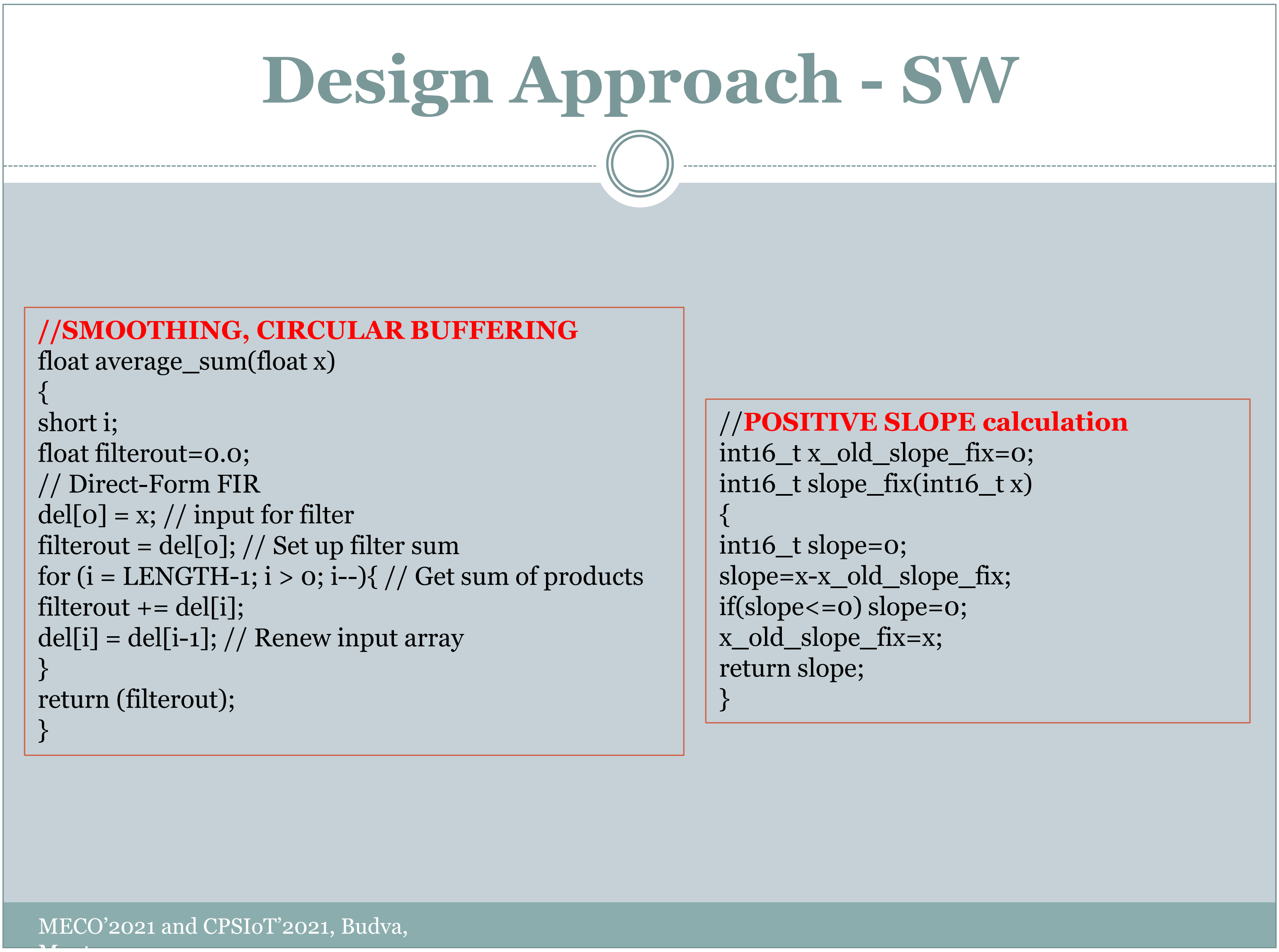
```
//DC REMOVAL
float al=0.995;
float yn_1=0;
float xn_1=0;

float DC_removal(float x)
{
            float y;
            y=al*yn_1+x-xn_1;
            yn_1=y;
            xn_1=x;
            return(y);

}
```

```
//DC TRACKING
int32_t ydc_old=0;
int DC_Tracking(int x)
{
int32_t ydc;
  ydc= ydc_old+((((int32_t) x << 16) - ydc_old) >> 9);
  ydc_old=ydc;
  return (ydc>>16);
}
```

$$H(z)=\frac{1-2\cos\omega_0 z^{-1}+z^{-2}}{1-2r\cos\omega_0 z^{-1}+r^2 z^{-2}}$$

```
//IIR NOTCH FILTER WITH
//COEFFICIENTS CALCULATION
fs=1000;
f0=50;  // REMOVE 50Hz flicker
b0=1;
b1=-2*cos(2*pi*f0/fs);
b2=1; r=0.999;
a0=1;
a1=-2*r*cos(2*pi*f0/fs)
a2=r*r;
```

MECO'2021 and CPSIoT'2021, Budva, Montenegro

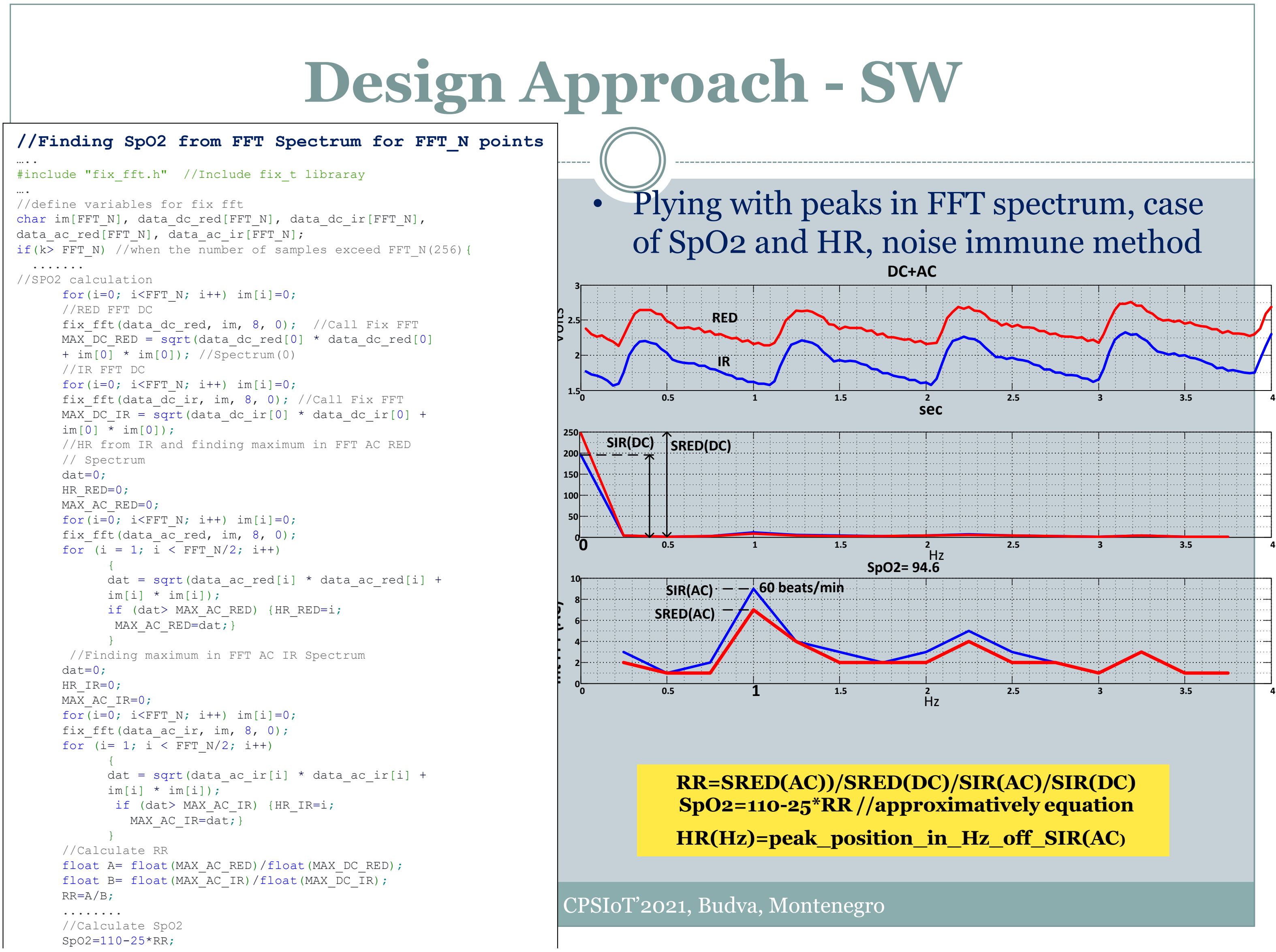


Design Approach - SW

```
//SMOOTHING, CIRCULAR BUFFERING
float average_sum(float x)
{
short i;
float filterout=0.0;
// Direct-Form FIR
del[0] = x; // input for filter
filterout = del[0]; // Set up filter sum
for (i = LENGTH-1; i > 0; i--){ // Get sum of products
filterout += del[i];
del[i] = del[i-1]; // Renew input array
}
return (filterout);
}
```

```
//POSITIVE SLOPE calculation
int16_t x_old_slope_fix=0;
int16_t slope_fix(int16_t x)
{
int16_t slope=0;
slope=x-x_old_slope_fix;
if(slope<=0) slope=0;
x_old_slope_fix=x;
return slope;
}
```

MECO’2021 and CPSIoT’2021, Budva,



Design Approach - SW

```
//Finding SpO2 from FFT Spectrum for FFT_N points
…..
#include "fix_fft.h"  //Include fix_t libraray
….
//define variables for fix fft
char im[FFT_N], data_dc_red[FFT_N], data_dc_ir[FFT_N],
data_ac_red[FFT_N], data_ac_ir[FFT_N];
if(k> FFT_N) //when the number of samples exceed FFT_N(256){
  .......
//SPO2 calculation
      for(i=0; i<FFT_N; i++) im[i]=0;
      //RED FFT DC
      fix_fft(data_dc_red, im, 8, 0);  //Call Fix FFT
      MAX_DC_RED = sqrt(data_dc_red[0] * data_dc_red[0]
      + im[0] * im[0]); //Spectrum(0)
      //IR FFT DC
      for(i=0; i<FFT_N; i++) im[i]=0;
      fix_fft(data_dc_ir, im, 8, 0); //Call Fix FFT
      MAX_DC_IR = sqrt(data_dc_ir[0] * data_dc_ir[0] +
      im[0] * im[0]);
      //HR from IR and finding maximum in FFT AC RED
      // Spectrum
      dat=0;
      HR_RED=0;
      MAX_AC_RED=0;
      for(i=0; i<FFT_N; i++) im[i]=0;
      fix_fft(data_ac_red, im, 8, 0);
      for (i = 1; i < FFT_N/2; i++)
            {
            dat = sqrt(data_ac_red[i] * data_ac_red[i] +
            im[i] * im[i]);
            if (dat> MAX_AC_RED) {HR_RED=i;
             MAX_AC_RED=dat;}
            }
       //Finding maximum in FFT AC IR Spectrum
      dat=0;
      HR_IR=0;
      MAX_AC_IR=0;
      for(i=0; i<FFT_N; i++) im[i]=0;
      fix_fft(data_ac_ir, im, 8, 0);
      for (i= 1; i < FFT_N/2; i++)
            {
            dat = sqrt(data_ac_ir[i] * data_ac_ir[i] +
            im[i] * im[i]);
             if (dat> MAX_AC_IR) {HR_IR=i;
               MAX_AC_IR=dat;}
            }
      //Calculate RR
      float A= float(MAX_AC_RED)/float(MAX_DC_RED);
      float B= float(MAX_AC_IR)/float(MAX_DC_IR);
      RR=A/B;
      ........
      //Calculate SpO2
      SpO2=110-25*RR;
```

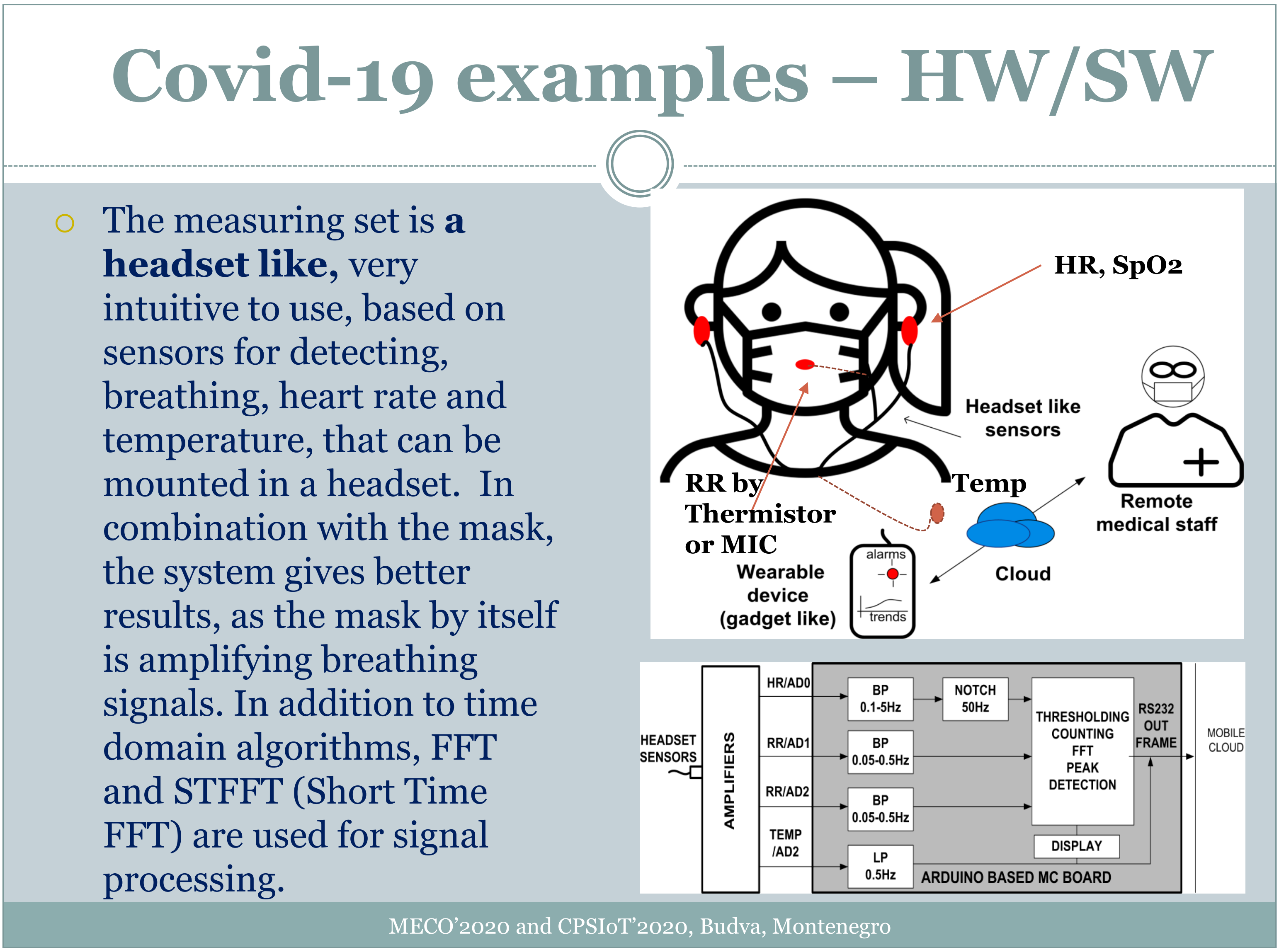
- Plying with peaks in FFT spectrum, case of SpO2 and HR, noise immune method

RR=SRED(AC))/SRED(DC)/SIR(AC)/SIR(DC)
SpO2=110-25*RR //approximatively equation

HR(Hz)=peak_position_in_Hz_off_SIR(AC)

CPSIoT’2021, Budva, Montenegro

©MECO.net

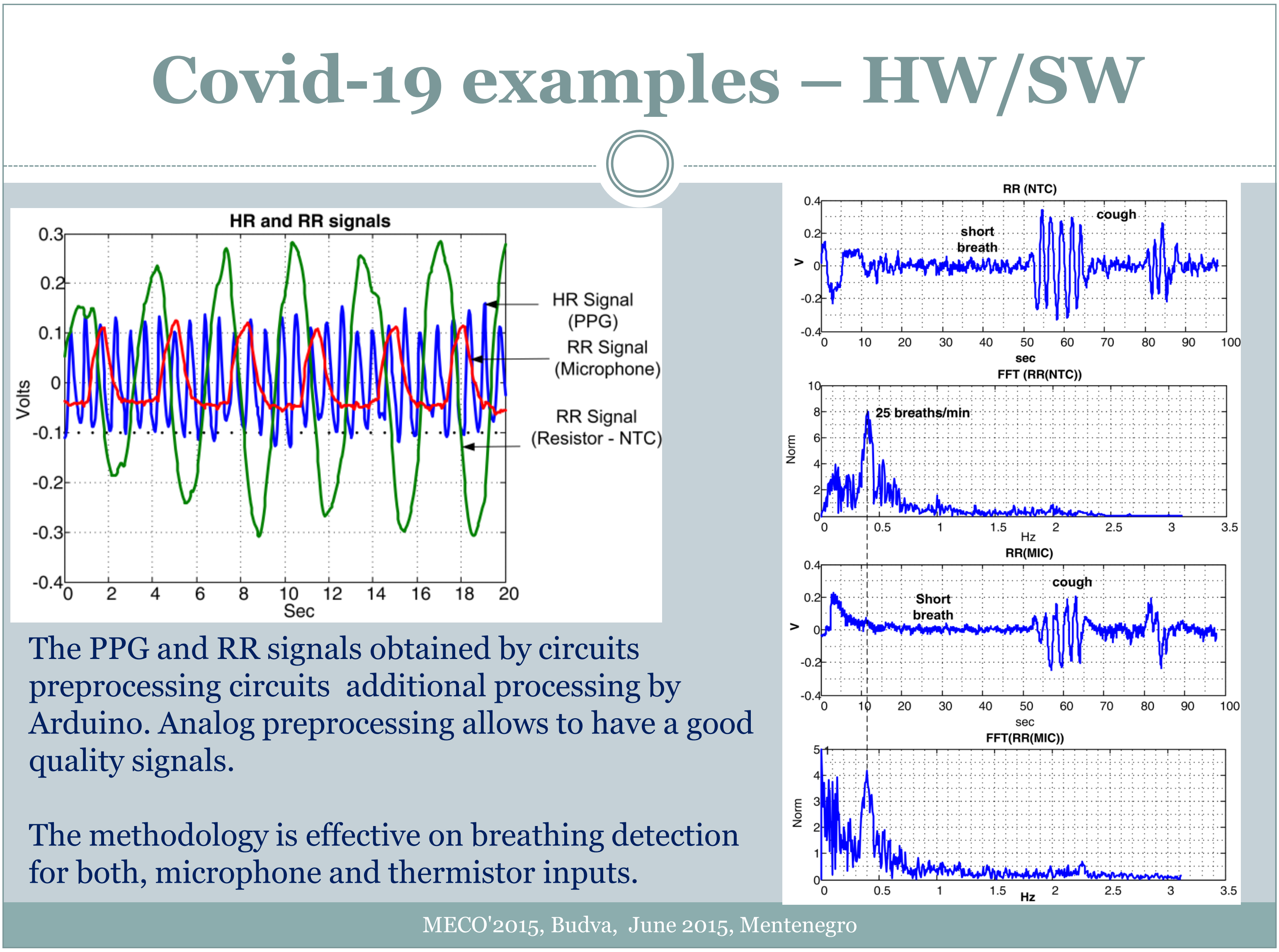


Covid-19 examples – HW/SW

- The measuring set is **a headset like,** very intuitive to use, based on sensors for detecting, breathing, heart rate and temperature, that can be mounted in a headset. In combination with the mask, the system gives better results, as the mask by itself is amplifying breathing signals. In addition to time domain algorithms, FFT and STFFT (Short Time FFT) are used for signal processing.

MECO'2020 and CPSIoT'2020, Budva, Montenegro

©MECO.net



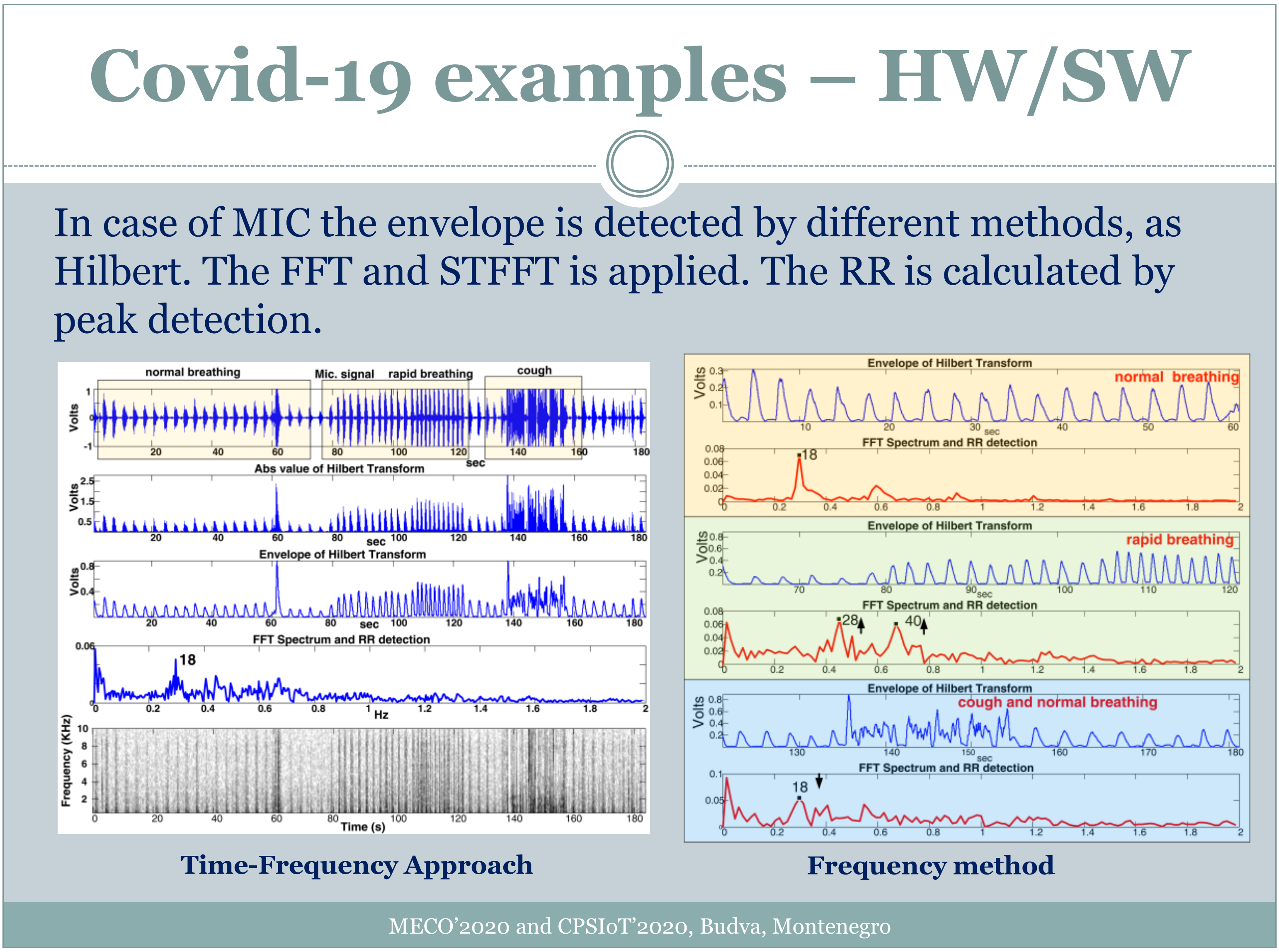
Covid-19 examples – HW/SW

The PPG and RR signals obtained by circuits preprocessing circuits additional processing by Arduino. Analog preprocessing allows to have a good quality signals.

The methodology is effective on breathing detection for both, microphone and thermistor inputs.

MECO'2015, Budva, June 2015, Mentenegro

©MECO.net



Covid-19 examples – HW/SW

In case of MIC the envelope is detected by different methods, as Hilbert. The FFT and STFFT is applied. The RR is calculated by peak detection.

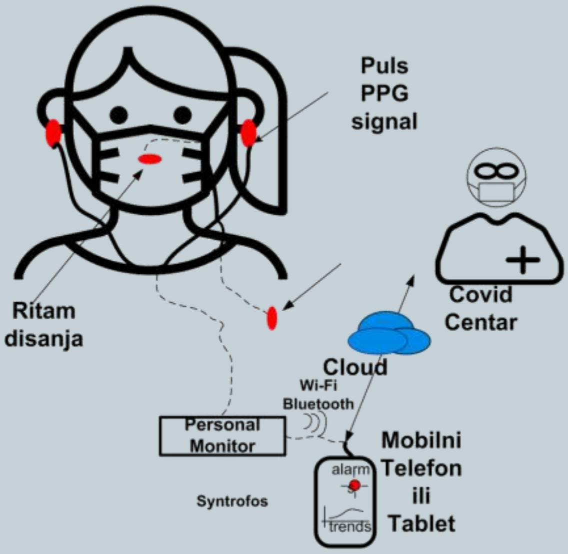
Time-Frequency Approach

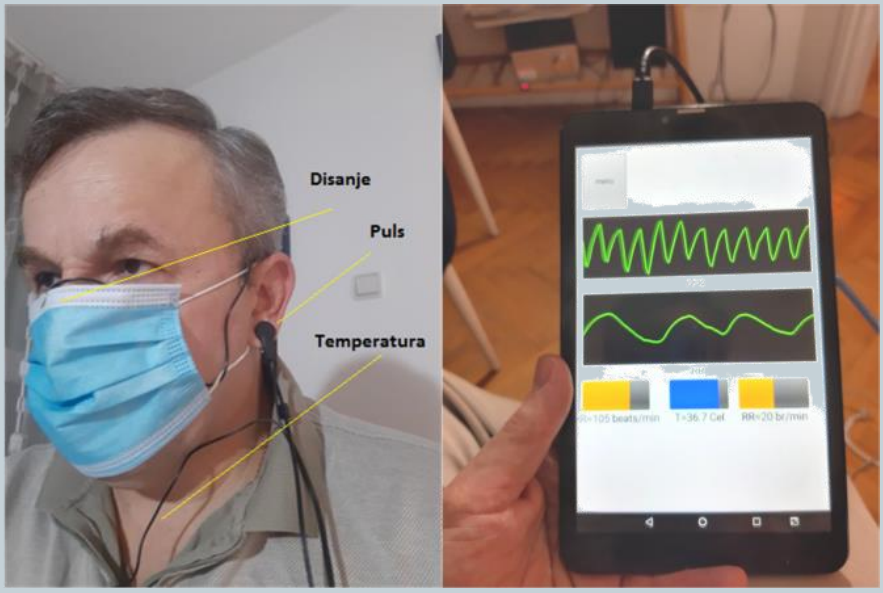
Frequency method

MECO'2020 and CPSIoT'2020, Budva, Montenegro

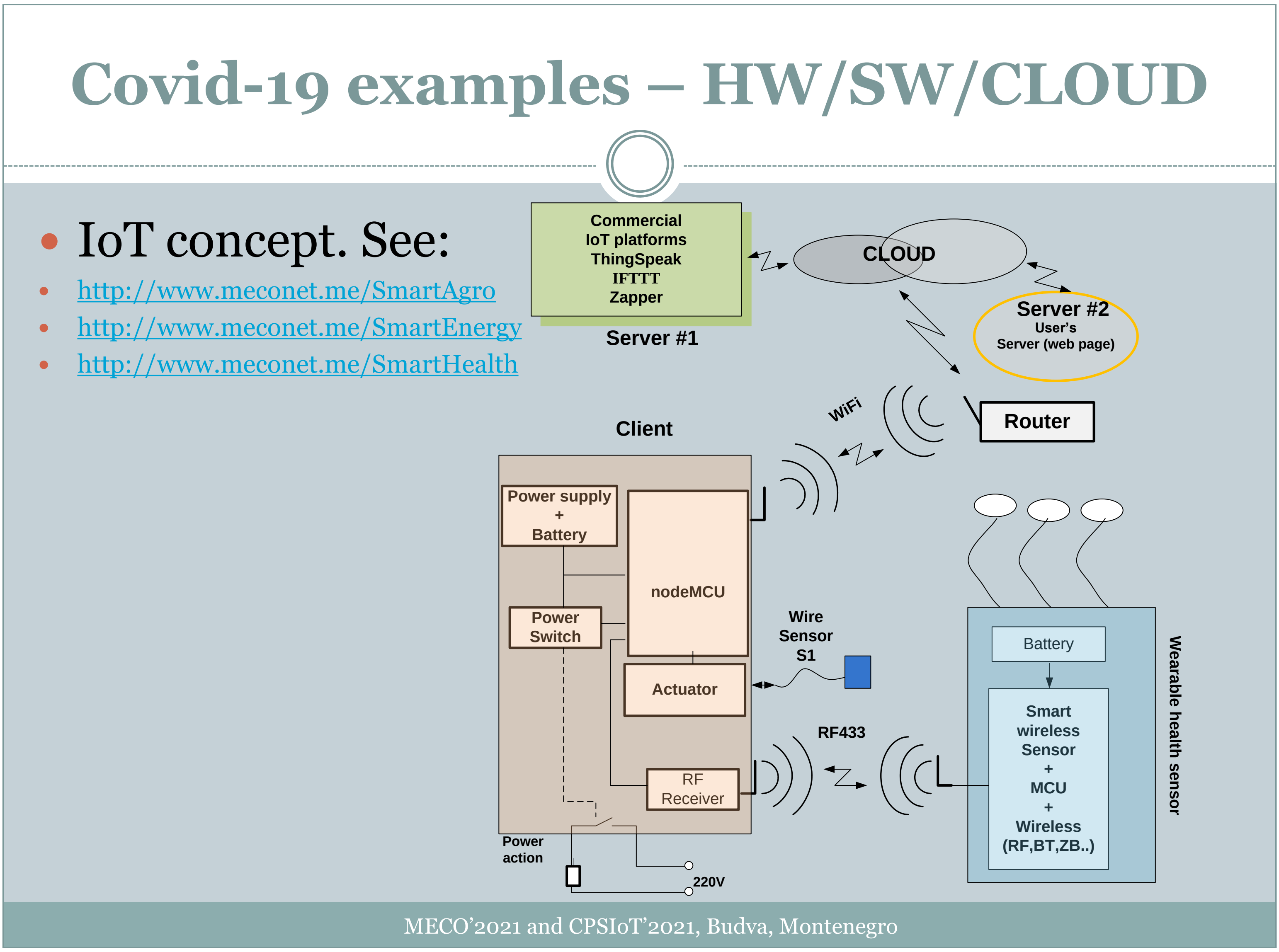
Covid-19 examples – HW/SW

By "Syntrofos" device, it is possible for everyone to have a personal COVID signal monitor, 24/7/365. The Syntrofos Basic version monitors Temperature, Pulse, Respiration Rhythm , sisplaying PhotoPlethysmographic Signal (PPG) and Respiration Signal (RR). VIDEO.





MECO'2020 and CPSIoT'2020, Budva, Montenegro

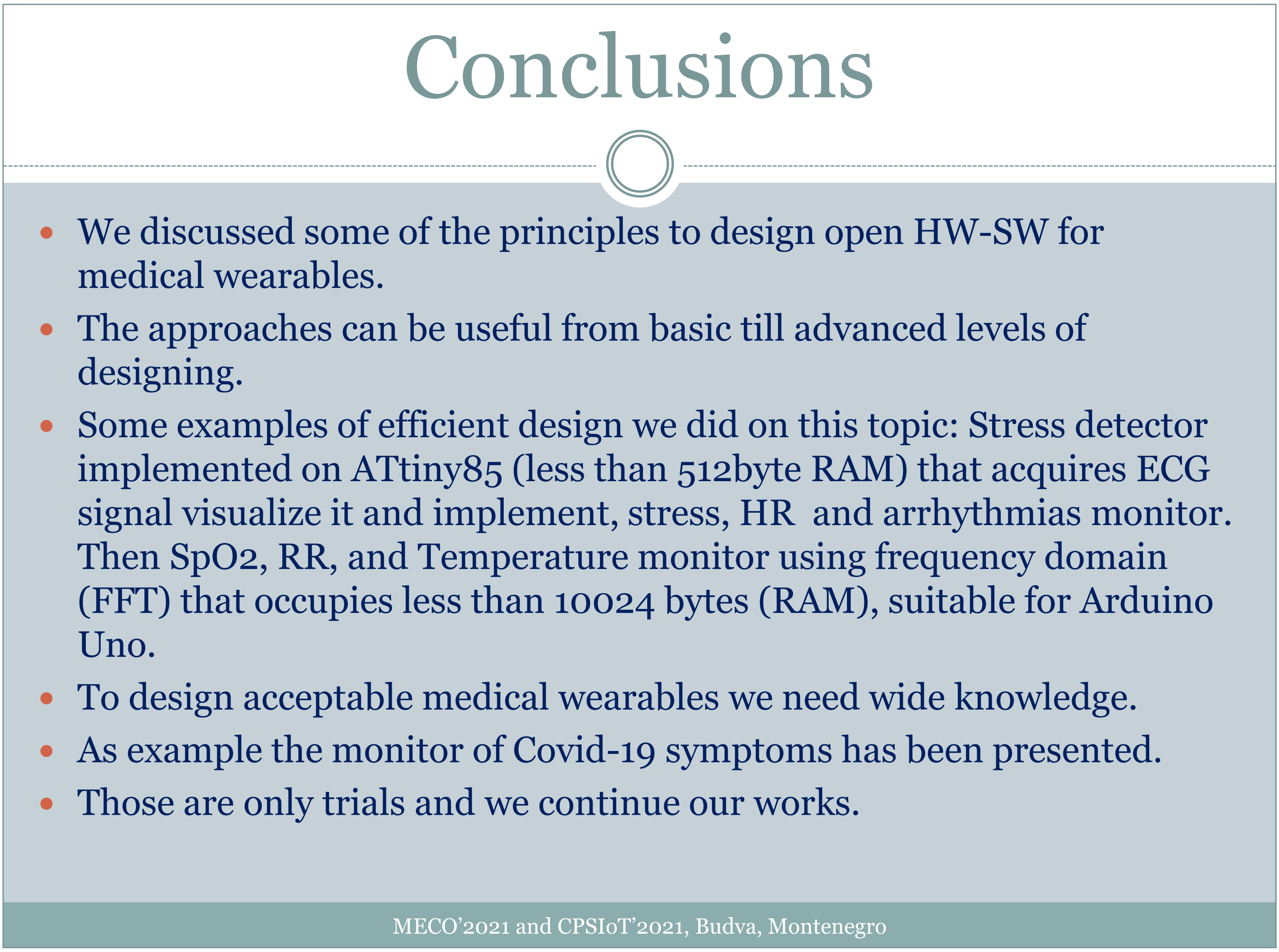


Covid-19 examples – HW/SW/CLOUD

- IoT concept. See:
  - http://www.meconet.me/SmartAgro
  - http://www.meconet.me/SmartEnergy
  - http://www.meconet.me/SmartHealth

MECO'2021 and CPSIoT'2021, Budva, Montenegro

©MECO.net



Conclusions

- We discussed some of the principles to design open HW-SW for medical wearables.
- The approaches can be useful from basic till advanced levels of designing.
- Some examples of efficient design we did on this topic: Stress detector implemented on ATtiny85 (less than 512byte RAM) that acquires ECG signal visualize it and implement, stress, HR and arrhythmias monitor. Then SpO2, RR, and Temperature monitor using frequency domain (FFT) that occupies less than 10024 bytes (RAM), suitable for Arduino Uno.
- To design acceptable medical wearables we need wide knowledge.
- As example the monitor of Covid-19 symptoms has been presented.
- Those are only trials and we continue our works.

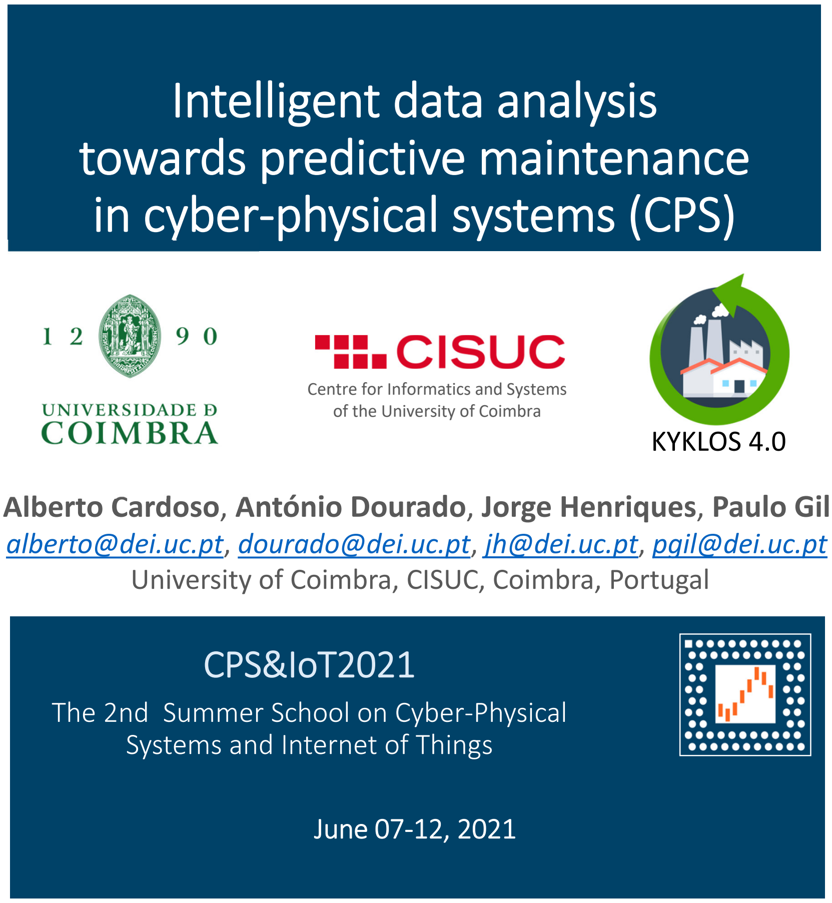
MECO'2021 and CPSIoT'2021, Budva, Montenegro

THANK YOU

The work is partly supported by SMART4ALL project, H2020

Radovan Stojanovic
stox@ucg.ac.me

MECO'2021 and CPSIoT'2021, Budva, Montenegro



Intelligent data analysis towards predictive maintenance in cyber-physical systems (CPS)

1 2 9 0 UNIVERSIDADE D COIMBRA

CISUC Centre for Informatics and Systems of the University of Coimbra

KYKLOS 4.0

Alberto Cardoso, António Dourado, Jorge Henriques, Paulo Gil
alberto@dei.uc.pt, *dourado@dei.uc.pt*, *jh@dei.uc.pt*, *pgil@dei.uc.pt*
University of Coimbra, CISUC, Coimbra, Portugal

CPS&IoT2021

The 2nd Summer School on Cyber-Physical Systems and Internet of Things

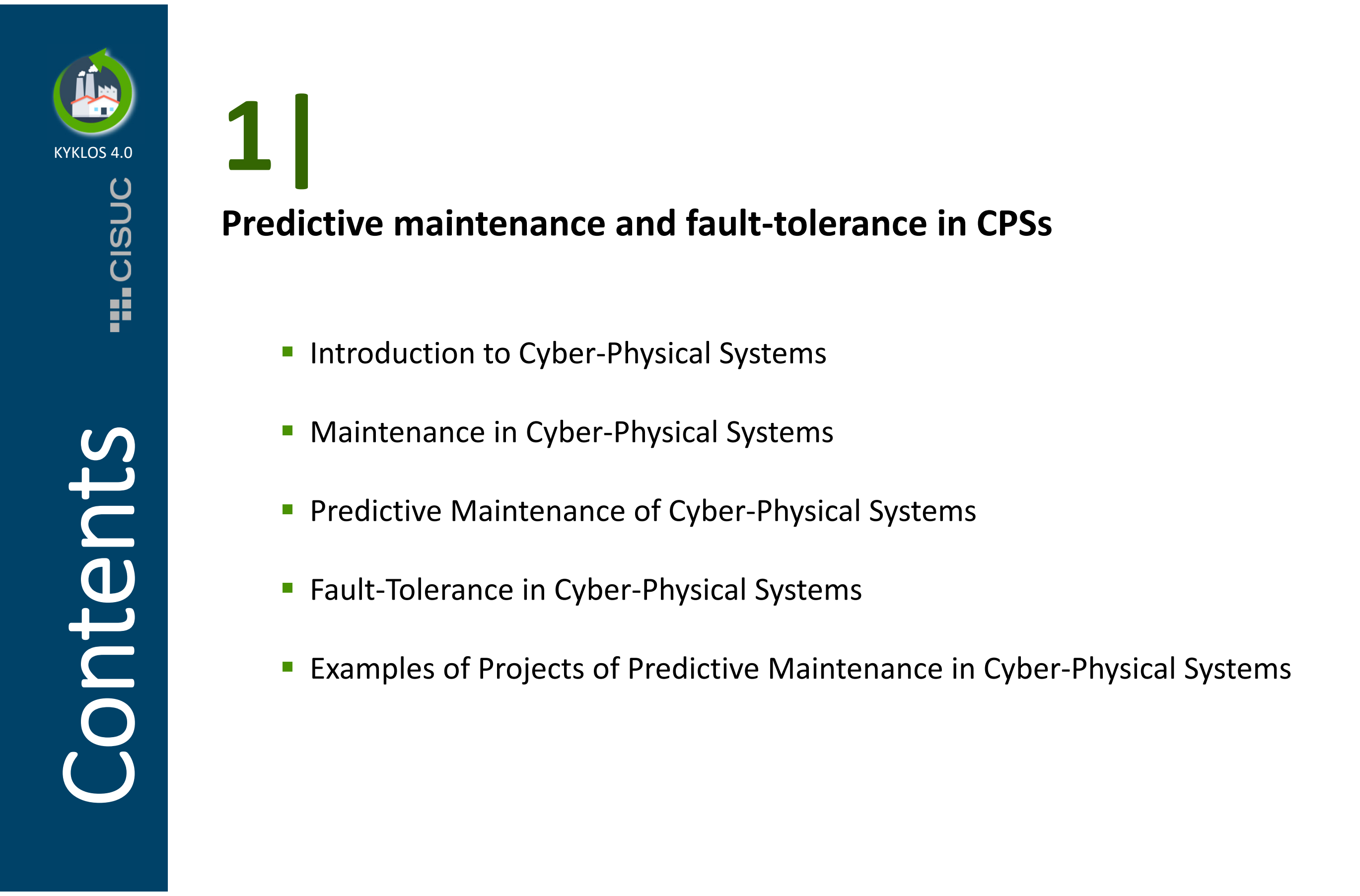
June 07-12, 2021

KYKLOS 4.0

CISUC

Contents

- **1| Predictive maintenance and fault-tolerance in CPSs**
- 2| Outliers detection for transient time-series
- 3| Reduction of the dimension of the data space by "multidimensional scaling" applying several optimization algorithms
- 4| Detection of similarities and prediction of the evolution of the health condition of a machine, as a previous step to estimate the RUL
- 5| References and bibliography



KYKLOS 4.0

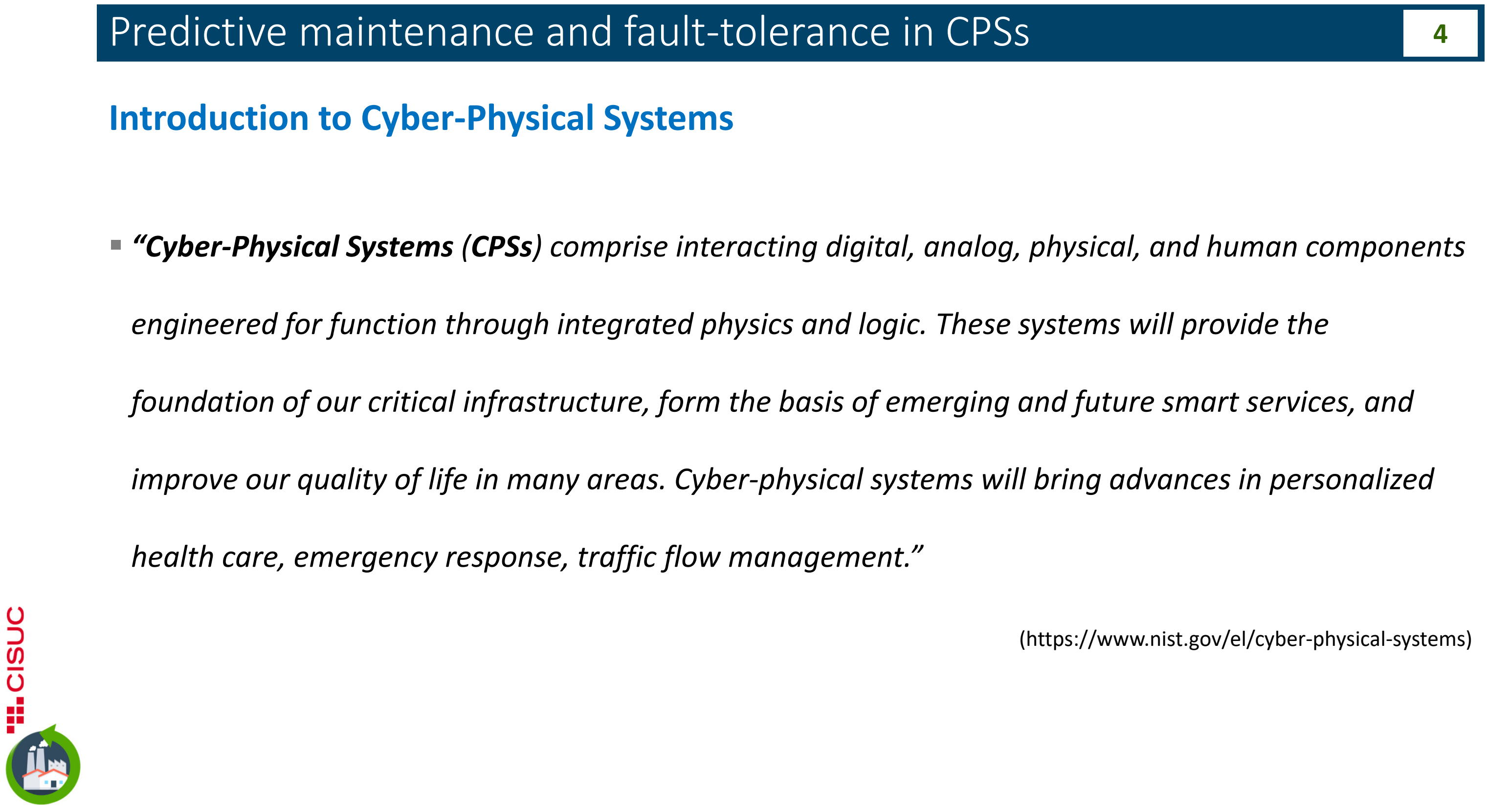
CISUC

Contents

1|

Predictive maintenance and fault-tolerance in CPSs

- Introduction to Cyber-Physical Systems
- Maintenance in Cyber-Physical Systems
- Predictive Maintenance of Cyber-Physical Systems
- Fault-Tolerance in Cyber-Physical Systems
- Examples of Projects of Predictive Maintenance in Cyber-Physical Systems



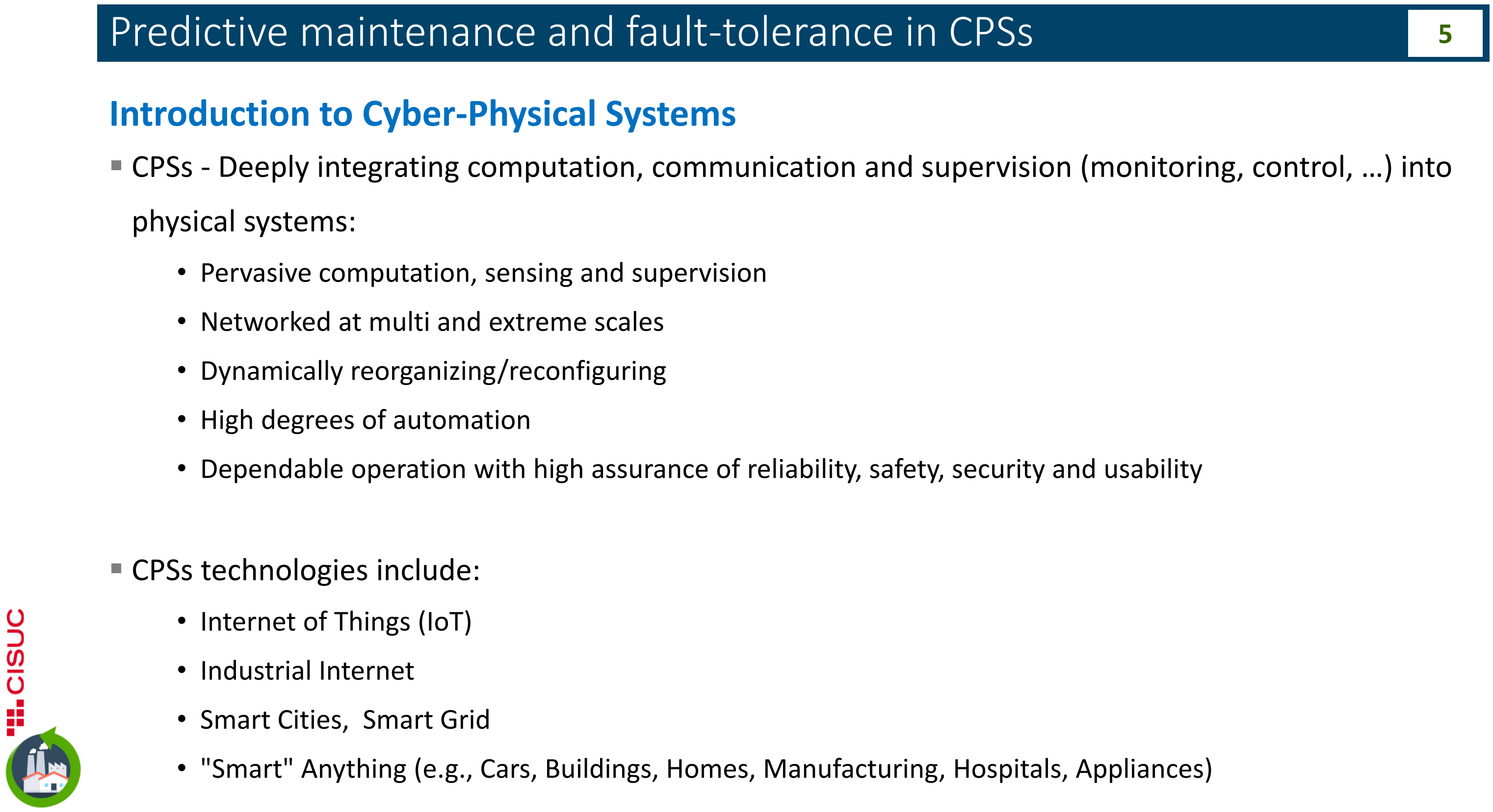
Predictive maintenance and fault-tolerance in CPSs

4

Introduction to Cyber-Physical Systems

- ***"Cyber-Physical Systems*** (***CPSs***) *comprise interacting digital, analog, physical, and human components engineered for function through integrated physics and logic. These systems will provide the foundation of our critical infrastructure, form the basis of emerging and future smart services, and improve our quality of life in many areas. Cyber-physical systems will bring advances in personalized health care, emergency response, traffic flow management."*

(https://www.nist.gov/el/cyber-physical-systems)



Predictive maintenance and fault-tolerance in CPSs 5

Introduction to Cyber-Physical Systems

- CPSs - Deeply integrating computation, communication and supervision (monitoring, control, …) into physical systems:
  - Pervasive computation, sensing and supervision
  - Networked at multi and extreme scales
  - Dynamically reorganizing/reconfiguring
  - High degrees of automation
  - Dependable operation with high assurance of reliability, safety, security and usability

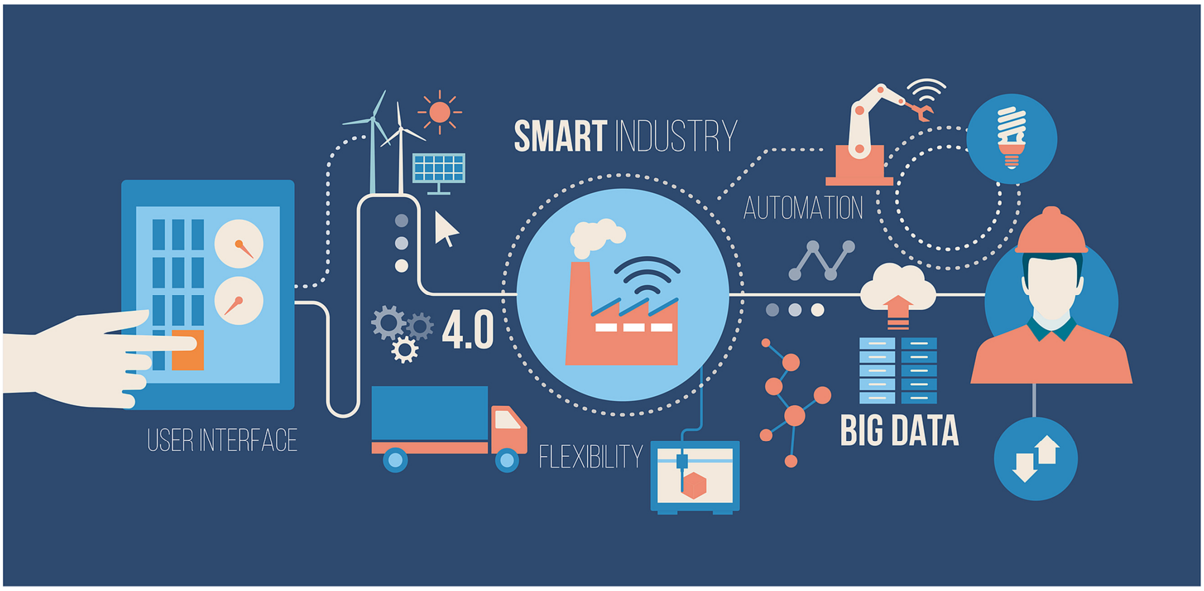
- CPSs technologies include:
  - Internet of Things (IoT)
  - Industrial Internet
  - Smart Cities, Smart Grid
  - "Smart" Anything (e.g., Cars, Buildings, Homes, Manufacturing, Hospitals, Appliances)

Predictive maintenance and fault-tolerance in CPSs

6

Introduction to Cyber-Physical Systems

- CPSs: Interactions with the physical world (example: Smart Industry)



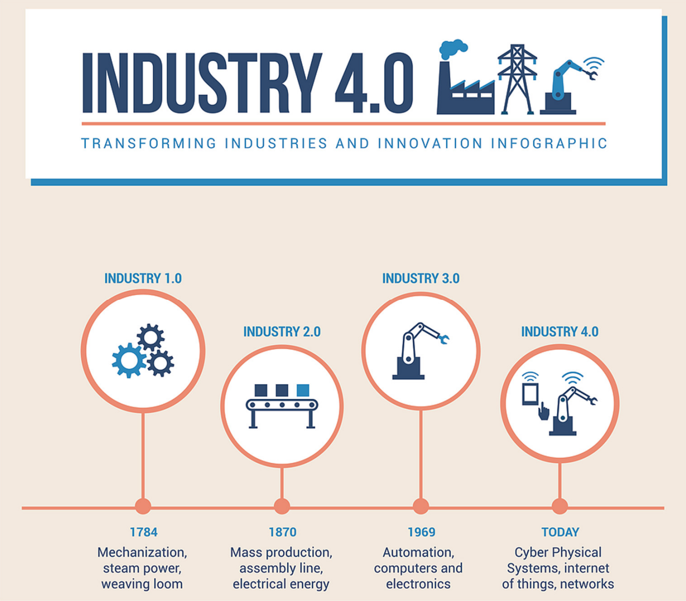
(https://iiot-world.com/industrial-iot/connected-industry/iic-industrial-iot-reference-architecture/)

Predictive maintenance and fault-tolerance in CPSs

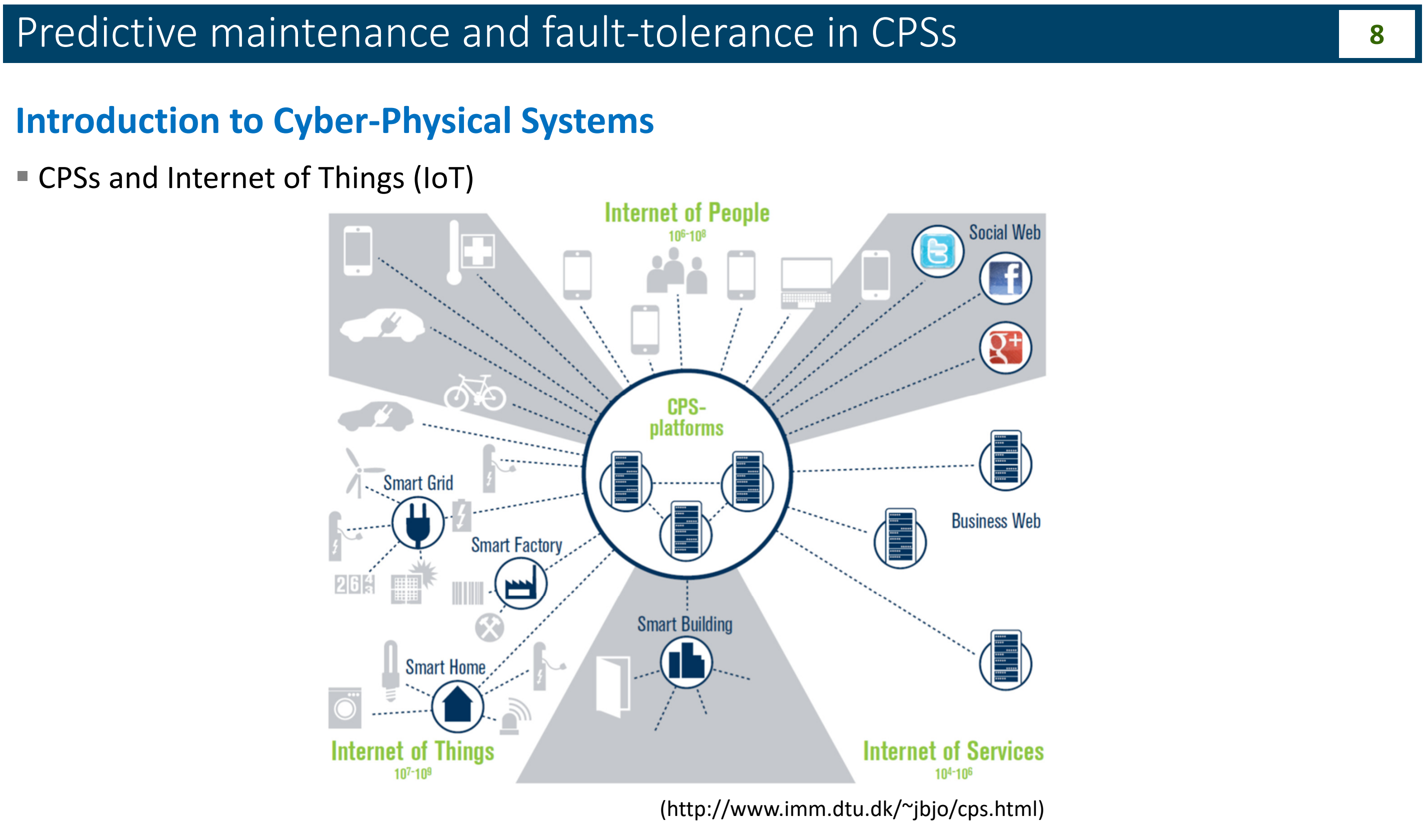
7

Introduction to Cyber-Physical Systems

- CPSs and Industry 4.0


INDUSTRY 4.0
TRANSFORMING INDUSTRIES AND INNOVATION INFOGRAPHIC
INDUSTRY 1.0
INDUSTRY 2.0
INDUSTRY 3.0
INDUSTRY 4.0
1784
Mechanization, steam power, weaving loom
1870
Mass production, assembly line, electrical energy
1969
Automation, computers and electronics
TODAY
Cyber Physical Systems, internet of things, networks

(http://www.imm.dtu.dk/~jbjo/cps.html)



Predictive maintenance and fault-tolerance in CPSs 8

Introduction to Cyber-Physical Systems

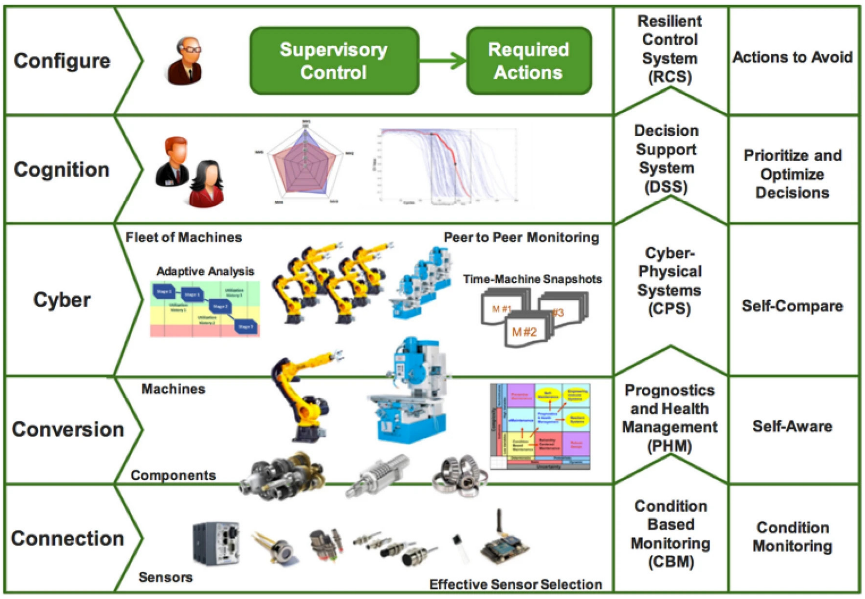
- CPSs and Internet of Things (IoT)

(http://www.imm.dtu.dk/~jbjo/cps.html)

Predictive maintenance and fault-tolerance in CPSs

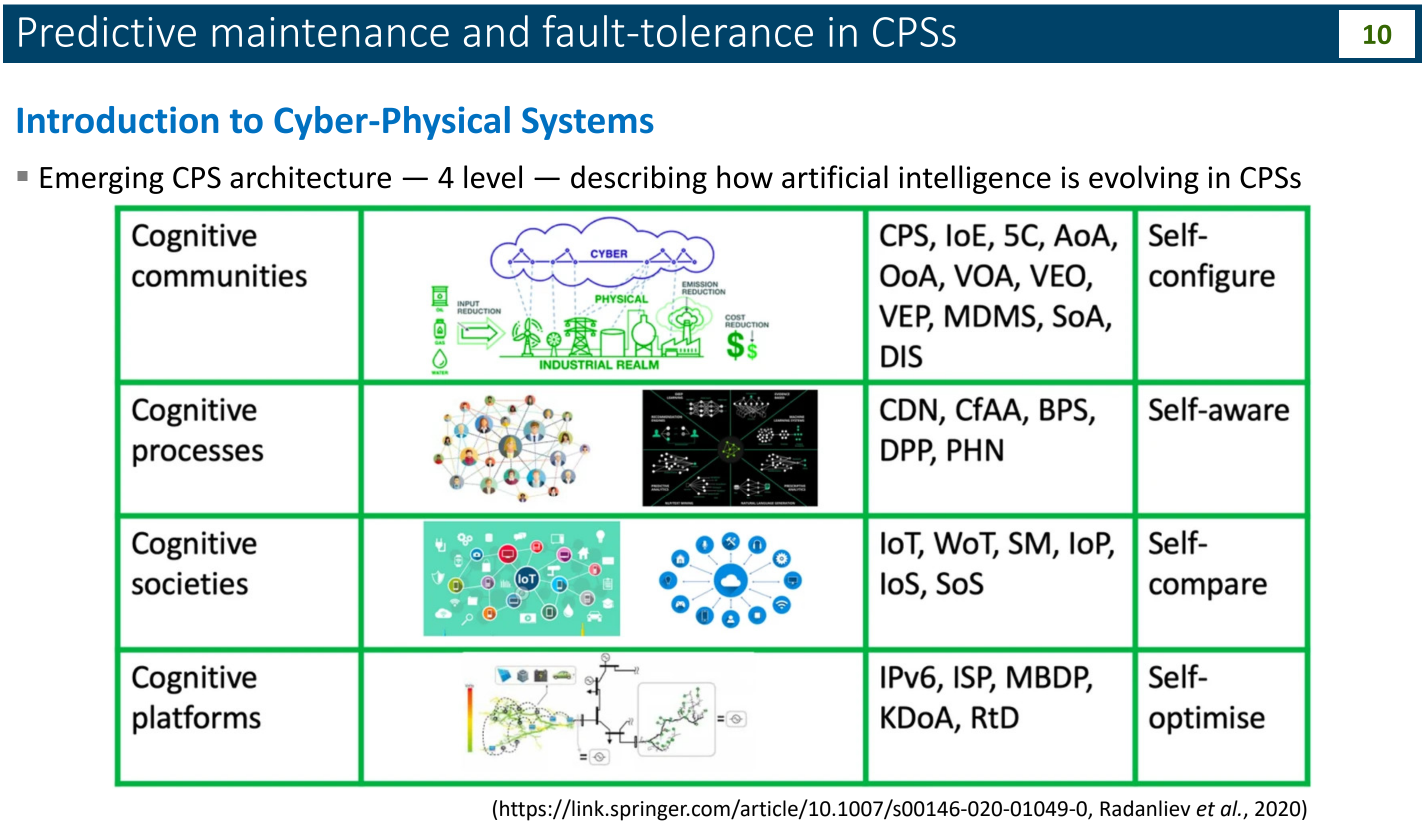
Introduction to Cyber-Physical Systems

- The 5 levels cyber physical system architecture — commonly referred to as 5C architecture



Configure	Resilient Control System (RCS)	Actions to Avoid
Cognition	Decision Support System (DSS)	Prioritize and Optimize Decisions
Cyber	Cyber-Physical Systems (CPS)	Self-Compare
Conversion	Prognostics and Health Management (PHM)	Self-Aware
Connection	Condition Based Monitoring (CBM)	Condition Monitoring

(https://link.springer.com/article/10.1007/s00146-020-01049-0, Radanliev *et al.*, 2020)



CYBER
PHYSICAL
INPUT REDUCTION
EMISSION REDUCTION
COST REDUCTION
INDUSTRIAL REALM
IoT

Predictive maintenance and fault-tolerance in CPSs

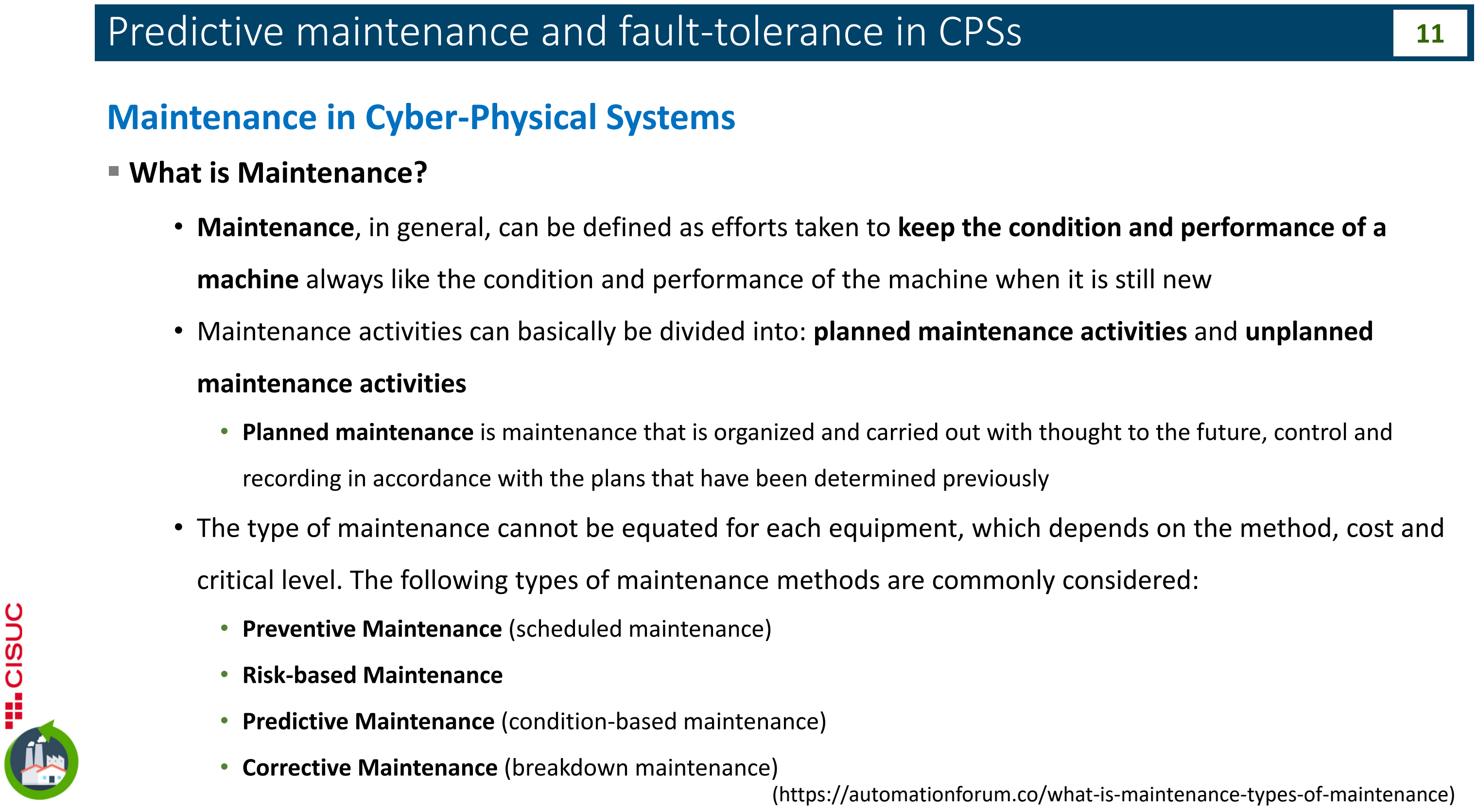
10

Introduction to Cyber-Physical Systems

- Emerging CPS architecture — 4 level — describing how artificial intelligence is evolving in CPSs

Cognitive communities		CPS, IoE, 5C, AoA, OoA, VOA, VEO, VEP, MDMS, SoA, DIS	Self-configure
Cognitive processes		CDN, CfAA, BPS, DPP, PHN	Self-aware
Cognitive societies		IoT, WoT, SM, IoP, IoS, SoS	Self-compare
Cognitive platforms		IPv6, ISP, MBDP, KDoA, RtD	Self-optimise

(https://link.springer.com/article/10.1007/s00146-020-01049-0, Radanliev *et al.*, 2020)



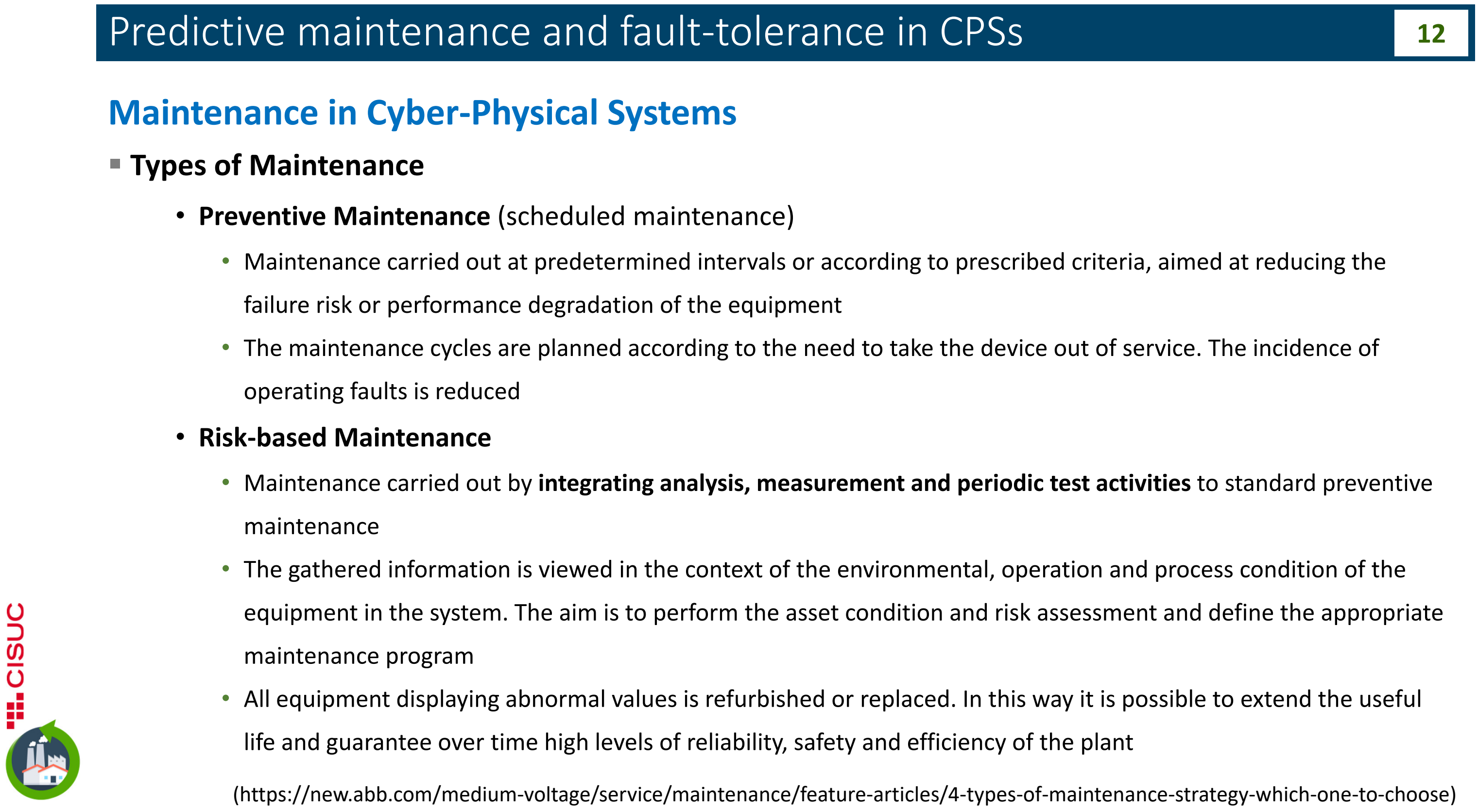
Predictive maintenance and fault-tolerance in CPSs

11

Maintenance in Cyber-Physical Systems

- **What is Maintenance?**
  - **Maintenance**, in general, can be defined as efforts taken to **keep the condition and performance of a machine** always like the condition and performance of the machine when it is still new
  - Maintenance activities can basically be divided into: **planned maintenance activities** and **unplanned maintenance activities**
    - **Planned maintenance** is maintenance that is organized and carried out with thought to the future, control and recording in accordance with the plans that have been determined previously
  - The type of maintenance cannot be equated for each equipment, which depends on the method, cost and critical level. The following types of maintenance methods are commonly considered:
    - **Preventive Maintenance** (scheduled maintenance)
    - **Risk-based Maintenance**
    - **Predictive Maintenance** (condition-based maintenance)
    - **Corrective Maintenance** (breakdown maintenance)

(https://automationforum.co/what-is-maintenance-types-of-maintenance)

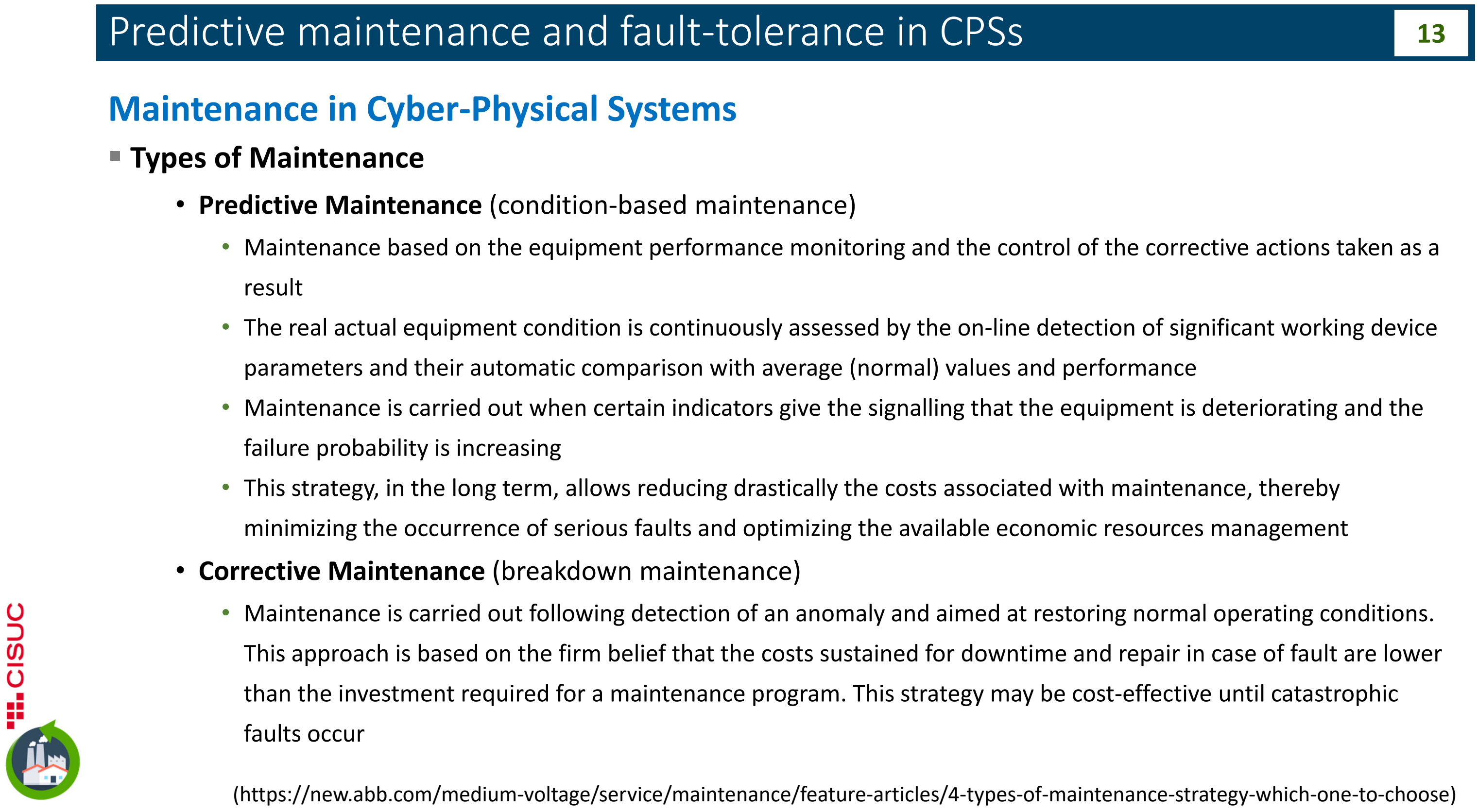


Predictive maintenance and fault-tolerance in CPSs 12

Maintenance in Cyber-Physical Systems

- **Types of Maintenance**
  - **Preventive Maintenance** (scheduled maintenance)
    - Maintenance carried out at predetermined intervals or according to prescribed criteria, aimed at reducing the failure risk or performance degradation of the equipment
    - The maintenance cycles are planned according to the need to take the device out of service. The incidence of operating faults is reduced
  - **Risk-based Maintenance**
    - Maintenance carried out by **integrating analysis, measurement and periodic test activities** to standard preventive maintenance
    - The gathered information is viewed in the context of the environmental, operation and process condition of the equipment in the system. The aim is to perform the asset condition and risk assessment and define the appropriate maintenance program
    - All equipment displaying abnormal values is refurbished or replaced. In this way it is possible to extend the useful life and guarantee over time high levels of reliability, safety and efficiency of the plant

(https://new.abb.com/medium-voltage/service/maintenance/feature-articles/4-types-of-maintenance-strategy-which-one-to-choose)

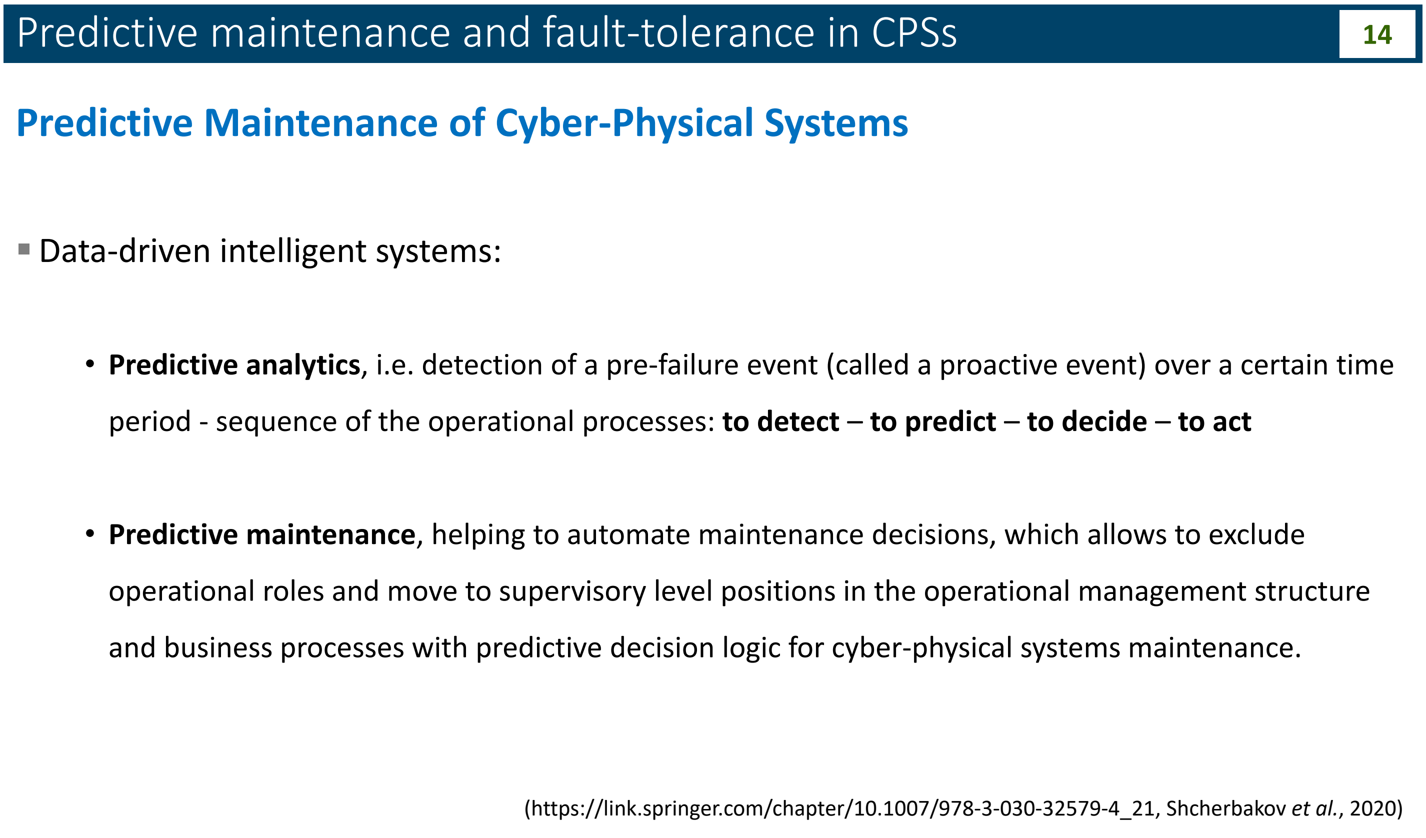


Predictive maintenance and fault-tolerance in CPSs 13

Maintenance in Cyber-Physical Systems

- **Types of Maintenance**
  - **Predictive Maintenance** (condition-based maintenance)
    - Maintenance based on the equipment performance monitoring and the control of the corrective actions taken as a result
    - The real actual equipment condition is continuously assessed by the on-line detection of significant working device parameters and their automatic comparison with average (normal) values and performance
    - Maintenance is carried out when certain indicators give the signalling that the equipment is deteriorating and the failure probability is increasing
    - This strategy, in the long term, allows reducing drastically the costs associated with maintenance, thereby minimizing the occurrence of serious faults and optimizing the available economic resources management
  - **Corrective Maintenance** (breakdown maintenance)
    - Maintenance is carried out following detection of an anomaly and aimed at restoring normal operating conditions. This approach is based on the firm belief that the costs sustained for downtime and repair in case of fault are lower than the investment required for a maintenance program. This strategy may be cost-effective until catastrophic faults occur

(https://new.abb.com/medium-voltage/service/maintenance/feature-articles/4-types-of-maintenance-strategy-which-one-to-choose)



Predictive maintenance and fault-tolerance in CPSs 14

Predictive Maintenance of Cyber-Physical Systems

- Data-driven intelligent systems:
  - **Predictive analytics**, i.e. detection of a pre-failure event (called a proactive event) over a certain time period - sequence of the operational processes: **to detect – to predict – to decide – to act**
  - **Predictive maintenance**, helping to automate maintenance decisions, which allows to exclude operational roles and move to supervisory level positions in the operational management structure and business processes with predictive decision logic for cyber-physical systems maintenance.

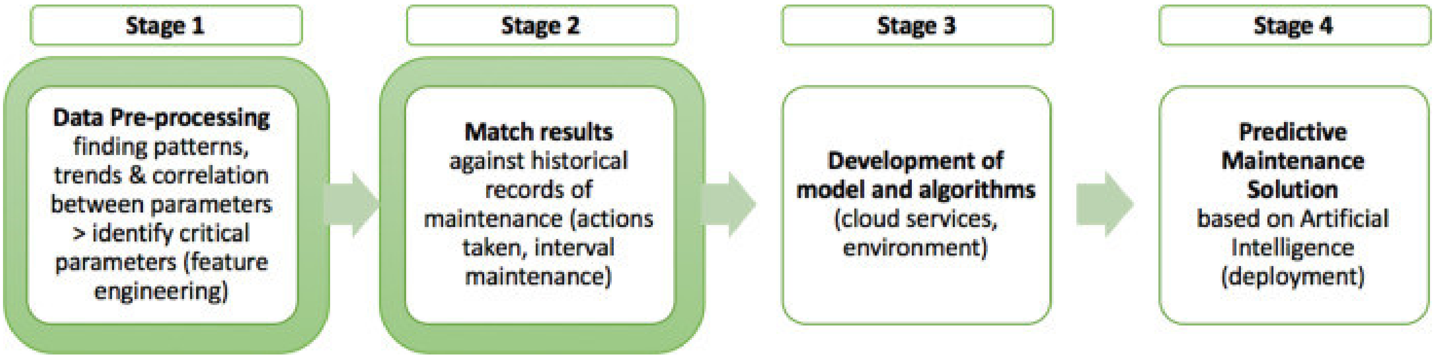
(https://link.springer.com/chapter/10.1007/978-3-030-32579-4_21, Shcherbakov *et al.*, 2020)

Predictive maintenance and fault-tolerance in CPSs

15

Predictive Maintenance of Cyber-Physical Systems

- Framework for achieving predictive maintenance:



Stage 1

Data Pre-processing finding patterns, trends & correlation between parameters > identify critical parameters (feature engineering)

Stage 2

Match results against historical records of maintenance (actions taken, interval maintenance)

Stage 3

Development of model and algorithms (cloud services, environment)

Stage 4

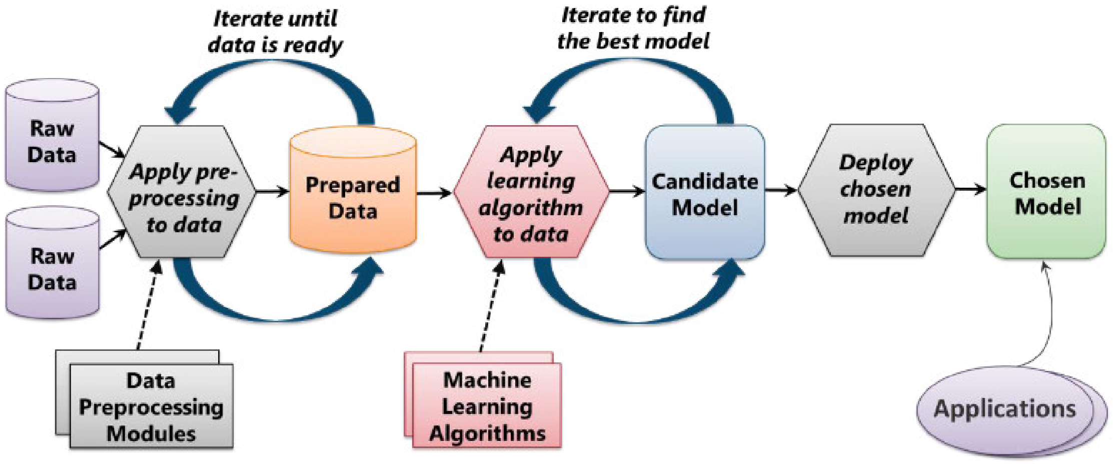
Predictive Maintenance Solution based on Artificial Intelligence (deployment)

(https://www.sciencedirect.com/science/article/pii/S2468013320300279 , Jimenez *et al.*, 2020)

Predictive maintenance and fault-tolerance in CPSs 16

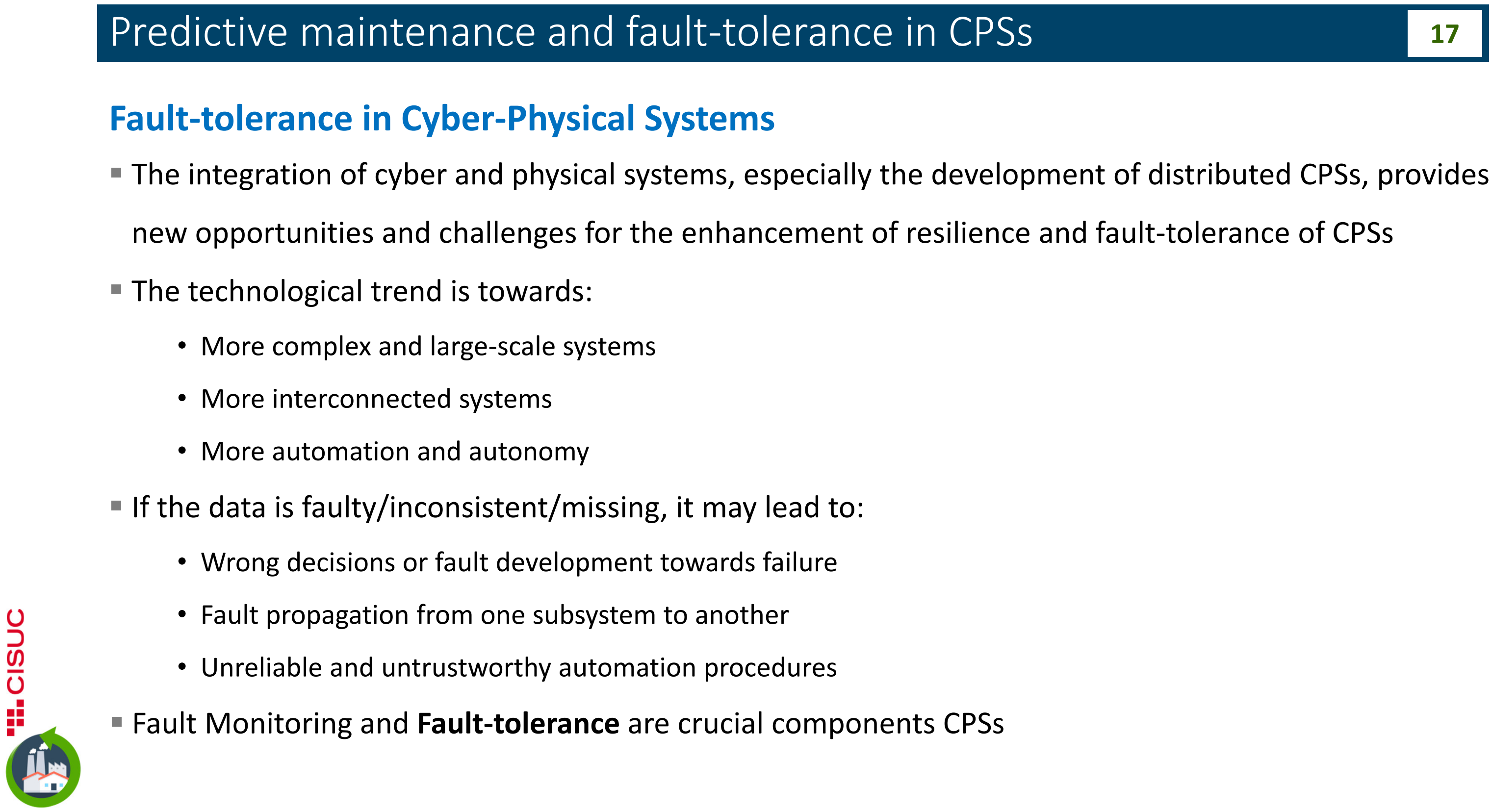
Predictive Maintenance of Cyber-Physical Systems

- Predictive maintenance: from the raw data to the model using a machine learning process


Iterate until data is ready
Iterate to find the best model
Raw Data
Raw Data
Apply pre-processing to data
Prepared Data
Apply learning algorithm to data
Candidate Model
Deploy chosen model
Chosen Model
Data Preprocessing Modules
Machine Learning Algorithms
Applications

(Chappell, 2015)

CISUC



Predictive maintenance and fault-tolerance in CPSs

17

Fault-tolerance in Cyber-Physical Systems

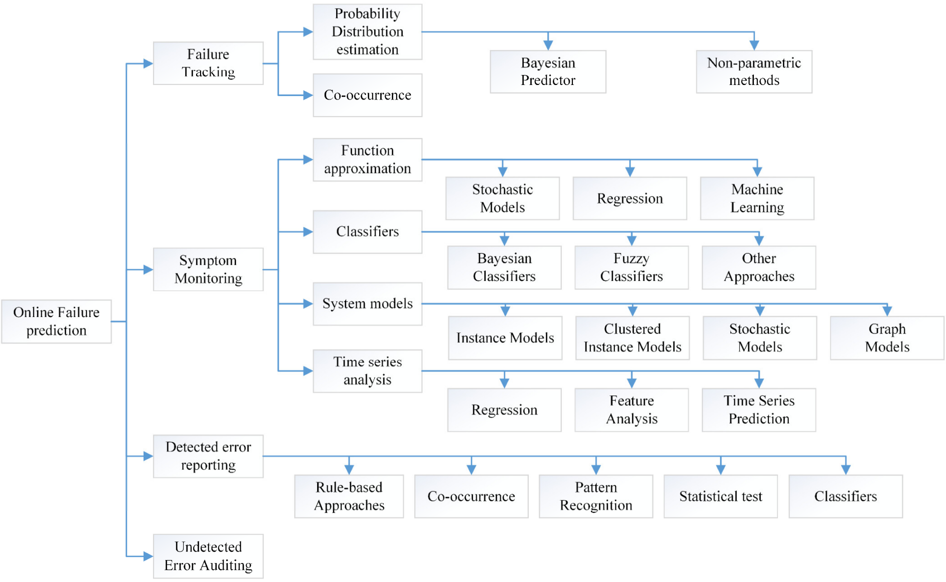
- The integration of cyber and physical systems, especially the development of distributed CPSs, provides new opportunities and challenges for the enhancement of resilience and fault-tolerance of CPSs
- The technological trend is towards:
  - More complex and large-scale systems
  - More interconnected systems
  - More automation and autonomy
- If the data is faulty/inconsistent/missing, it may lead to:
  - Wrong decisions or fault development towards failure
  - Fault propagation from one subsystem to another
  - Unreliable and untrustworthy automation procedures
- Fault Monitoring and **Fault-tolerance** are crucial components CPSs

Predictive maintenance and fault-tolerance in CPSs

18

Fault-tolerance in Cyber-Physical Systems

- A taxonomy for online failure prediction approaches:



Online Failure prediction

Failure Tracking

Probability Distribution estimation

Bayesian Predictor

Non-parametric methods

Co-occurrence

Symptom Monitoring

Function approximation

Stochastic Models

Regression

Machine Learning

Classifiers

Bayesian Classifiers

Fuzzy Classifiers

Other Approaches

System models

Instance Models

Clustered Instance Models

Stochastic Models

Graph Models

Time series analysis

Regression

Feature Analysis

Time Series Prediction

Detected error reporting

Rule-based Approaches

Co-occurrence

Pattern Recognition

Statistical test

Classifiers

Undetected Error Auditing

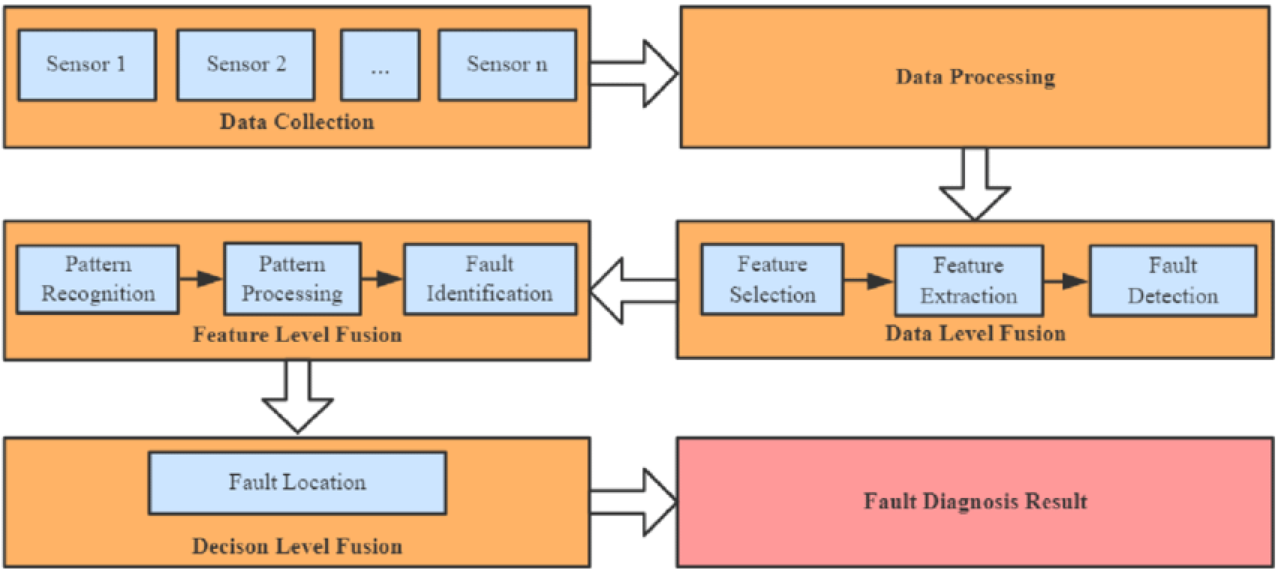
(Zhou *et al.*, 2019)

Predictive maintenance and fault-tolerance in CPSs

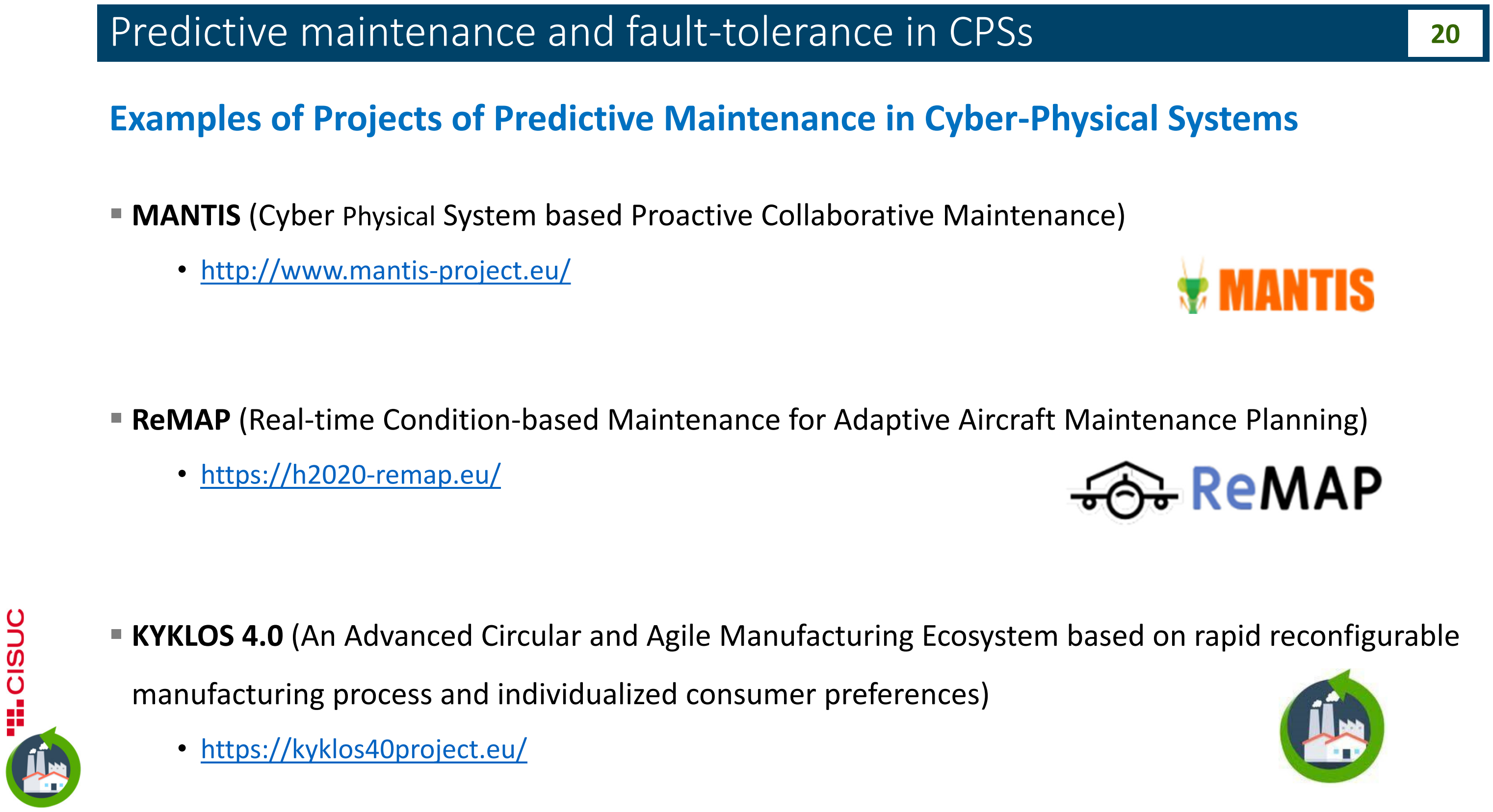
19

Fault-tolerance in Cyber-Physical Systems

- Hierarchical fusion model for fault diagnosis:



(Huang *et al.*, 2020)



Predictive maintenance and fault-tolerance in CPSs

20

Examples of Projects of Predictive Maintenance in Cyber-Physical Systems

- **MANTIS** (Cyber Physical System based Proactive Collaborative Maintenance)
  - http://www.mantis-project.eu/
- **ReMAP** (Real-time Condition-based Maintenance for Adaptive Aircraft Maintenance Planning)
  - https://h2020-remap.eu/
- **KYKLOS 4.0** (An Advanced Circular and Agile Manufacturing Ecosystem based on rapid reconfigurable manufacturing process and individualized consumer preferences)
  - https://kyklos40project.eu/

KYKLOS 4.0

CISUC

Contents

- 1| Predictive maintenance and fault-tolerance in CPSs
- **2| Outliers detection for transient time-series**
- 3| Reduction of the dimension of the data space by "multidimensional scaling" applying several optimization algorithms
- 4| Detection of similarities and prediction of the evolution of the health condition of a machine, as a previous step to estimate the RUL
- 5| References and bibliography

KYKLOS 4.0

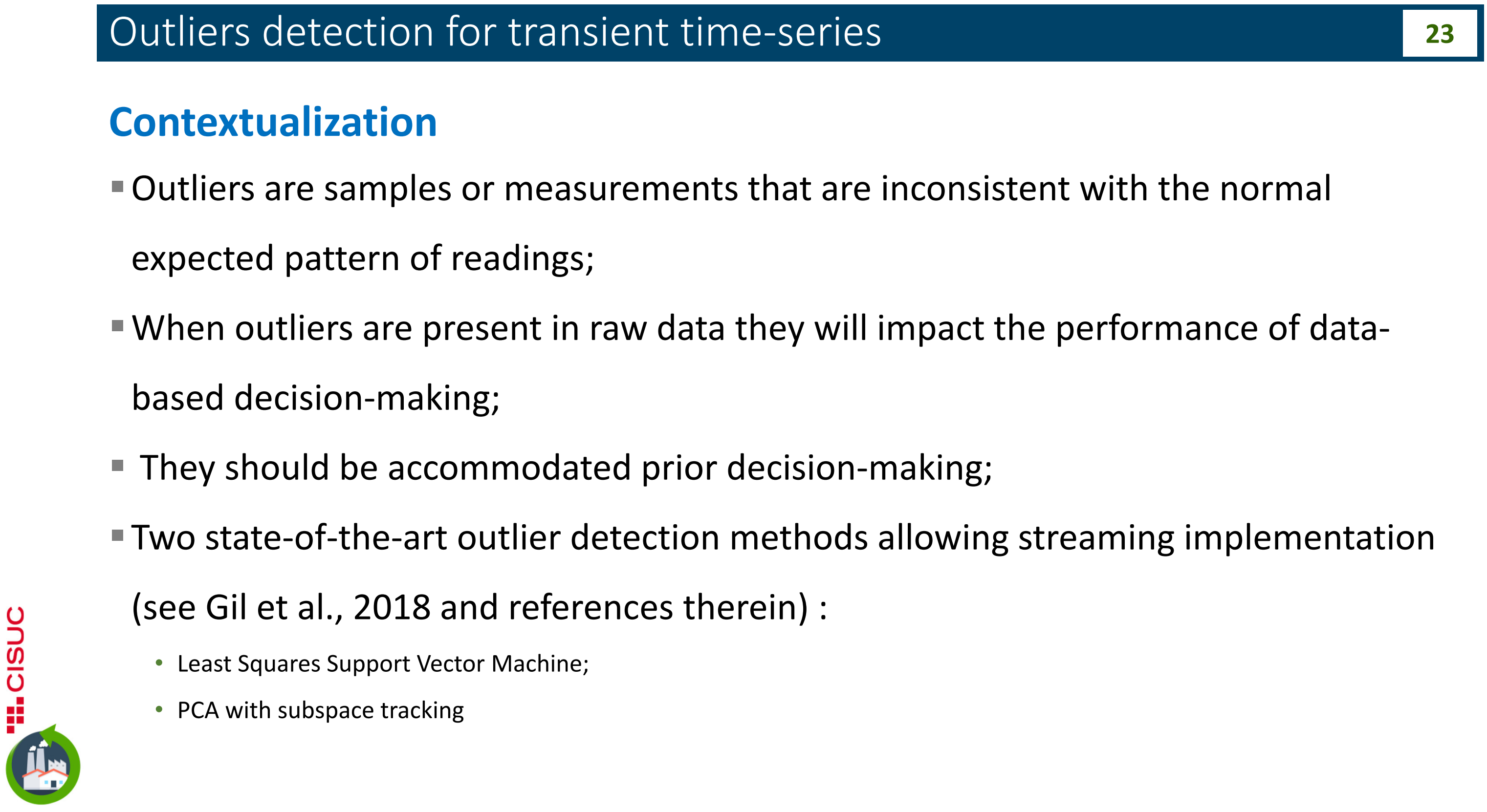
CISUC

Contents

2|

Outliers detection for transient time-series

- Contextualization
- Least Squares Support Vector Machine
- Principal Components Analysis
- Case Study
- Conclusions



Outliers detection for transient time-series

23

Contextualization

- Outliers are samples or measurements that are inconsistent with the normal expected pattern of readings;
- When outliers are present in raw data they will impact the performance of data-based decision-making;
- They should be accommodated prior decision-making;
- Two state-of-the-art outlier detection methods allowing streaming implementation (see Gil et al., 2018 and references therein) :
  - Least Squares Support Vector Machine;
  - PCA with subspace tracking

Outliers detection for transient time-series

Least Squares Support Vector Machine

- Given a sequence $X = \{x_1, \cdots, x_m\} \sim p_0$ (unknown), the problem consists in categorising a new reading x under two hypothesis (H_0, H_1);
- Find a function $f_x(x)$ and a real number b such that:
  - $f_x(x) - b \geq 0 \Rightarrow x$ is a "normal" reading
  - otherwise x is an outlier
- $f_x(x)$ is constructed taking into account 2 constraints:
  - the training set is mostly composed of uncorrupted samples
  - the bound surrounding the "normal" data set should be minimal
- $f_x(x)$ is reduced to a Reproducing Kernel Hilbert Space with kernel:

$$k(x_1, x_2) = exp\left(-\frac{1}{2\sigma^2}\|x_1 - x_2\|^2\right)$$

Outliers detection for transient time-series

Least Squares Support Vector Machine

The optimal solution for the decision function $f(x)$ is:

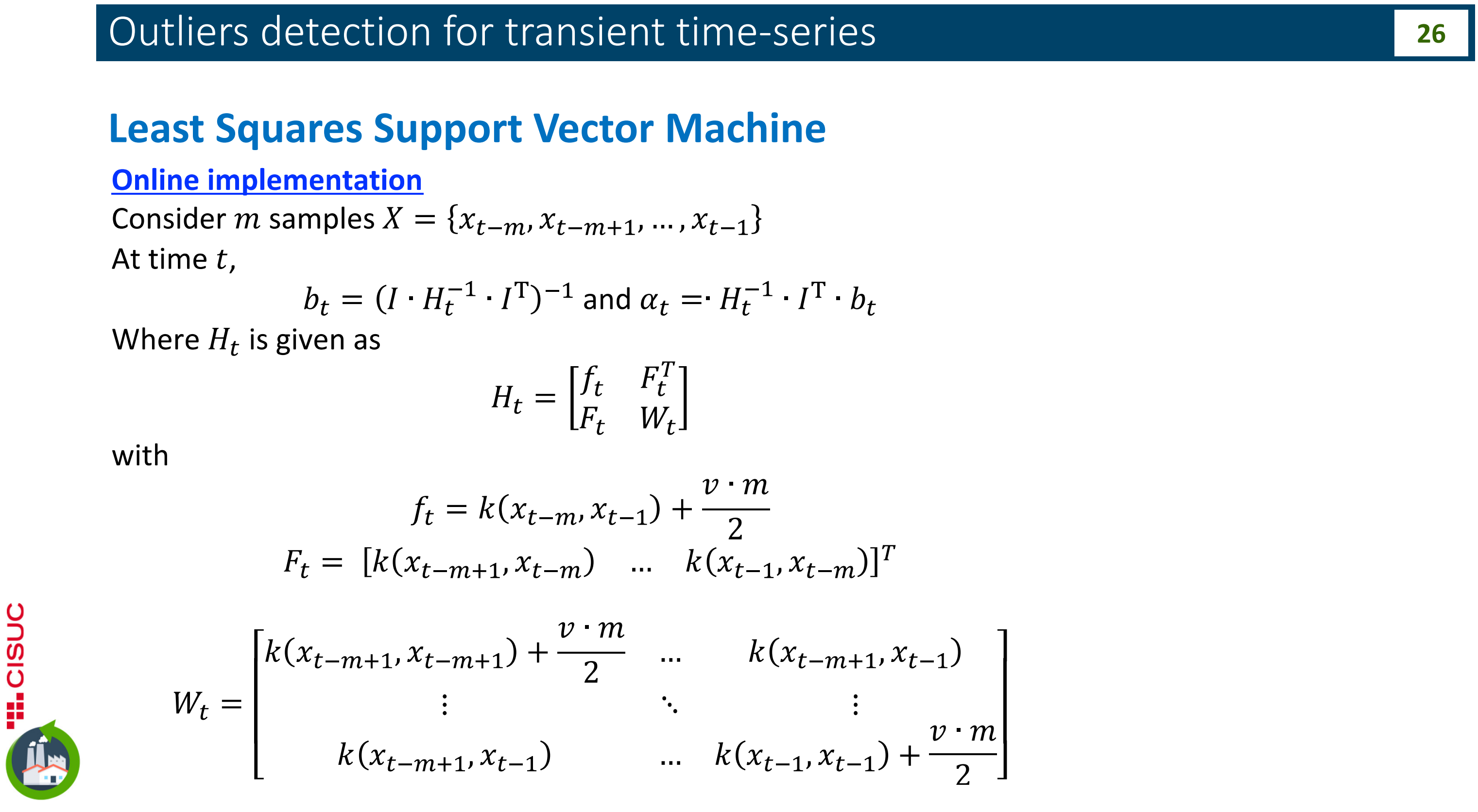
$$f(x) = \sum_{i} \alpha_i k(x, x_i) - b$$

with α and β computed by solving the following linear matrix equation:

$$\begin{bmatrix} 0 & I \\ -I^{\mathrm{T}} & H \end{bmatrix} \begin{bmatrix} b \\ \alpha \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

where H takes the following form:

$$H = \begin{bmatrix} k(x_1, x_1) + \frac{v \cdot m}{2} & \dots & k(x_1, x_m) \\ \vdots & \ddots & \vdots \\ k(x_m, x_1) & \dots & k(x_m, x_m) + \frac{v \cdot m}{2} \end{bmatrix}$$



Outliers detection for transient time-series 26

Least Squares Support Vector Machine

Online implementation

Consider m samples $X = \{x_{t-m}, x_{t-m+1}, \dots, x_{t-1}\}$

At time t,

$$b_t = (I \cdot H_t^{-1} \cdot I^{\mathrm{T}})^{-1} \text{ and } \alpha_t =\cdot H_t^{-1} \cdot I^{\mathrm{T}} \cdot b_t$$

Where H_t is given as

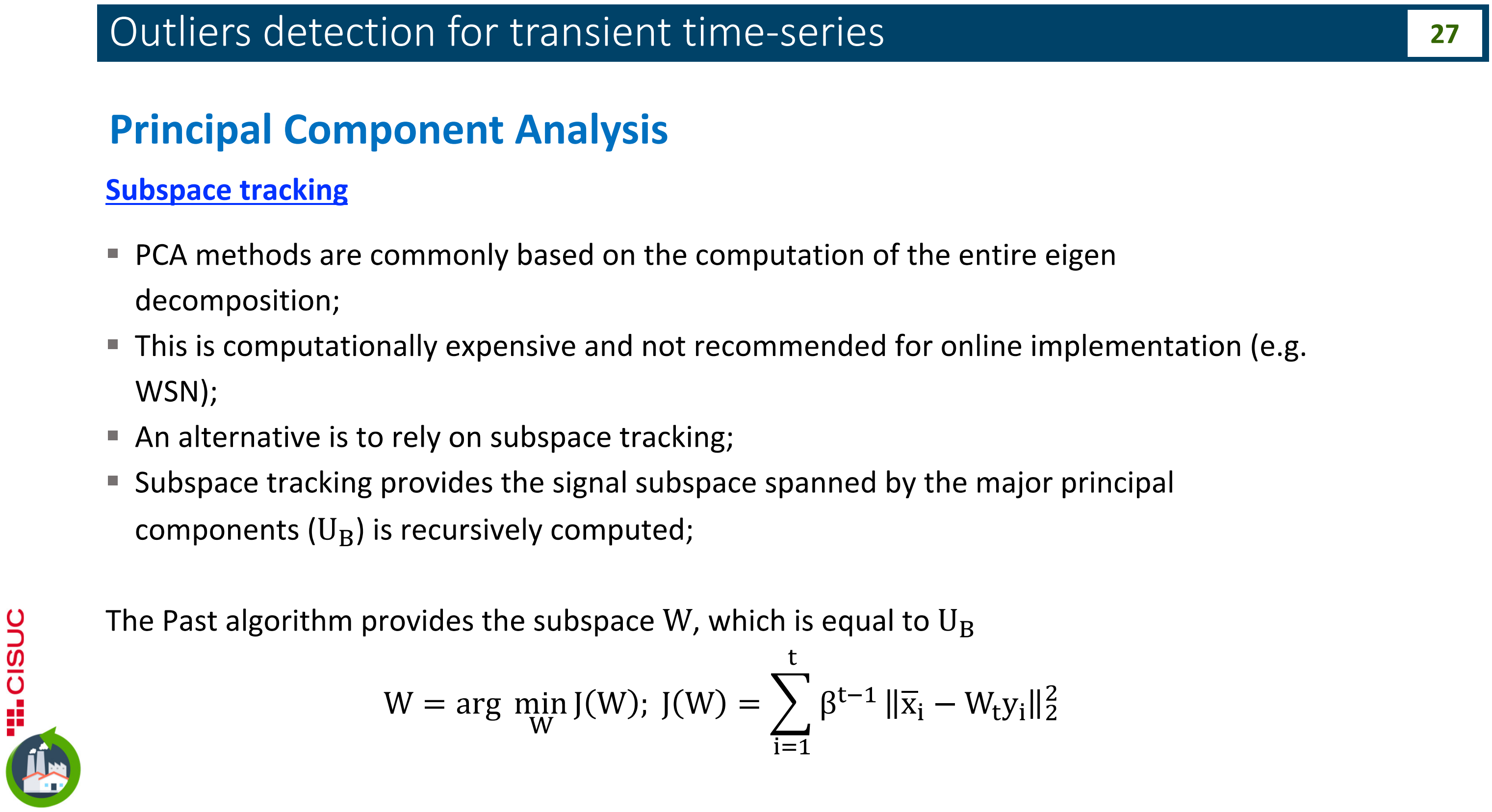
$$H_t = \begin{bmatrix} f_t & F_t^T \\ F_t & W_t \end{bmatrix}$$

with

$$f_t = k(x_{t-m}, x_{t-1}) + \frac{v \cdot m}{2}$$

$$F_t = [k(x_{t-m+1}, x_{t-m}) \quad \dots \quad k(x_{t-1}, x_{t-m})]^T$$

$$W_t = \begin{bmatrix} k(x_{t-m+1}, x_{t-m+1}) + \frac{v \cdot m}{2} & \dots & k(x_{t-m+1}, x_{t-1}) \\ \vdots & \ddots & \vdots \\ k(x_{t-m+1}, x_{t-1}) & \dots & k(x_{t-1}, x_{t-1}) + \frac{v \cdot m}{2} \end{bmatrix}$$



Outliers detection for transient time-series

27

Principal Component Analysis

Subspace tracking

- PCA methods are commonly based on the computation of the entire eigen decomposition;
- This is computationally expensive and not recommended for online implementation (e.g. WSN);
- An alternative is to rely on subspace tracking;
- Subspace tracking provides the signal subspace spanned by the major principal components (U_B) is recursively computed;

The Past algorithm provides the subspace W, which is equal to U_B

$$W = \arg \min_{W} J(W); \; J(W) = \sum_{i=1}^{t} \beta^{t-1} \|\bar{x}_i - W_t y_i\|_2^2$$

©MECO.net

Outliers detection for transient time-series

28

Principal Component Analysis

Discriminants

- The detection of outliers is carried out based on 2 metrics
  - Square Prediction Error

$$\mathrm{SPE(t)} = \left\| \bar{\mathrm{x}}(\mathrm{t}) - \mathrm{U_B(t)U_B^T(t)}\bar{\mathrm{x}}(\mathrm{t}) \right\|_2^2$$

  - Hotteling T^2

$$\mathrm{T^2(t)} = \left\| \bar{\mathrm{x}}^{\mathrm{T}}(\mathrm{t})\mathrm{U_B(t)}\Lambda_{\mathrm{B}}^{-1}(\mathrm{t})\mathrm{U_B^T(t)}\bar{\mathrm{x}}(\mathrm{t}) \right\|_2^2$$

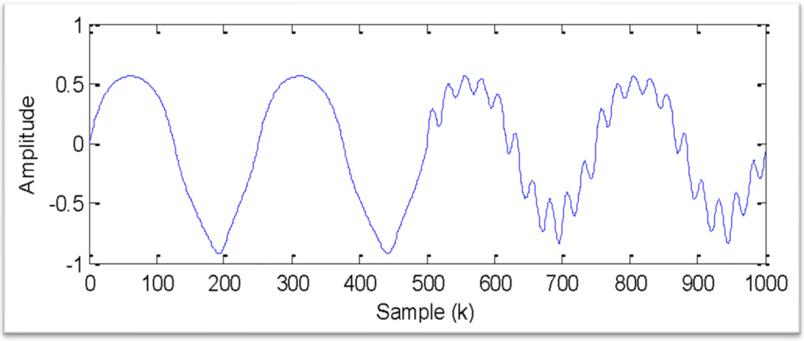
Outliers detection for transient time-series

Case Study

Nonlinear model

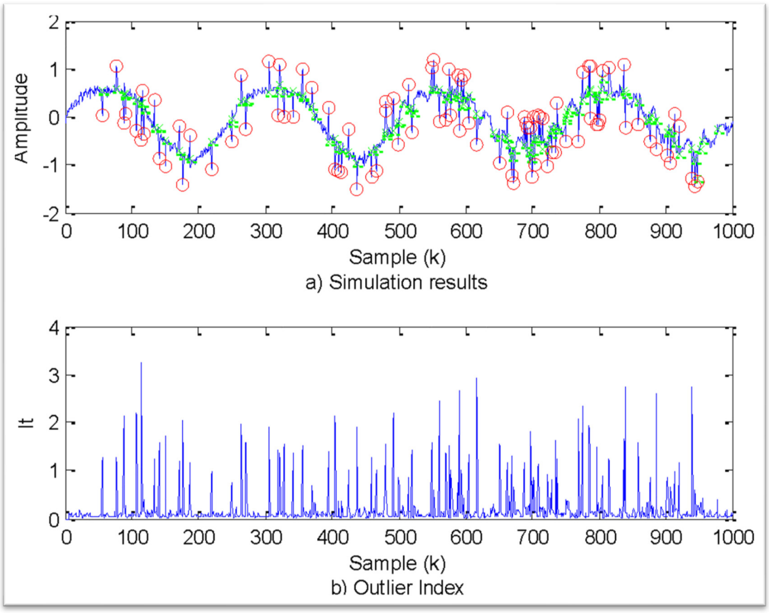
$$y(k) = \frac{y(k-1)y(k-2)y(k-3)u(k-2)[y(k-3)-1]+u(k-1)}{1+y^2(k-2)+y^2(k-3)}$$

$$u(k) = \begin{cases} \sin\left(\frac{2\pi k}{250}\right), & k \leqq 0 \\ 0.8\ \sin\left(\frac{2\pi k}{250}\right) + 0.2\sin\left(\frac{2\pi k}{250}\right), & x > 0 \end{cases}$$



Outliers detection for transient time-series

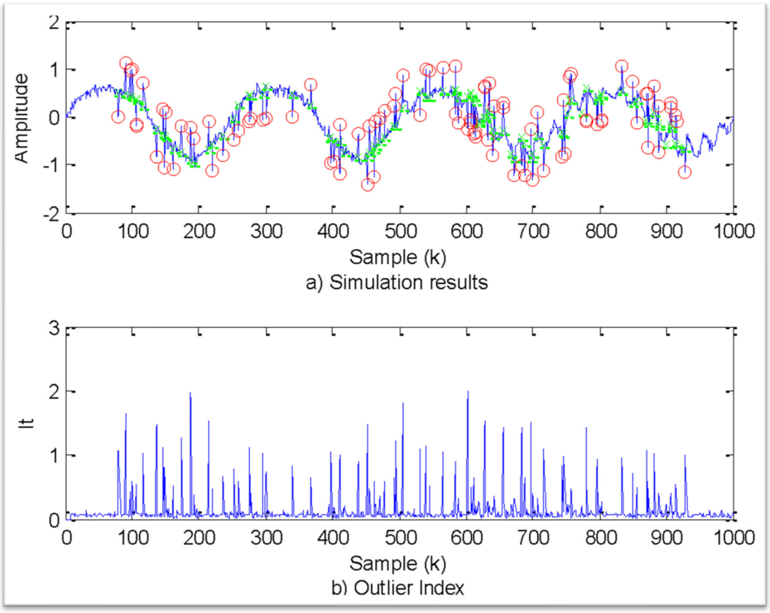
LS-SVM with Standard Gaussian kernel



Outliers detection for transient time-series

31

LS-SVM with modified Gaussian kernel



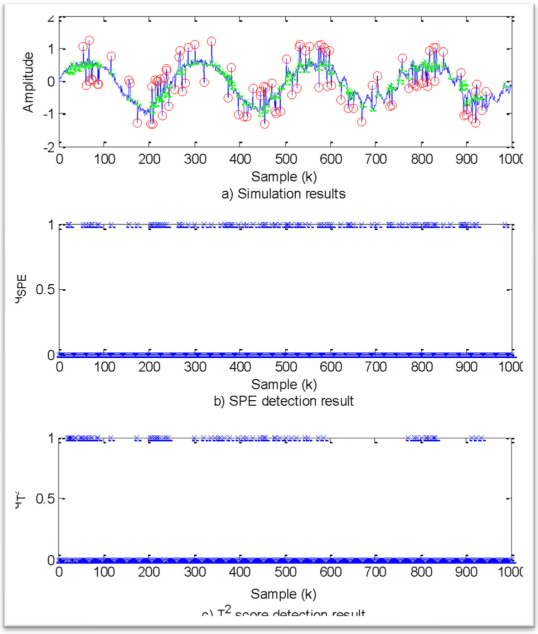
a) Simulation results

b) Outlier Index

Outliers detection for transient time-series

32

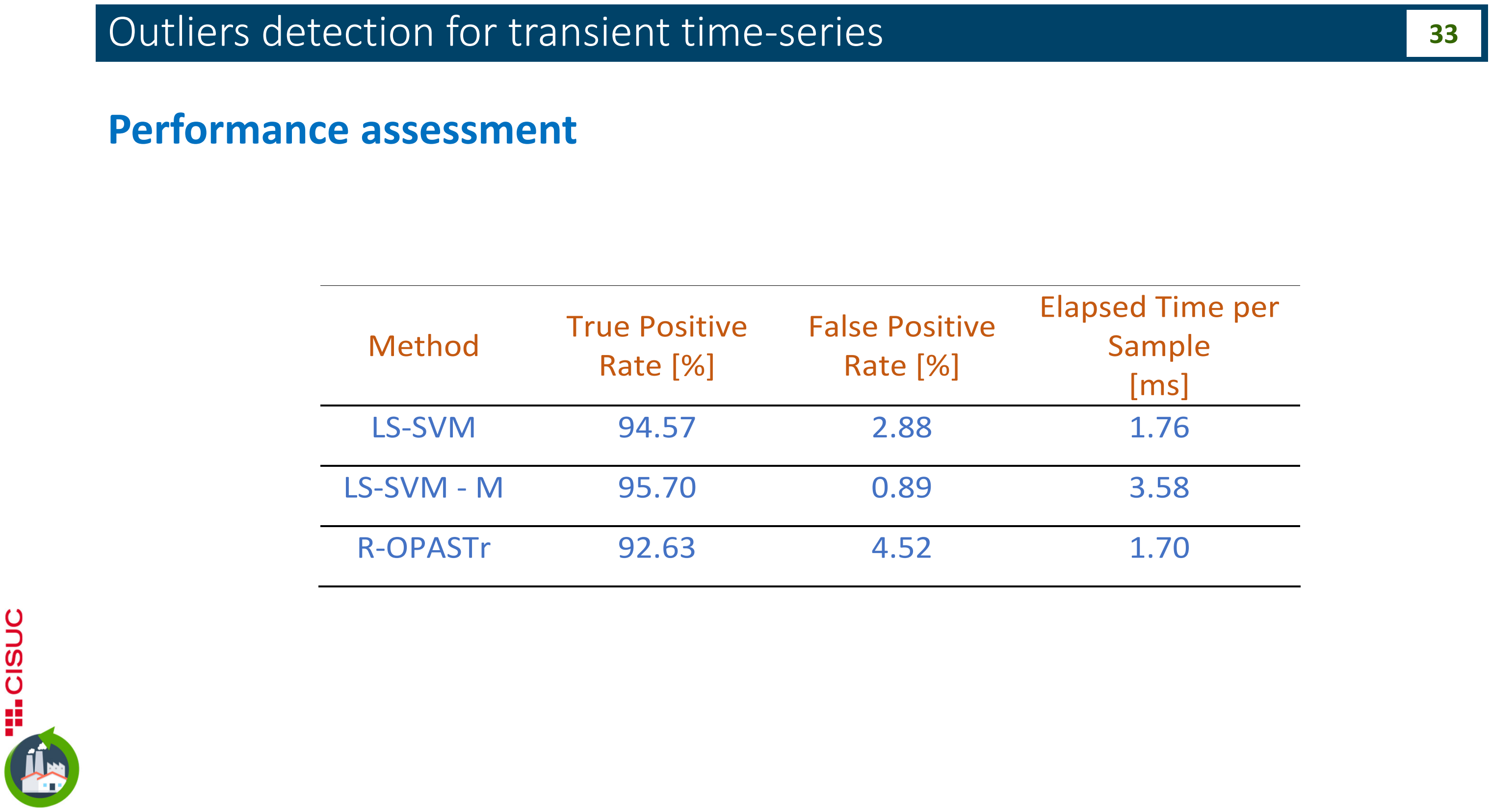
PCA-based approach (R-OPASTr)



a) Simulation results

b) SPE detection result

c) T^2 score detection result

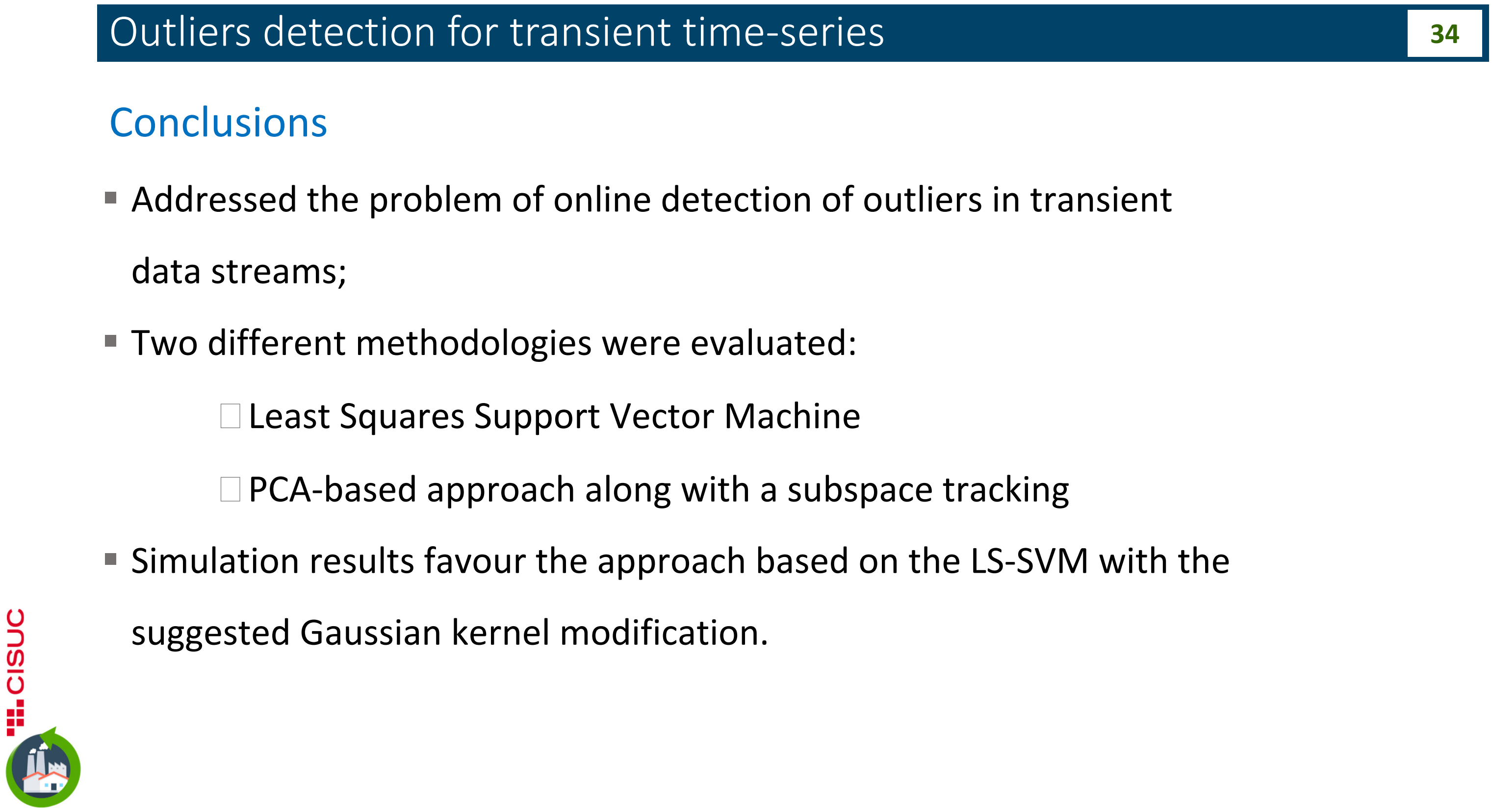


Outliers detection for transient time-series

33

Performance assessment

Method	True Positive Rate [%]	False Positive Rate [%]	Elapsed Time per Sample [ms]
LS-SVM	94.57	2.88	1.76
LS-SVM - M	95.70	0.89	3.58
R-OPASTr	92.63	4.52	1.70



Outliers detection for transient time-series

34

Conclusions

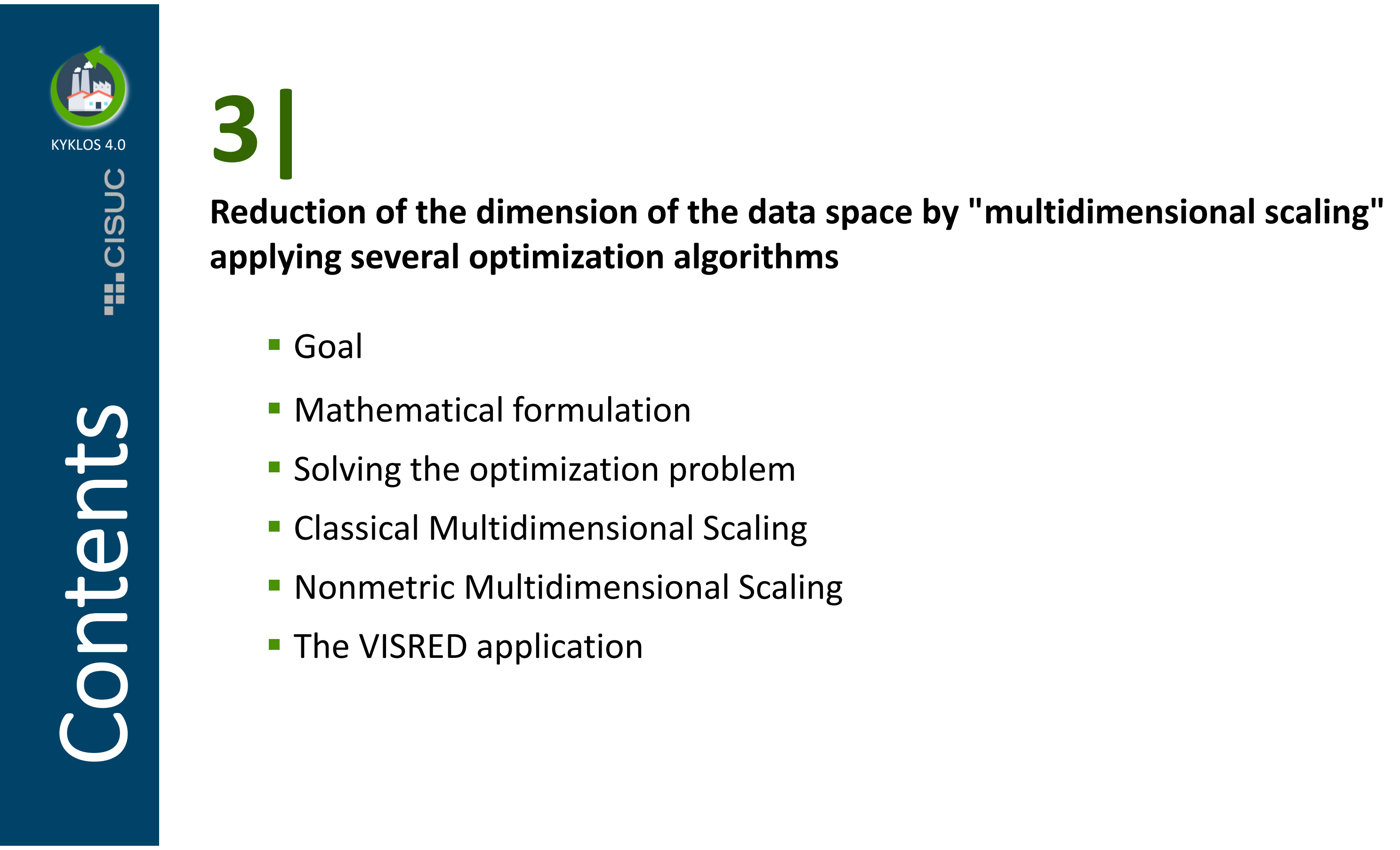
- Addressed the problem of online detection of outliers in transient data streams;
- Two different methodologies were evaluated:
  - □ Least Squares Support Vector Machine
  - □ PCA-based approach along with a subspace tracking
- Simulation results favour the approach based on the LS-SVM with the suggested Gaussian kernel modification.

KYKLOS 4.0

CISUC

Contents

- 1| Predictive maintenance and fault-tolerance in CPSs
- 2| Outliers detection for transient time-series
- **3| Reduction of the dimension of the data space by "multidimensional scaling" applying several optimization algorithms**
- 4| Detection of similarities and prediction of the evolution of the health condition of a machine, as a previous step to estimate the RUL
- 5| References and bibliography

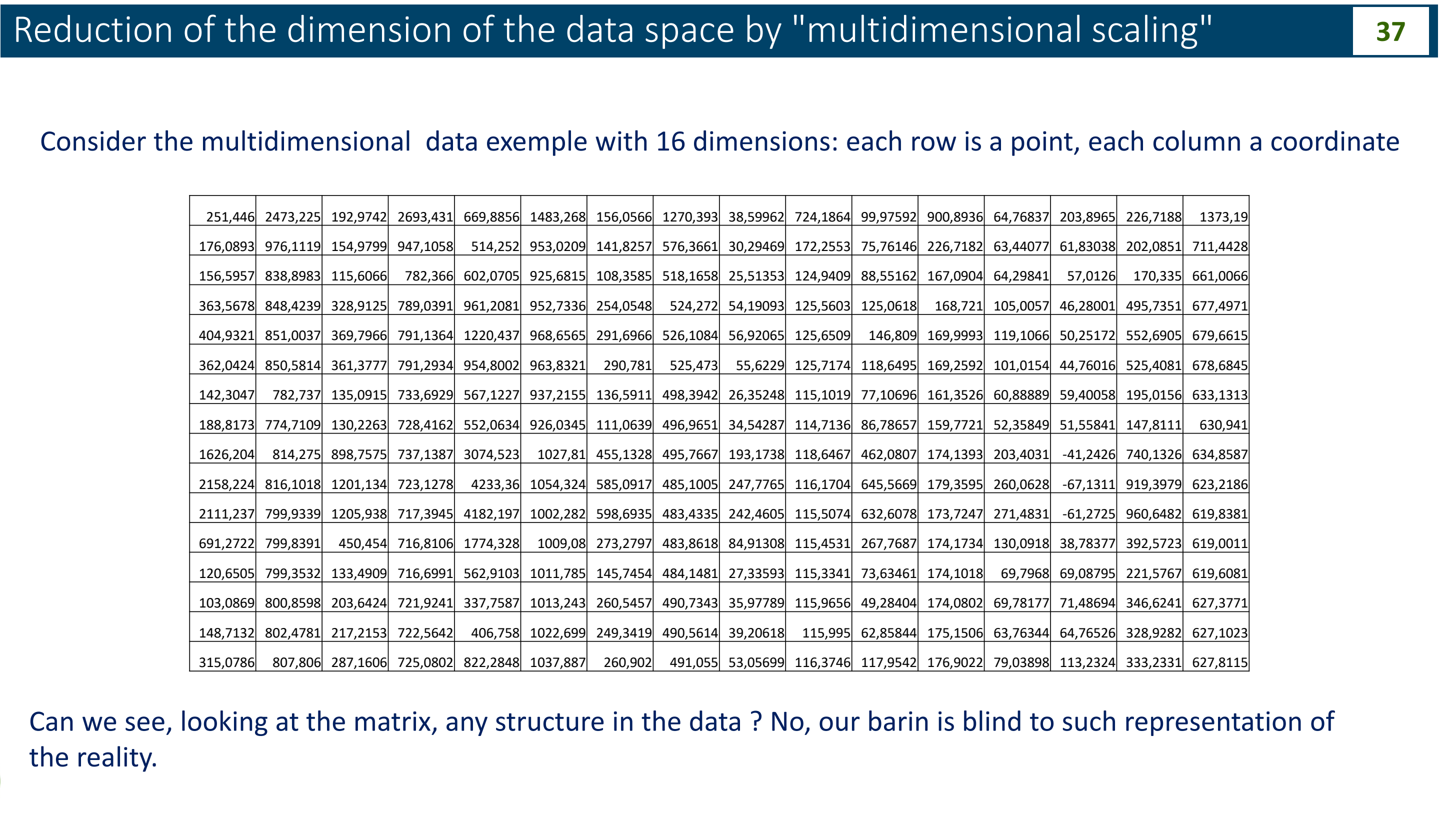


Contents

3|

Reduction of the dimension of the data space by "multidimensional scaling" applying several optimization algorithms

- Goal
- Mathematical formulation
- Solving the optimization problem
- Classical Multidimensional Scaling
- Nonmetric Multidimensional Scaling
- The VISRED application



Reduction of the dimension of the data space by "multidimensional scaling"

37

Consider the multidimensional data exemple with 16 dimensions: each row is a point, each column a coordinate

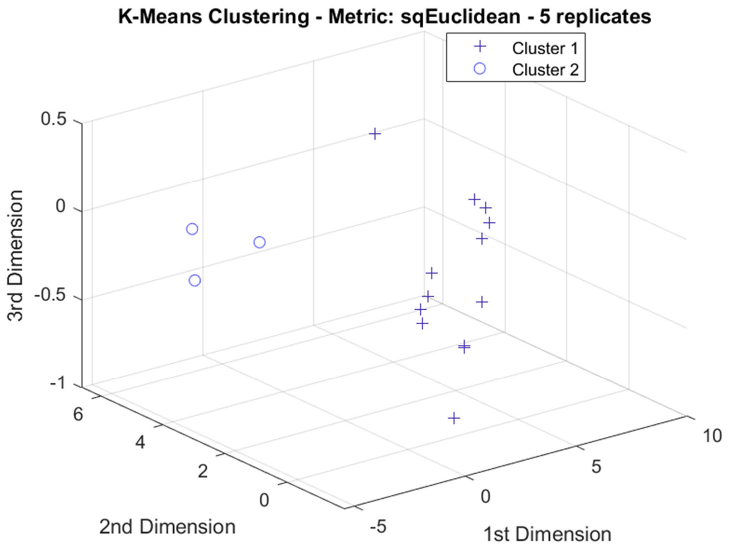
251,446	2473,225	192,9742	2693,431	669,8856	1483,268	156,0566	1270,393	38,59962	724,1864	99,97592	900,8936	64,76837	203,8965	226,7188	1373,19
176,0893	976,1119	154,9799	947,1058	514,252	953,0209	141,8257	576,3661	30,29469	172,2553	75,76146	226,7182	63,44077	61,83038	202,0851	711,4428
156,5957	838,8983	115,6066	782,366	602,0705	925,6815	108,3585	518,1658	25,51353	124,9409	88,55162	167,0904	64,29841	57,0126	170,335	661,0066
363,5678	848,4239	328,9125	789,0391	961,2081	952,7336	254,0548	524,272	54,19093	125,5603	125,0618	168,721	105,0057	46,28001	495,7351	677,4971
404,9321	851,0037	369,7966	791,1364	1220,437	968,6565	291,6966	526,1084	56,92065	125,6509	146,809	169,9993	119,1066	50,25172	552,6905	679,6615
362,0424	850,5814	361,3777	791,2934	954,8002	963,8321	290,781	525,473	55,6229	125,7174	118,6495	169,2592	101,0154	44,76016	525,4081	678,6845
142,3047	782,737	135,0915	733,6929	567,1227	937,2155	136,5911	498,3942	26,35248	115,1019	77,10696	161,3526	60,88889	59,40058	195,0156	633,1313
188,8173	774,7109	130,2263	728,4162	552,0634	926,0345	111,0639	496,9651	34,54287	114,7136	86,78657	159,7721	52,35849	51,55841	147,8111	630,941
1626,204	814,275	898,7575	737,1387	3074,523	1027,81	455,1328	495,7667	193,1738	118,6467	462,0807	174,1393	203,4031	-41,2426	740,1326	634,8587
2158,224	816,1018	1201,134	723,1278	4233,36	1054,324	585,0917	485,1005	247,7765	116,1704	645,5669	179,3595	260,0628	-67,1311	919,3979	623,2186
2111,237	799,9339	1205,938	717,3945	4182,197	1002,282	598,6935	483,4335	242,4605	115,5074	632,6078	173,7247	271,4831	-61,2725	960,6482	619,8381
691,2722	799,8391	450,454	716,8106	1774,328	1009,08	273,2797	483,8618	84,91308	115,4531	267,7687	174,1734	130,0918	38,78377	392,5723	619,0011
120,6505	799,3532	133,4909	716,6991	562,9103	1011,785	145,7454	484,1481	27,33593	115,3341	73,63461	174,1018	69,7968	69,08795	221,5767	619,6081
103,0869	800,8598	203,6424	721,9241	337,7587	1013,243	260,5457	490,7343	35,97789	115,9656	49,28404	174,0802	69,78177	71,48694	346,6241	627,3771
148,7132	802,4781	217,2153	722,5642	406,758	1022,699	249,3419	490,5614	39,20618	115,995	62,85844	175,1506	63,76344	64,76526	328,9282	627,1023
315,0786	807,806	287,1606	725,0802	822,2848	1037,887	260,902	491,055	53,05699	116,3746	117,9542	176,9022	79,03898	113,2324	333,2331	627,8115

Can we see, looking at the matrix, any structure in the data ? No, our barin is blind to such representation of the reality.

Reduction of the dimension of the data space by "multidimensional scaling"

Normalizing the data (zero mean, unit variance), applying MDS and clustering afterwards:

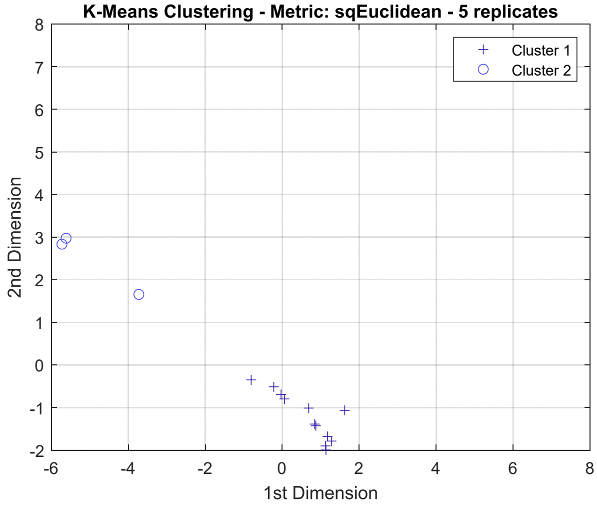
With three dimensions 99% of explained variance is obtained



Now, with 3 dimensions, we can see some structure in the data, and the loss of information is only 1%, with respect to the variance of the original 18 dimensions data .

Reduction of the dimension of the data space by "multidimensional scaling"

Normalizing the data in the same way, applying MDS reducing to two dimensions, still remains 97.64% of explained variance :



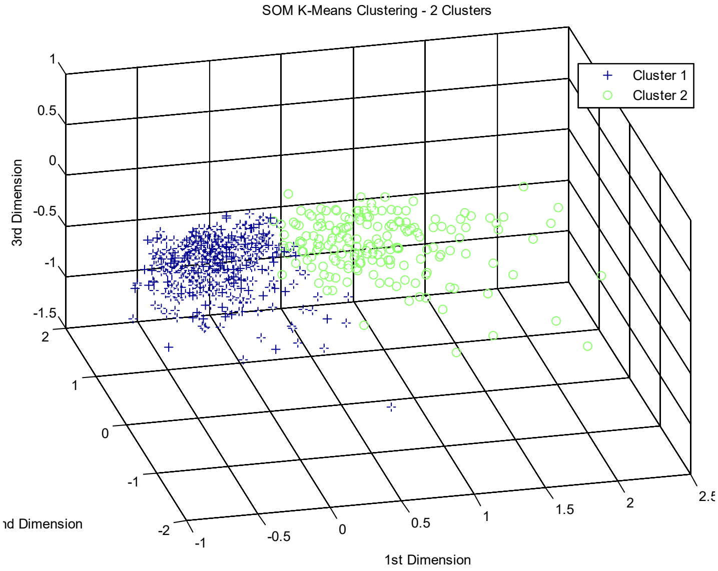
Reducing more to 2 dimensions,, and the loss of information is only 2.36%, with respect to the variance of the original 18 dimensions data.

We can see clearly two classes of points, that may be associated with some properties of the system generating the data (for example one faulty state, one healthy state)

Reduction of the dimension of the data space by "multidimensional scaling"

40

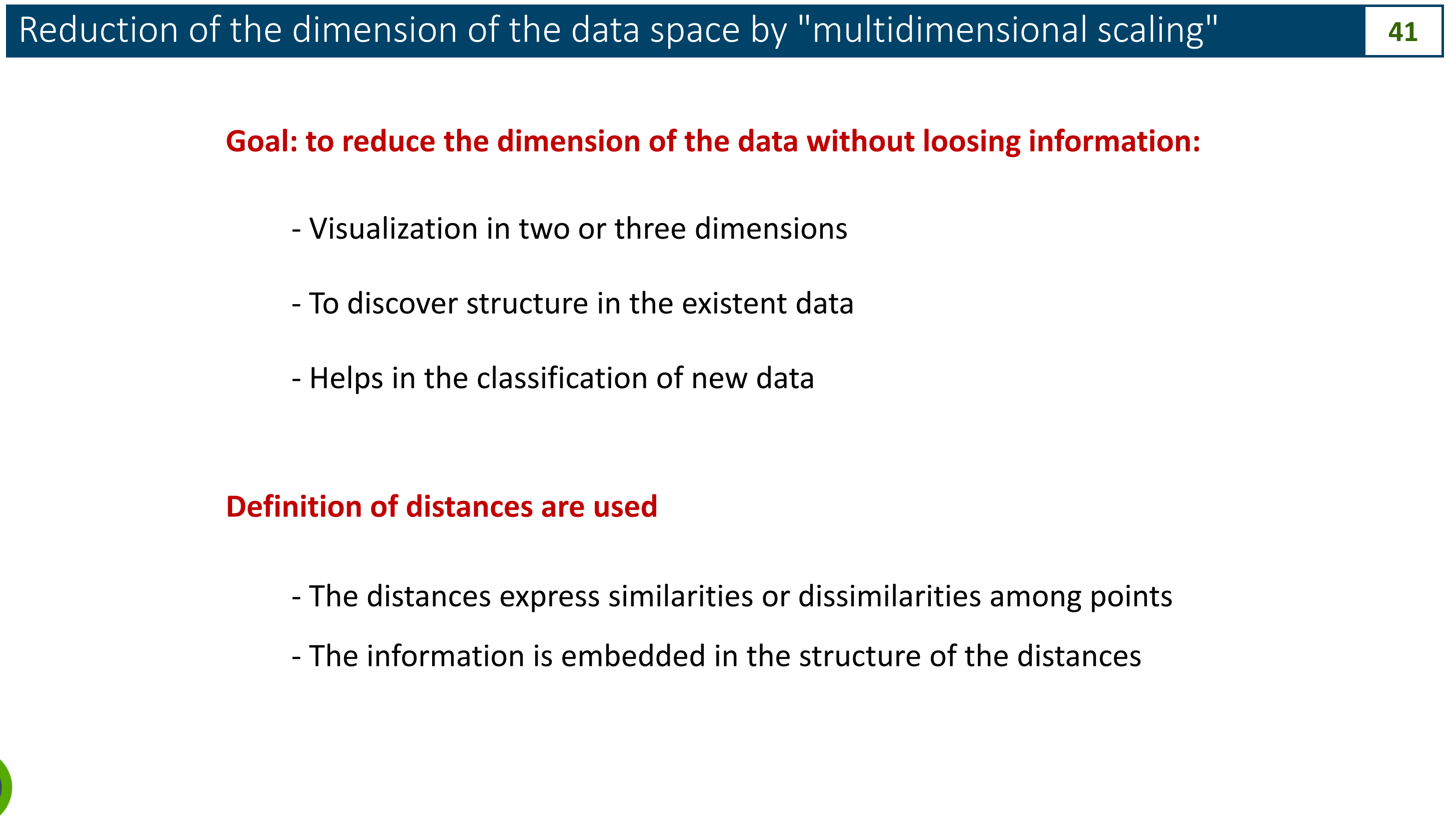
For a big dataset … in 3 dimensions it can give, eventually, after clustering:



When clusters appear visible, structure of the data is discovered, and may be associated to different states of the process.

MDS is a step towards useful knowledge extraction from numerical data

©MECO.net



Reduction of the dimension of the data space by "multidimensional scaling"

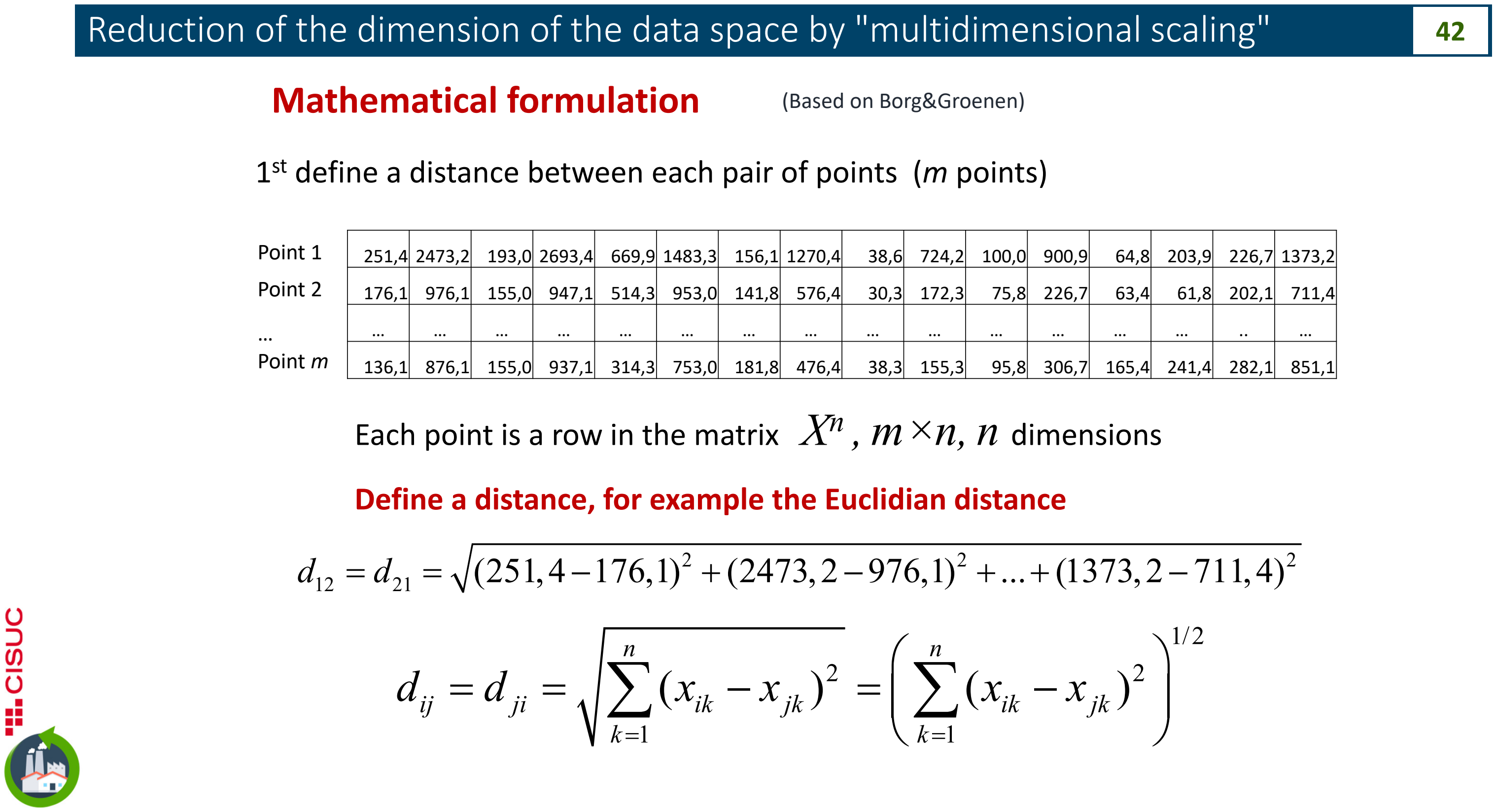
41

Goal: to reduce the dimension of the data without loosing information:

- Visualization in two or three dimensions
- To discover structure in the existent data
- Helps in the classification of new data

Definition of distances are used

- The distances express similarities or dissimilarities among points
- The information is embedded in the structure of the distances



Reduction of the dimension of the data space by "multidimensional scaling"

42

Mathematical formulation

(Based on Borg&Groenen)

1st define a distance between each pair of points (*m* points)

Point 1	251,4	2473,2	193,0	2693,4	669,9	1483,3	156,1	1270,4	38,6	724,2	100,0	900,9	64,8	203,9	226,7	1373,2
Point 2	176,1	976,1	155,0	947,1	514,3	953,0	141,8	576,4	30,3	172,3	75,8	226,7	63,4	61,8	202,1	711,4
…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	..	…
Point *m*	136,1	876,1	155,0	937,1	314,3	753,0	181,8	476,4	38,3	155,3	95,8	306,7	165,4	241,4	282,1	851,1

Each point is a row in the matrix X^n, $m \times n$, n dimensions

Define a distance, for example the Euclidian distance

$$d_{12} = d_{21} = \sqrt{(251,4-176,1)^2 + (2473,2-976,1)^2 + \ldots + (1373,2-711,4)^2}$$

$$d_{ij} = d_{ji} = \sqrt{\sum_{k=1}^{n} (x_{ik} - x_{jk})^2} = \left(\sum_{k=1}^{n} (x_{ik} - x_{jk})^2 \right)^{1/2}$$

Reduction of the dimension of the data space by "multidimensional scaling"

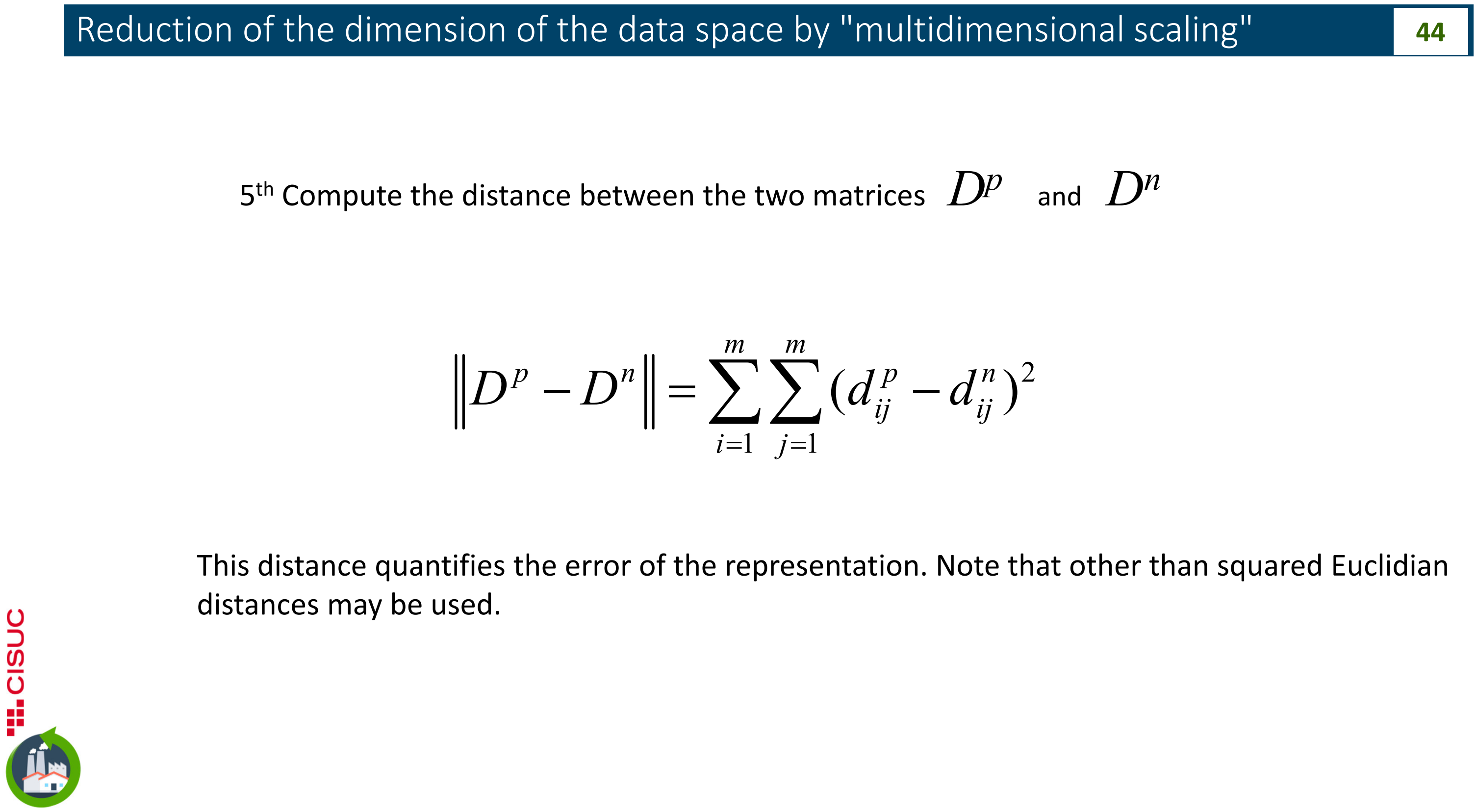
2nd Construct the matrix of distances, *dissimilarity matrix,* in the original space

Matrix D^n, square (*mxm*), symmetric, d^n_{ij} is the distance between point *i* and point *j*

3rd Chose *m* points in a space of *p* dimensions, *p* << *n*, each one is a row of the matrix Y^p

4th Compute the distances between each pair of points in the *p*-dimensional space, obtaining the dissimilarity matrix in the reduced space.

Matrix D^p, squared (*mxm*), symmetric, d^p_{ij} is the distance between point *i* and point *j*



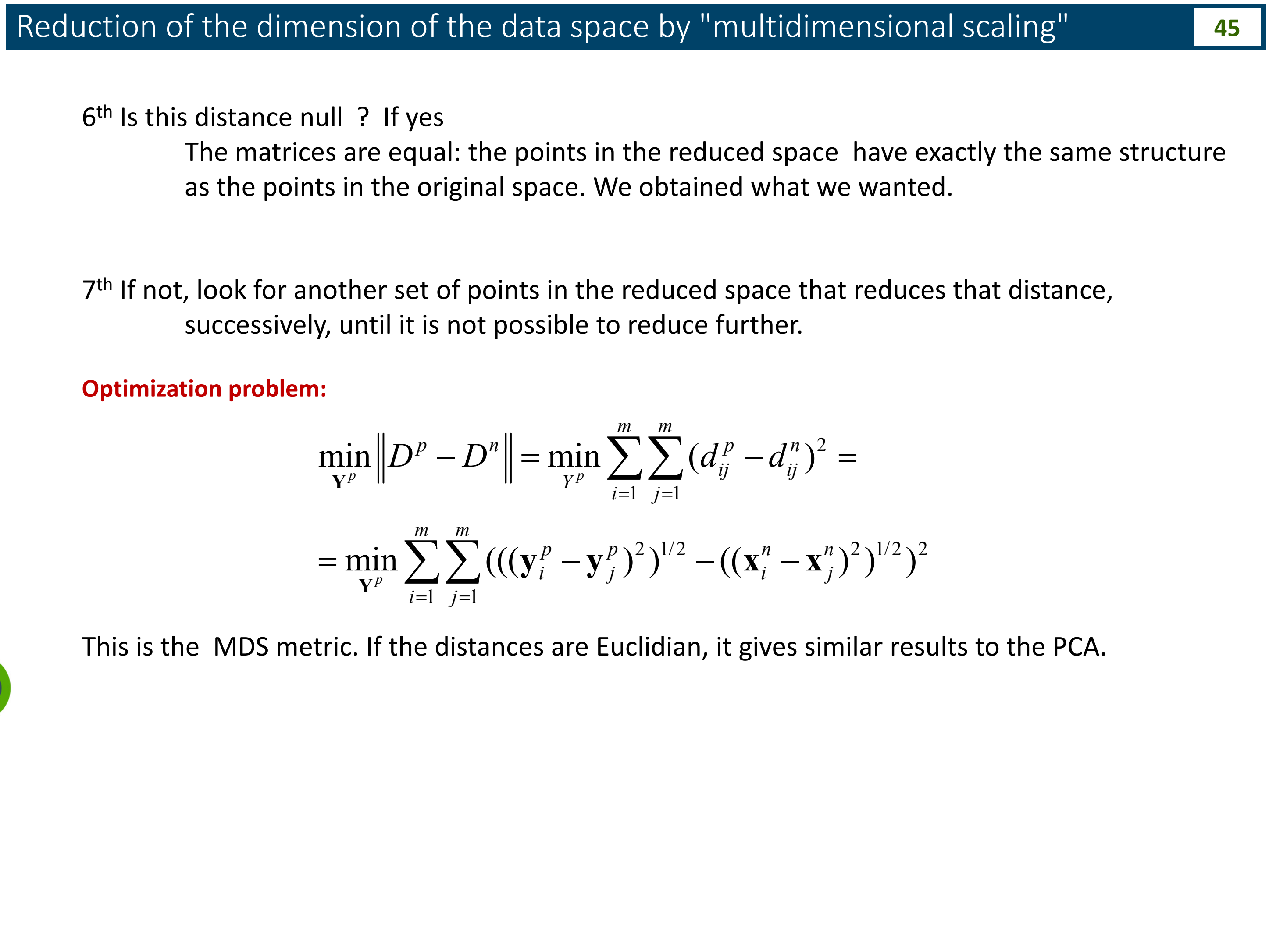
Reduction of the dimension of the data space by "multidimensional scaling"

44

5th Compute the distance between the two matrices D^p and D^n

$$\left\| D^p - D^n \right\| = \sum_{i=1}^{m} \sum_{j=1}^{m} (d_{ij}^{p} - d_{ij}^{n})^2$$

This distance quantifies the error of the representation. Note that other than squared Euclidian distances may be used.



Reduction of the dimension of the data space by "multidimensional scaling"

45

6th Is this distance null ? If yes

The matrices are equal: the points in the reduced space have exactly the same structure as the points in the original space. We obtained what we wanted.

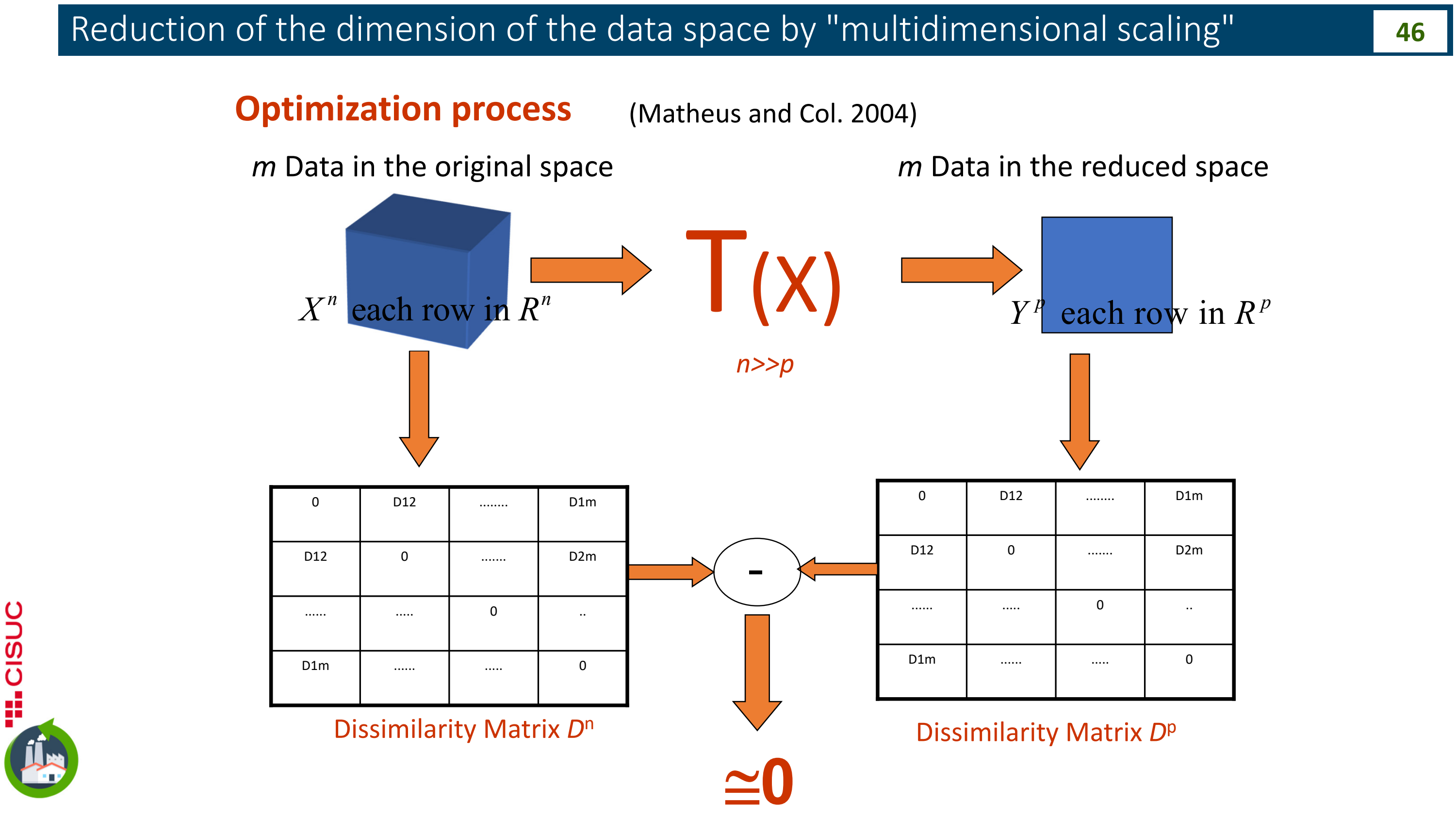
7th If not, look for another set of points in the reduced space that reduces that distance, successively, until it is not possible to reduce further.

Optimization problem:

$$\min_{\mathbf{Y}^p} \left\| D^p - D^n \right\| = \min_{Y^p} \sum_{i=1}^{m} \sum_{j=1}^{m} (d_{ij}^p - d_{ij}^n)^2 =$$

$$= \min_{\mathbf{Y}^p} \sum_{i=1}^{m} \sum_{j=1}^{m} (((\mathbf{y}_i^p - \mathbf{y}_j^p)^2)^{1/2} - ((\mathbf{x}_i^n - \mathbf{x}_j^n)^2)^{1/2})^2$$

This is the MDS metric. If the distances are Euclidian, it gives similar results to the PCA.



Reduction of the dimension of the data space by "multidimensional scaling"

46

Optimization process (Matheus and Col. 2004)

m Data in the original space

m Data in the reduced space

X^n each row in R^n

T(X)

n>>p

Y^p each row in R^p

0	D12	....	D1m
D12	0	....	D2m
......	.....	0	..
D1m	......	.....	0

Dissimilarity Matrix D^n

-

≅0

0	D12	....	D1m
D12	0	....	D2m
......	.....	0	..
D1m	......	.....	0

Dissimilarity Matrix D^p

©MECO.net

Reduction of the dimension of the data space by "multidimensional scaling" 47

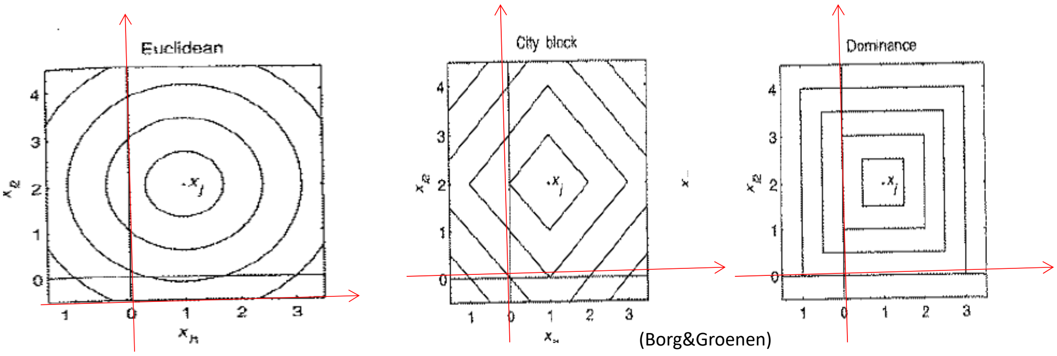
Other common distances between two points with *n* dimensions

Euclidian → $\delta_{ij} = \left(\sum_{a=1}^{n} (x_{ia} - x_{ja})^2 \right)^{1/2}$

City-block or Manhattan → $\delta_{ij} = \sum_{a=1}^{n} \left| x_{ia} - x_{ja} \right|$

Dominance or Chebychev → $\delta_{ij} = \max_{a=1}^{n} \left| x_{ia} - x_{ja} \right|$

Geometric places of the points equidistant from x_i



(Borg&Groenen)

Reduction of the dimension of the data space by "multidimensional scaling"

48

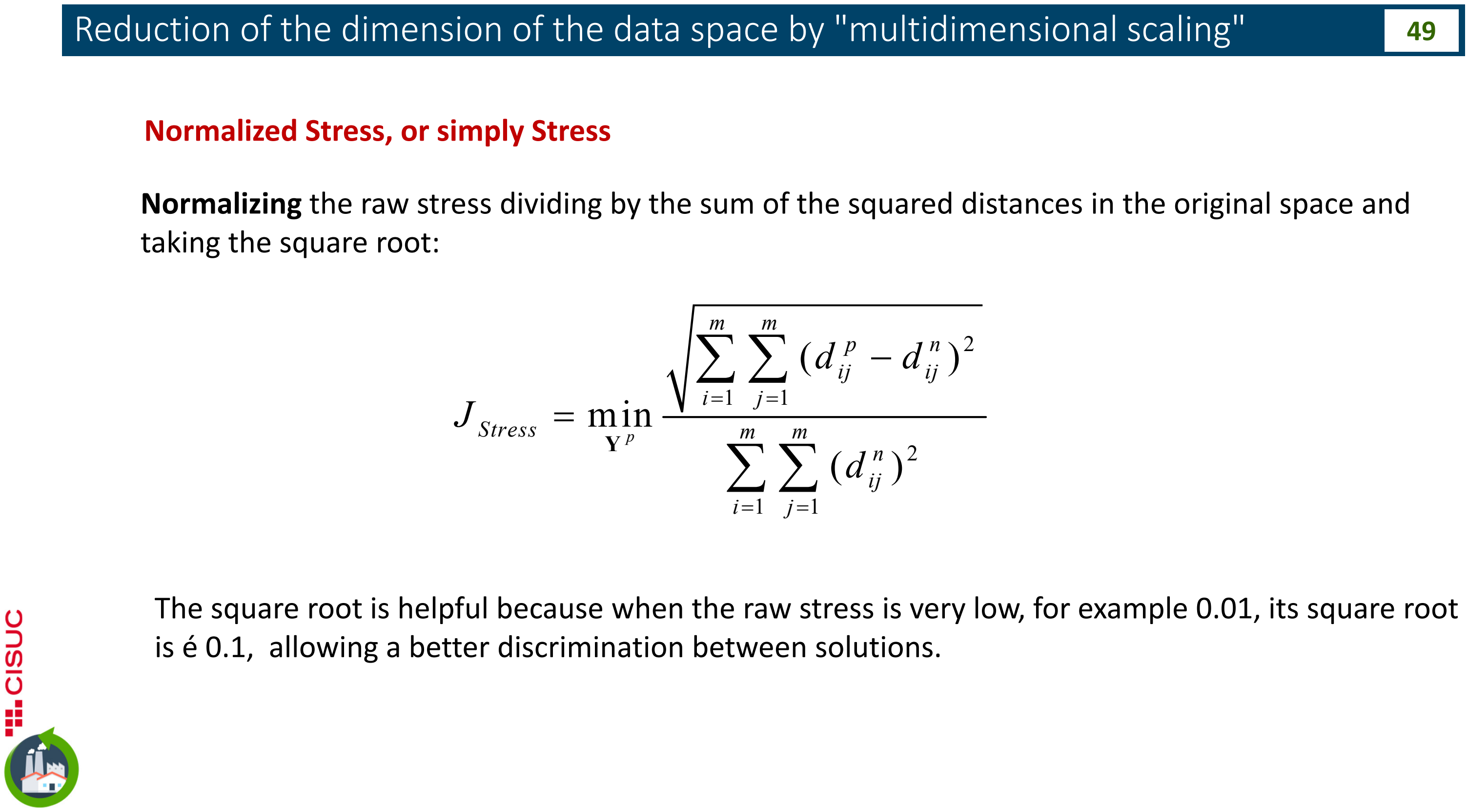
Other criteria for the difference between the two dissimilarity matrices

Raw stress

$$\min_{\mathbf{Y}^p} \left\| D^p - D^n \right\| = \min_{\mathbf{Y}^p} \sum_{i=1}^{m} \sum_{j=1}^{m} (d_{ij}^p - d_{ij}^n)^2 =$$

$$= \min_{\mathbf{Y}^p} \sum_{i=1}^{m} \sum_{j=1}^{m} ((\mathbf{y}_i^p - \mathbf{y}_j^p)^2 - (\mathbf{x}_i^n - \mathbf{x}_j^n)^2)^2$$

It can take high values even if the dimension reduction is not bad. Depends on the scale.



Reduction of the dimension of the data space by "multidimensional scaling"

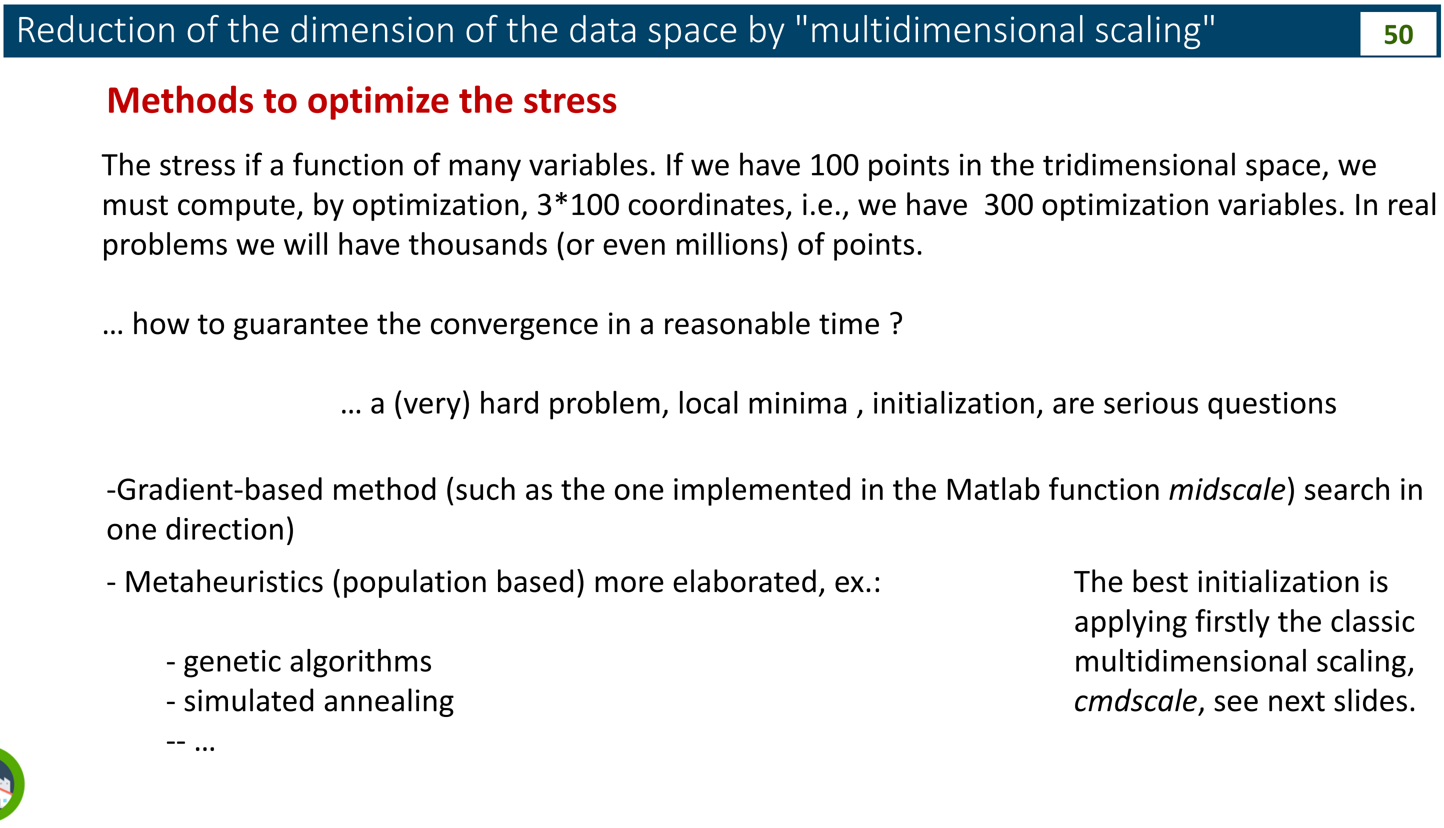
49

Normalized Stress, or simply Stress

Normalizing the raw stress dividing by the sum of the squared distances in the original space and taking the square root:

$$J_{Stress} = \min_{\mathbf{Y}^p} \frac{\sqrt{\sum_{i=1}^{m} \sum_{j=1}^{m} (d_{ij}^{p} - d_{ij}^{n})^2}}{\sum_{i=1}^{m} \sum_{j=1}^{m} (d_{ij}^{n})^2}$$

The square root is helpful because when the raw stress is very low, for example 0.01, its square root is é 0.1, allowing a better discrimination between solutions.



Reduction of the dimension of the data space by "multidimensional scaling" 50

Methods to optimize the stress

The stress if a function of many variables. If we have 100 points in the tridimensional space, we must compute, by optimization, 3*100 coordinates, i.e., we have 300 optimization variables. In real problems we will have thousands (or even millions) of points.

… how to guarantee the convergence in a reasonable time ?

… a (very) hard problem, local minima , initialization, are serious questions

-Gradient-based method (such as the one implemented in the Matlab function *midscale*) search in one direction)

- Metaheuristics (population based) more elaborated, ex.:

  - genetic algorithms
  - simulated annealing
  -- …

The best initialization is applying firstly the classic multidimensional scaling, *cmdscale*, see next slides.

Reduction of the dimension of the data space by "multidimensional scaling" 51

CMDS Classical multidimensional scaling

This classic method uses the following steps:

1- Compute the matrix $D=D^n$ (square symmetric matrix, in the original space)
2- Compute D^2 squaring each element of D
3- From D^2 generate the matrix doubled centered (by row and by column) B_D

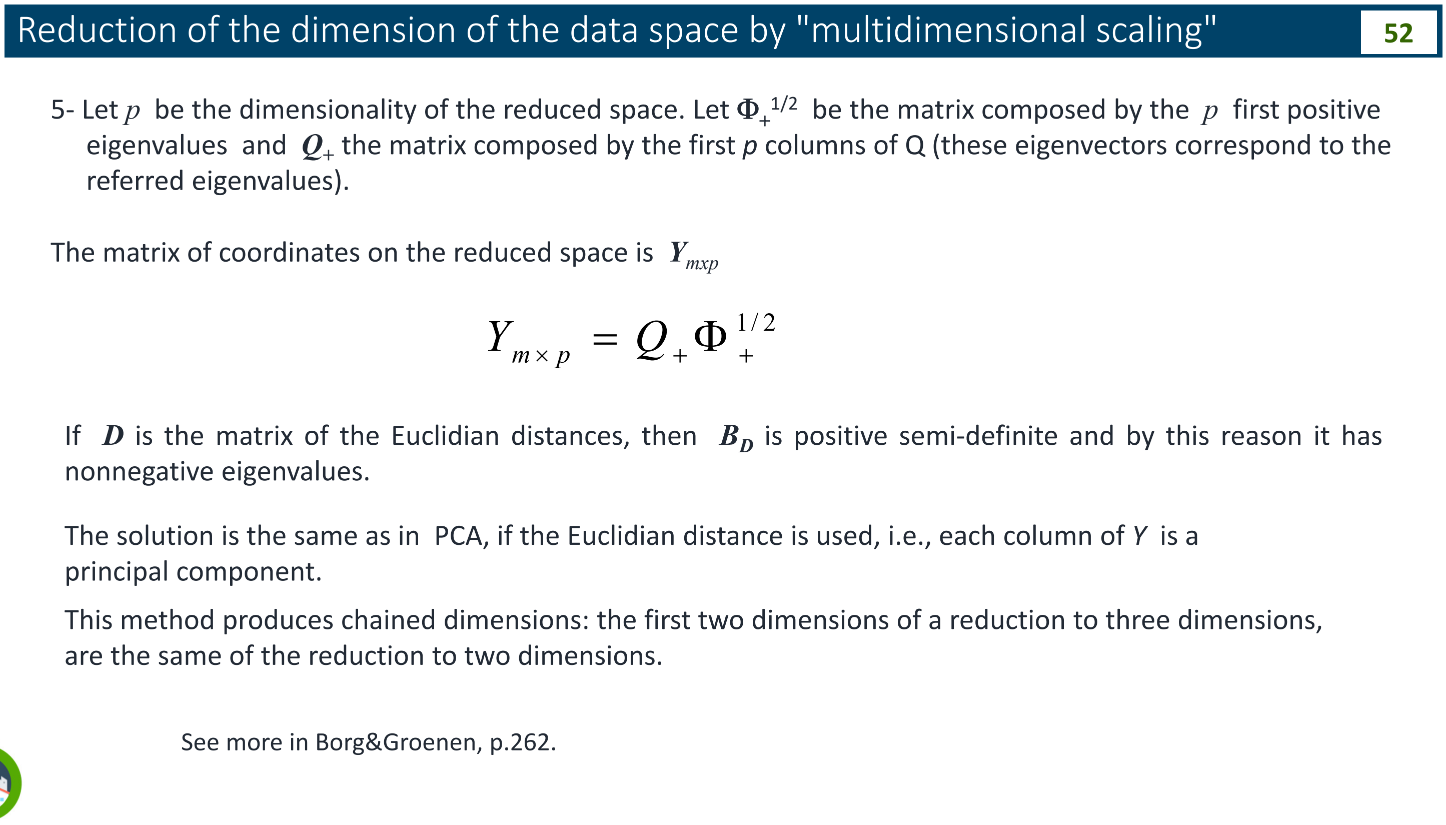
$$B_D = \frac{-1}{2} J D^2 J$$

The matrix $\boldsymbol{J}$ is the centering matrix $\boldsymbol{J} = \boldsymbol{I} - (m^{-1})\mathbf{1}\mathbf{1}^{\mathrm{T}}$ where **1** is the column vector composed by 1's. *m* is the number of points, i.e., the number of rows or of columns of the matrix *D.*

4- Compute the eigenvalues and eigenvectors of $\boldsymbol{B_D}$

$$B_D = Q \Phi Q^T$$

by the theorem of the constituent matrices, Φ is the diagonal matrix of the eigenvalues by decreasing order, and $\boldsymbol{Q}$ is the matrix of the corresponding eigenvectors. Let $\Phi^{1/2}$ be the diagonal matrix where each element is the square root of the corresponding element of Φ.



Reduction of the dimension of the data space by "multidimensional scaling"

52

5- Let p be the dimensionality of the reduced space. Let $\Phi_+^{1/2}$ be the matrix composed by the p first positive eigenvalues and $\boldsymbol{Q}_+$ the matrix composed by the first *p* columns of Q (these eigenvectors correspond to the referred eigenvalues).

The matrix of coordinates on the reduced space is $\boldsymbol{Y}_{mxp}$

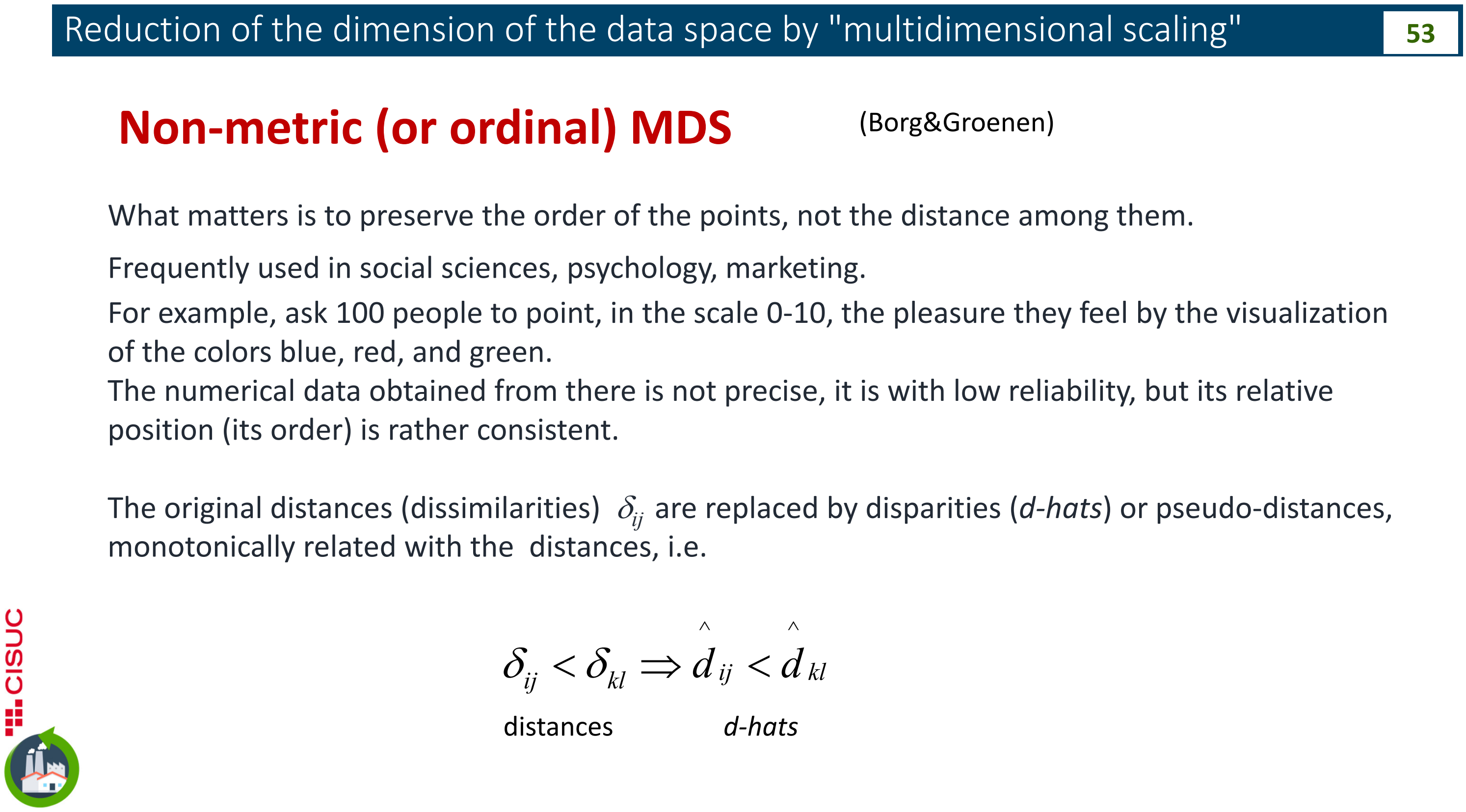
$$Y_{m \times p} = Q_+ \Phi_+^{1/2}$$

If $\boldsymbol{D}$ is the matrix of the Euclidian distances, then $\boldsymbol{B_D}$ is positive semi-definite and by this reason it has nonnegative eigenvalues.

The solution is the same as in PCA, if the Euclidian distance is used, i.e., each column of *Y* is a principal component.

This method produces chained dimensions: the first two dimensions of a reduction to three dimensions, are the same of the reduction to two dimensions.

See more in Borg&Groenen, p.262.



Reduction of the dimension of the data space by "multidimensional scaling" 53

Non-metric (or ordinal) MDS

(Borg&Groenen)

What matters is to preserve the order of the points, not the distance among them.

Frequently used in social sciences, psychology, marketing.

For example, ask 100 people to point, in the scale 0-10, the pleasure they feel by the visualization of the colors blue, red, and green.
The numerical data obtained from there is not precise, it is with low reliability, but its relative position (its order) is rather consistent.

The original distances (dissimilarities) δ_{ij} are replaced by disparities (*d-hats*) or pseudo-distances, monotonically related with the distances, i.e.

$$\delta_{ij} < \delta_{kl} \Rightarrow \hat{d}_{ij} < \hat{d}_{kl}$$

distances *d-hats*

Reduction of the dimension of the data space by "multidimensional scaling" 54

Given a set of dissimilarities $\{\delta_{ij}\}$, compute a representation, in a reduced space *p*, whose distances (for example Euclidian) $\{d_{ij}\}$ between points i and j have the same order as the $\{\delta_{ij}\}$.

The objective function to be minimized is

$$J_{Stress1} = \min_{\mathbf{Y}^p} \frac{\sqrt{\sum_{i<j}(d_{ij}^p - \overset{\wedge\ p}{d}_{ij})^2}}{\sum_{i<j}(d_{ij}^p)^2} \qquad \text{or} \qquad J_{Stress2} = \min_{\mathbf{Y}^p} \frac{\sqrt{\sum_{i<j}(d_{ij}^p - \overset{\wedge\ p}{d}_{ij})^2}}{\sum_{i<j}(d_{ij}^p - \bar{d})^2}$$

$\bar{d}$ is the average distance

Using the gradient method (steepest descent) to minimize *J ,* one obtains the algorithm of Shepard-Kruskal. It is necessary to compute the $d^{\wedge}_{ij}$ from the δ_{ij} .

Reduction of the dimension of the data space by "multidimensional scaling" 55

Algorithm of Shepard-Kruskal (Kruskal and Coll.)

1- Given the dissimilarities (original distances) $\{\delta_{ij}\}$, initialize $\{d_{ij}\}$ randomly

2- Estimate $\hat{d}_{ij}$ for the $\{d_{ij}\}$ by monotonic regression (isotonic*) from $\{d_{ij}\}$ in $\{\delta_{ij}\}$

3- Minimize the stress *J* by a steepest descent algorithm for a fix $\hat{d}_{ij}$ (obs.: the steepest descent is the direction opposed to the gradient).

4- Iterate 2 and 3 until convergence (the stress is no more reduced).

See more in Borg&Groenen, Chap. 9 p. 199.

(*) About isotonic regression see http://en.wikipedia.org/wiki/Isotonic_regression

Reduction of the dimension of the data space by "multidimensional scaling"

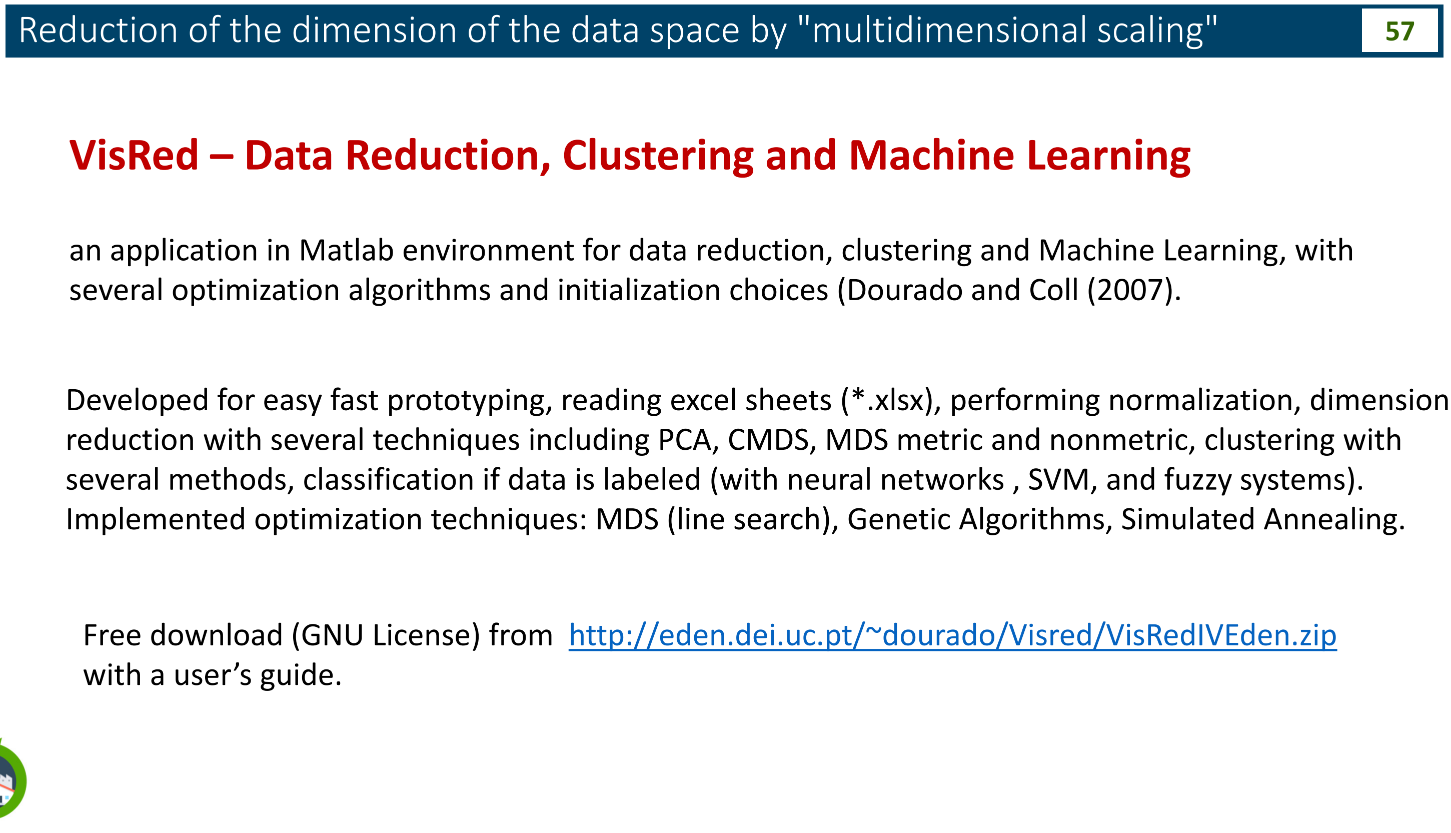
56

MDS for industrial processes monitoring

MDS has been used in many fields, from psychology and marketing to pattern recognition. For an extensive historical review see Saeed and Coll. (2018).

The use of MDS in industrial problems, namely for fault detection and monitoring, has been object of some studies (Matheus and Coll (2004, 2006), Yunus & Zhang (2010), and is regaining importance as can be seen by the works of Bing and Coll (2019), Geoffroy and Coll. (2019), Kodali (2020).

Nowadays with the quantity of data that the factories produce everyday and with the computational capabilities available, MDS, and in general dimension reduction, may have a very important role in developing automatic and intelligent systems for online monitoring the state of the machines and factories, to support maintenance, preventing faults and improving quality and productivity.



Reduction of the dimension of the data space by "multidimensional scaling"

57

VisRed – Data Reduction, Clustering and Machine Learning

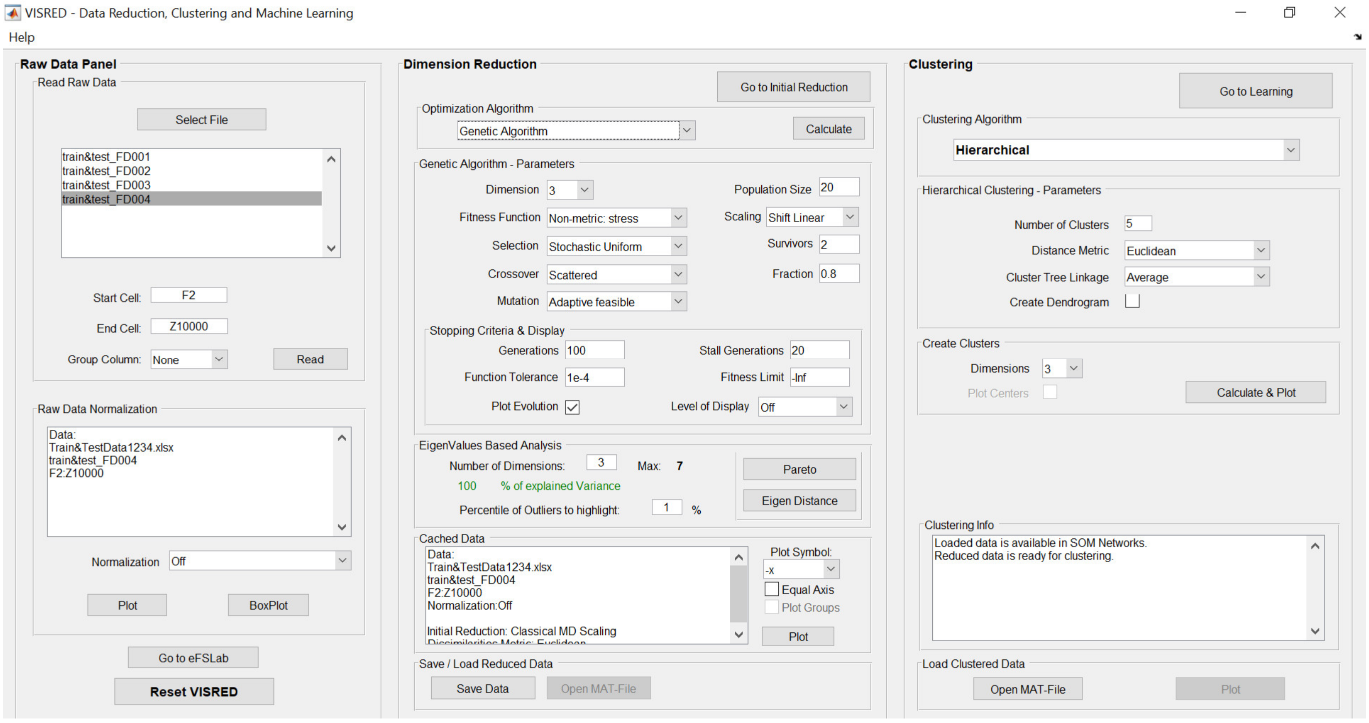
an application in Matlab environment for data reduction, clustering and Machine Learning, with several optimization algorithms and initialization choices (Dourado and Coll (2007).

Developed for easy fast prototyping, reading excel sheets (*.xlsx), performing normalization, dimension reduction with several techniques including PCA, CMDS, MDS metric and nonmetric, clustering with several methods, classification if data is labeled (with neural networks , SVM, and fuzzy systems). Implemented optimization techniques: MDS (line search), Genetic Algorithms, Simulated Annealing.

Free download (GNU License) from http://eden.dei.uc.pt/~dourado/Visred/VisRedIVEden.zip with a user's guide.

Reduction of the dimension of the data space by "multidimensional scaling"

58



VISRED - Data Reduction, Clustering and Machine Learning

Help

Raw Data Panel

Read Raw Data

train&test_FD001
train&test_FD002
train&test_FD003
train&test_FD004

Start Cell: F2

End Cell: Z10000

Group Column: None

Raw Data Normalization

Data:
Train&TestData1234.xlsx
train&test_FD004
F2:Z10000

Normalization: Off

Dimension Reduction

Optimization Algorithm: Genetic Algorithm

Genetic Algorithm - Parameters

Dimension 3
Population Size 20
Fitness Function Non-metric: stress
Scaling Shift Linear
Selection Stochastic Uniform
Survivors 2
Crossover Scattered
Fraction 0.8
Mutation Adaptive feasible

Stopping Criteria & Display

Generations 100
Stall Generations 20
Function Tolerance 1e-4
Fitness Limit -Inf
Plot Evolution ☑
Level of Display Off

EigenValues Based Analysis

Number of Dimensions: 3 Max: 7
100 % of explained Variance
Percentile of Outliers to highlight: 1 %

Cached Data

Data:
Train&TestData1234.xlsx
train&test_FD004
F2:Z10000
Normalization:Off

Initial Reduction: Classical MD Scaling
Dissimilarities Metric: Euclidean

Plot Symbol: -x
☐ Equal Axis
☐ Plot Groups

Save / Load Reduced Data

Clustering

Clustering Algorithm: **Hierarchical**

Hierarchical Clustering - Parameters

Number of Clusters 5
Distance Metric Euclidean
Cluster Tree Linkage Average
Create Dendrogram ☐

Create Clusters

Dimensions 3
Plot Centers ☐

Clustering Info

Loaded data is available in SOM Networks.
Reduced data is ready for clustering.

Load Clustered Data

KYKLOS 4.0

CISUC

Contents

- 1| Predictive maintenance and fault-tolerance in CPSs
- 2| Outliers detection for transient time-series
- 3| Reduction of the dimension of the data space by "multidimensional scaling" applying several optimization algorithms
- **4| Detection of similarities and prediction of the evolution of the health status of a machine, as a previous step to estimate the RUL**
- 5| References and bibliography

KYKLOS 4.0

CISUC

Contents

4|

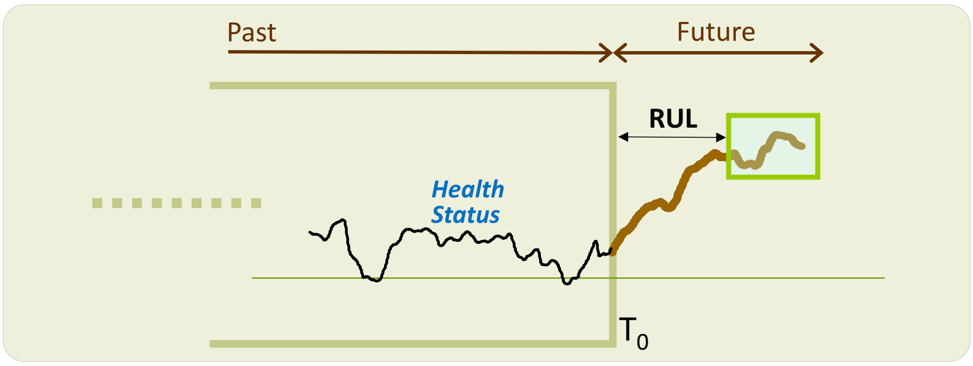
Detection of similarities and prediction of the evolution of the health condition of a machine, as a previous step to estimate the RUL

- Goal
- Approach
- Results
- Conclusions

Prediction health status for estimating RUL

Goal

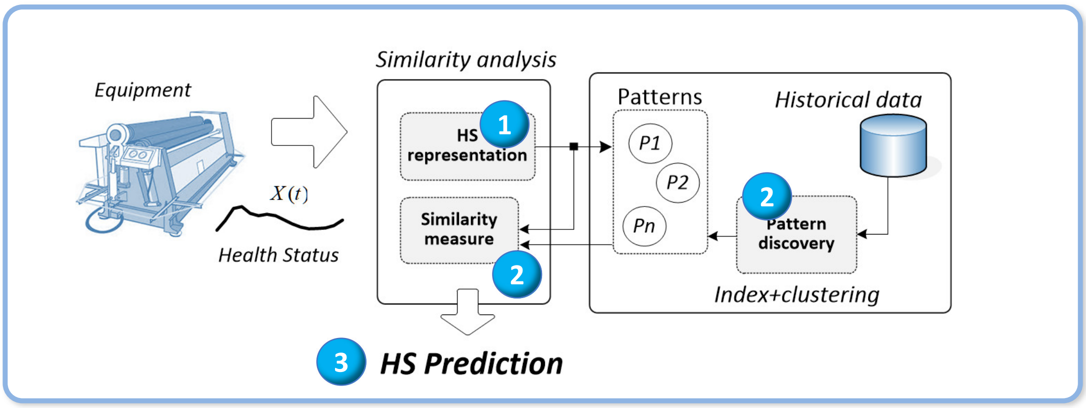
- Assume the knowledge of overall system's **health status indicator** (degradation level), by relying on time-dependent condition-based features or indicators
- **Predicting the future health status** as an indicator of the remaining useful life (RUL) of a component/system

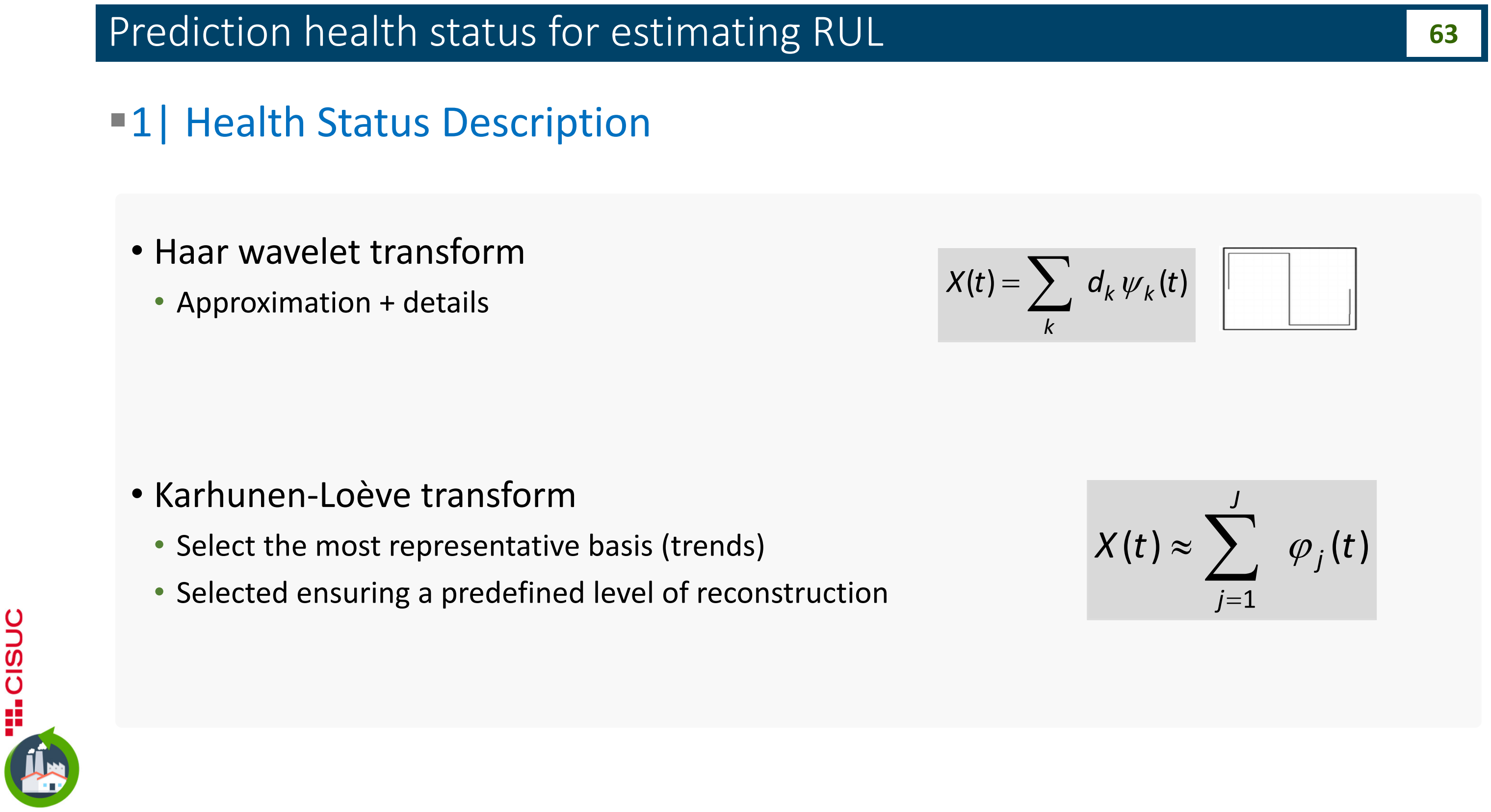


Prediction health status for estimating RUL

62

- Approach
  - **1.** Describe efficiently the health status | HS description
  - **2.** Find in the historic similar behaviors | similarity measure + indexing
  - **3.** Prediction | Based on the similar patterns





Prediction health status for estimating RUL

63

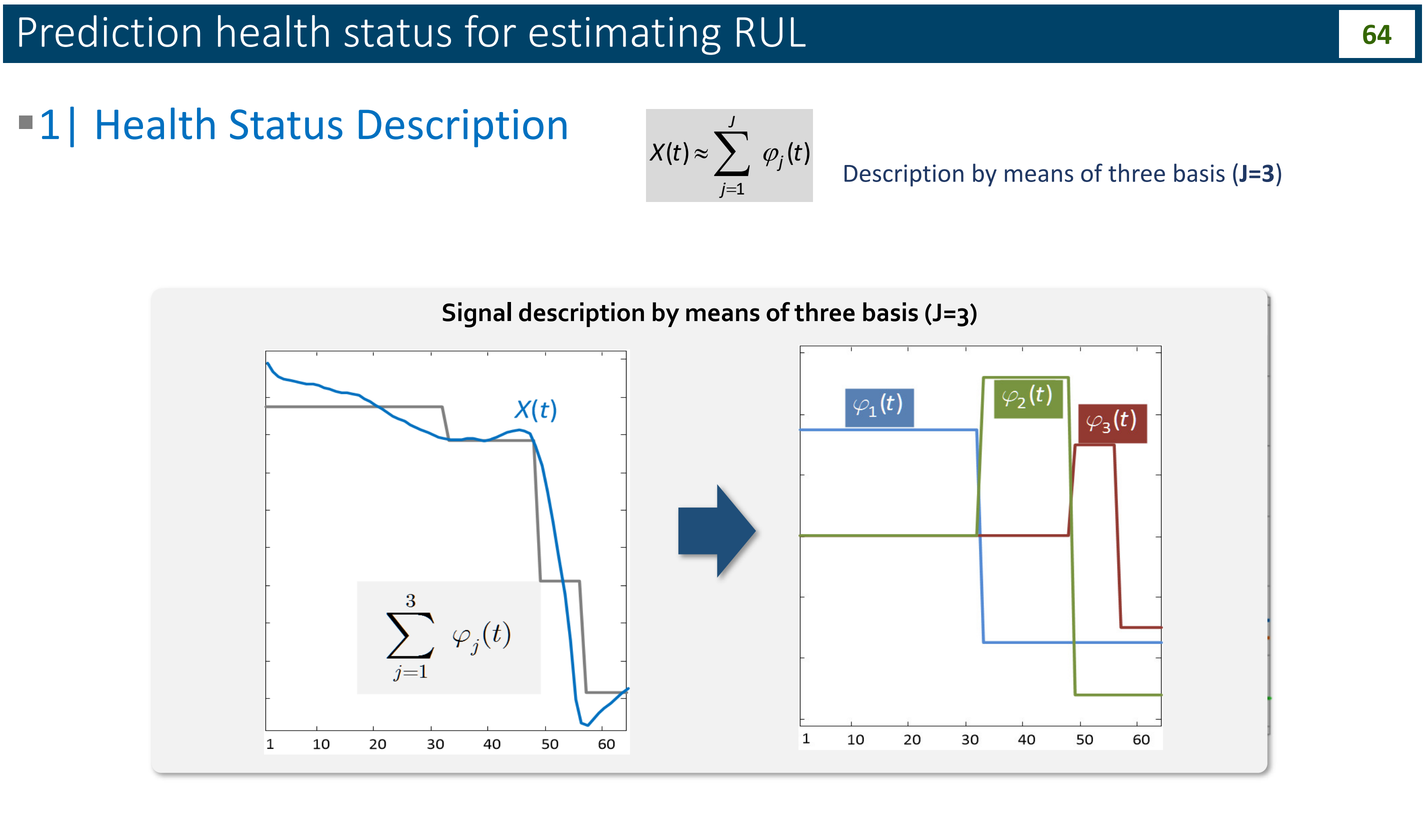
1| Health Status Description

- Haar wavelet transform
  - Approximation + details

$$X(t)=\sum_k d_k\,\psi_k(t)$$

- Karhunen-Loève transform
  - Select the most representative basis (trends)
  - Selected ensuring a predefined level of reconstruction

$$X(t)\approx\sum_{j=1}^{J}\varphi_j(t)$$



Prediction health status for estimating RUL

64

1| Health Status Description

$$X(t) \approx \sum_{j=1}^{J} \varphi_j(t)$$

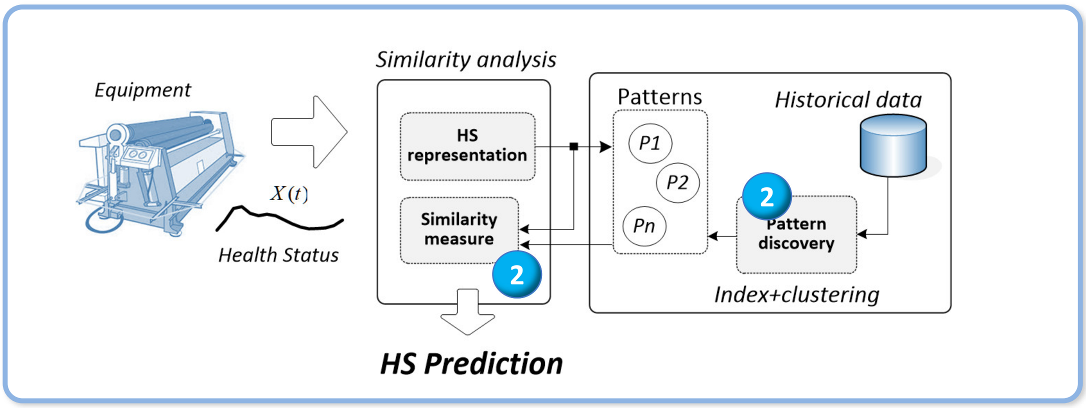
Description by means of three basis (**J=3**)

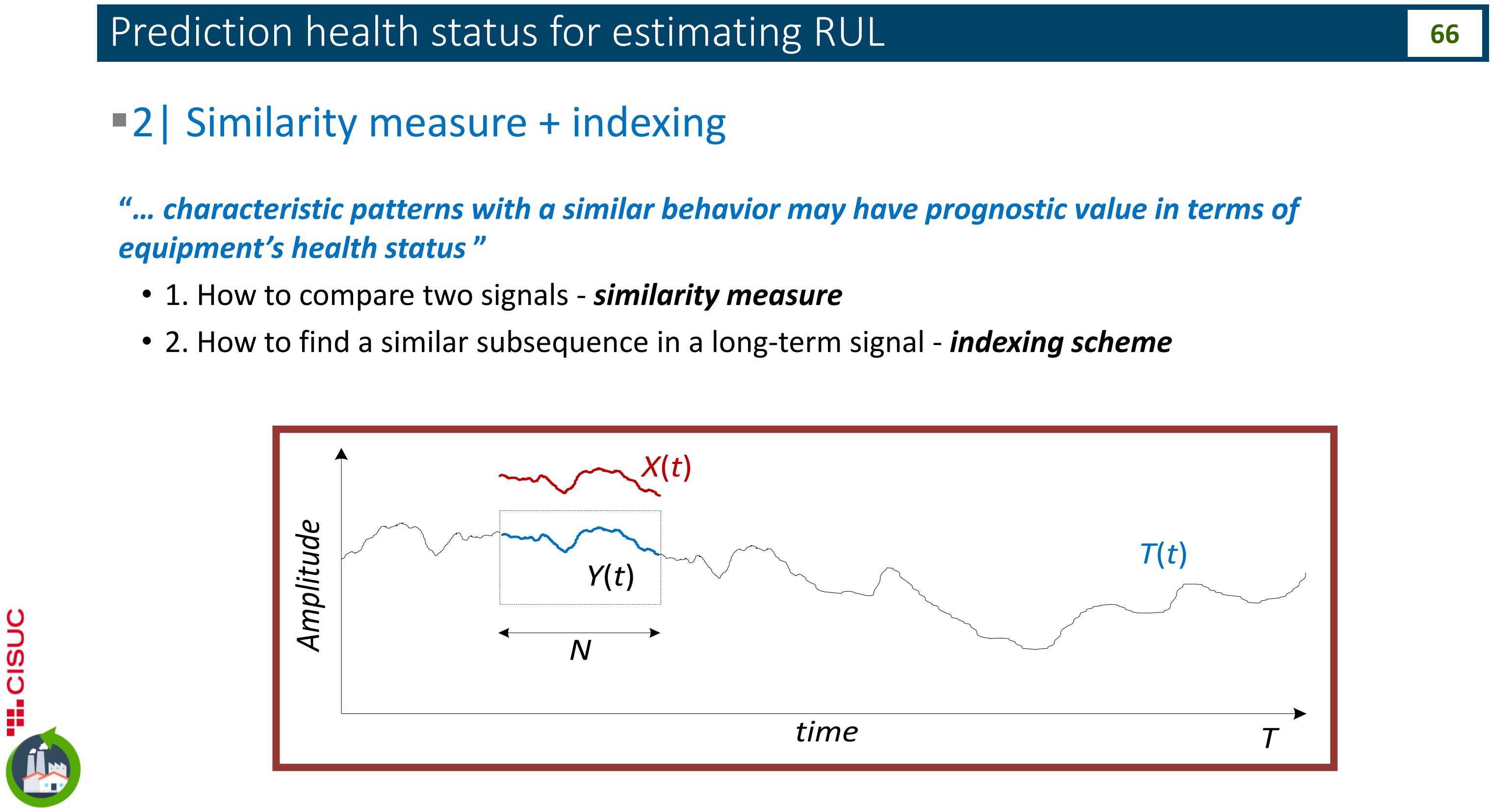
Signal description by means of three basis (J=3)

Prediction health status for estimating RUL

Approach

- **1.** Describe efficiently the health status | HS description
- **2. Find in the historic similar behaviors | similarity measure + indexing**
- **3.** Prediction | Based on the similar patterns





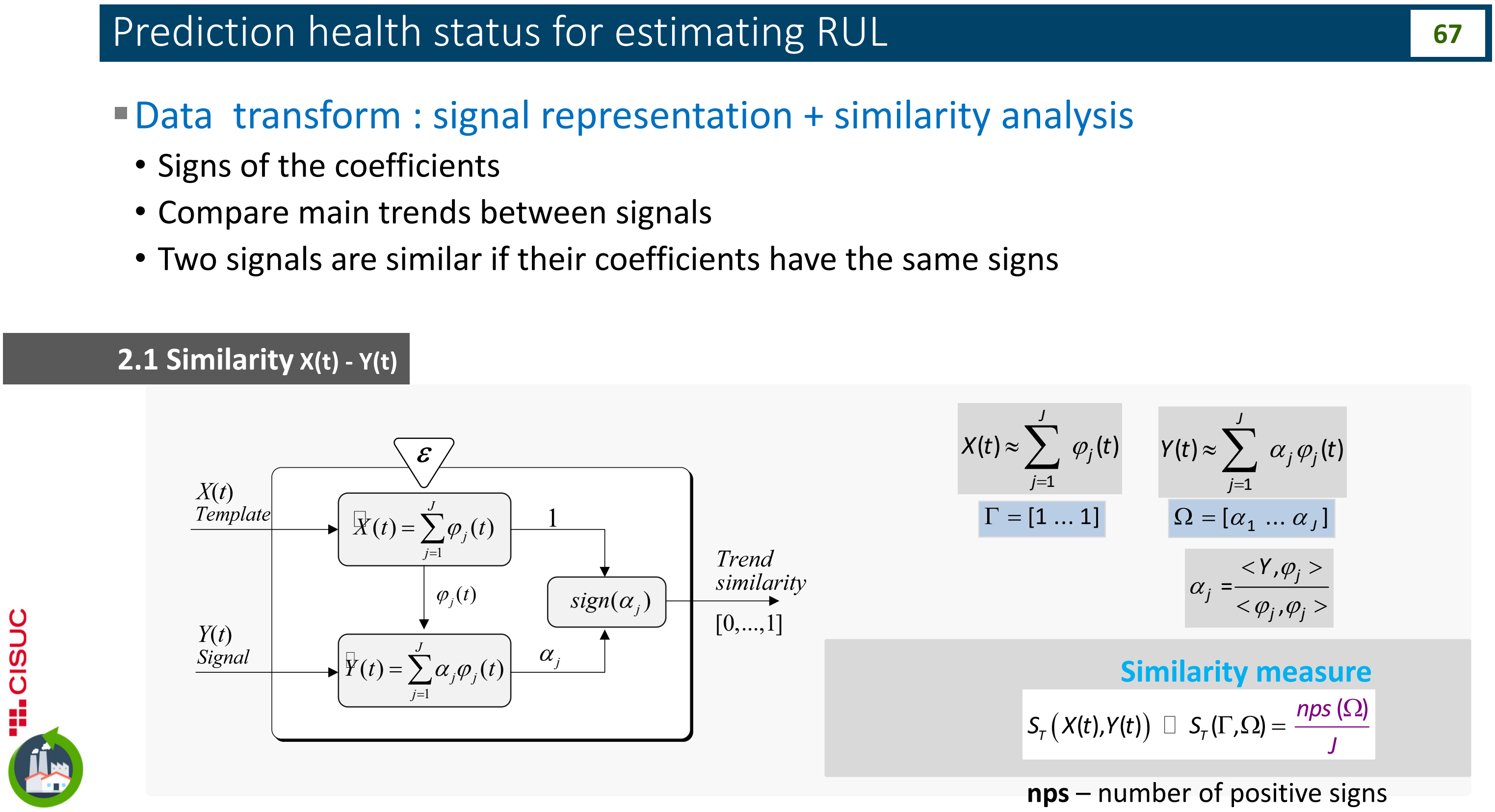
Prediction health status for estimating RUL

66

2| Similarity measure + indexing

"… characteristic patterns with a similar behavior may have prognostic value in terms of equipment's health status "

- 1. How to compare two signals - ***similarity measure***
- 2. How to find a similar subsequence in a long-term signal - ***indexing scheme***



Prediction health status for estimating RUL

67

- Data transform : signal representation + similarity analysis
  - Signs of the coefficients
  - Compare main trends between signals
  - Two signals are similar if their coefficients have the same signs

2.1 Similarity X(t) - Y(t)

$$X(t)\approx\sum_{j=1}^{J}\varphi_j(t)$$

$$\Gamma=[1\ \dots\ 1]$$

$$Y(t)\approx\sum_{j=1}^{J}\alpha_j\varphi_j(t)$$

$$\Omega=[\alpha_1\ \dots\ \alpha_J]$$

$$\alpha_j=\frac{<Y,\varphi_j>}{<\varphi_j,\varphi_j>}$$

Similarity measure

$$S_T\left(X(t),Y(t)\right)\ \square\ S_T(\Gamma,\Omega)=\frac{nps\,(\Omega)}{J}$$

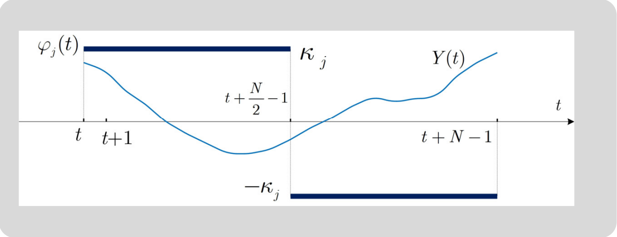
nps – number of positive signs

Prediction health status for estimating RUL

68

- Data transform : signal representation + similarity analysis
  - Iterative implementation, coefficient depends on the
    - Previous coefficient
    - Wavelet amplitude, kj , and
    - First, last, and middle values of the signal Y(t)

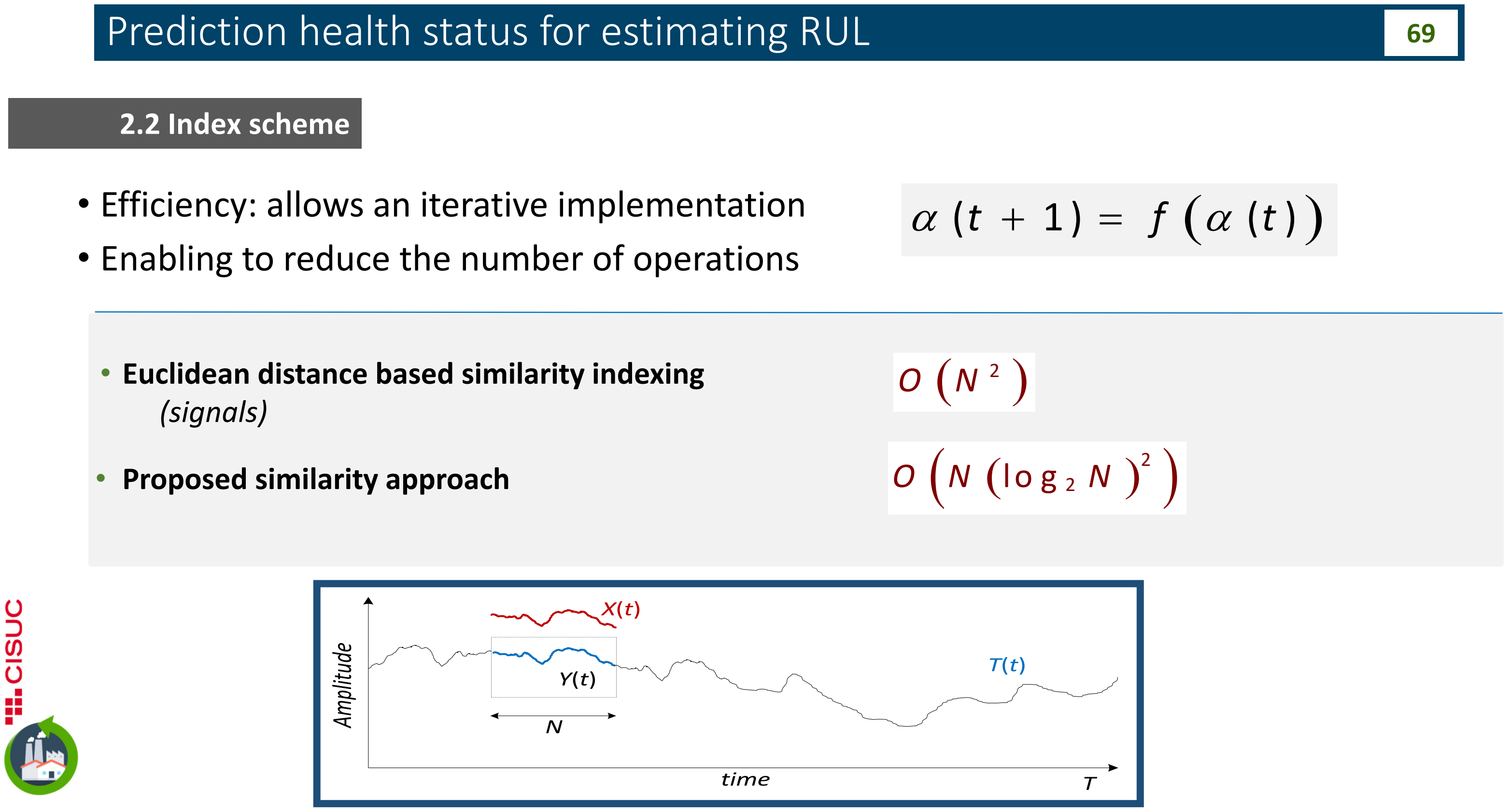
2.2 Index scheme



$$\alpha_j = \frac{<Y,\varphi_j>}{<\varphi_j,\varphi_j>}$$

$$\alpha(t+1) = f\left(\alpha(t)\right)$$

$$\alpha_j(t+1)=\alpha_j(t)+\kappa_j\left(-y(t)-y(t+N)+2\ y(t+\frac{N}{2})\right)$$



Prediction health status for estimating RUL

69

2.2 Index scheme

- Efficiency: allows an iterative implementation
- Enabling to reduce the number of operations

$$\alpha(t+1) = f(\alpha(t))$$

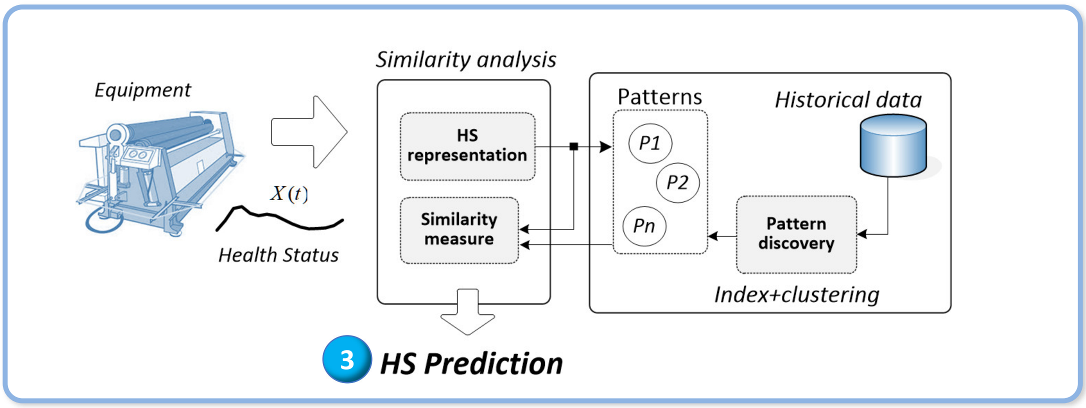
- **Euclidean distance based similarity indexing** *(signals)* $O(N^2)$
- **Proposed similarity approach** $O\left(N(\log_2 N)^2\right)$

Prediction health status for estimating RUL

70

Approach

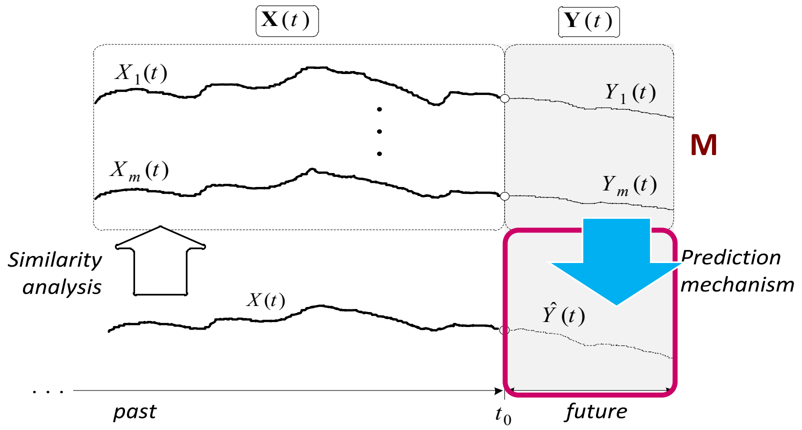
- 1. Describe efficiently the health status | HS description
- 2. Find in the historic similar behaviors | similarity measure + indexing
- 3. Prediction | Based on the similar patterns

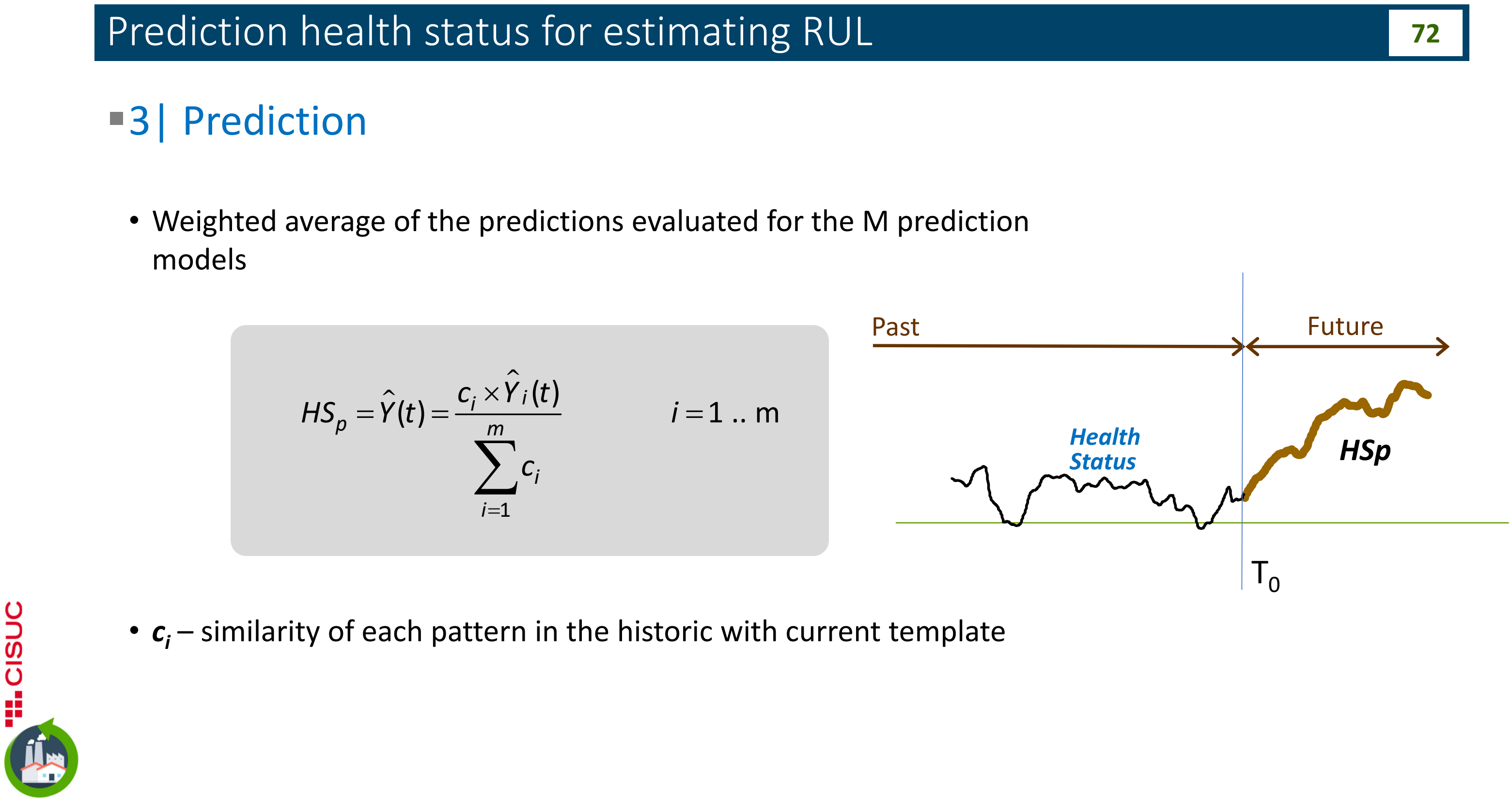


Prediction health status for estimating RUL

3| Prediction

- No explicit model
- Prediction using the most M similar behaviors
- Using the weight average of the “past” behaviours





Prediction health status for estimating RUL

72

3| Prediction

- Weighted average of the predictions evaluated for the M prediction models

$$HS_p = \hat{Y}(t) = \frac{c_i \times \hat{Y}_i(t)}{\sum_{i=1}^{m} c_i} \qquad i = 1 \,..\, \mathrm{m}$$

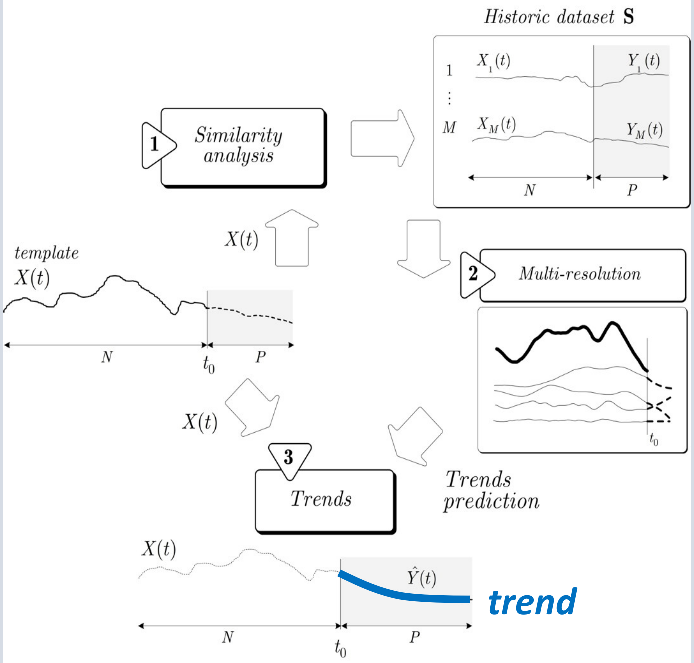
- c_i – similarity of each pattern in the historic with current template

Prediction health status for estimating RUL

73

3| Prediction - **alternatives**

- Other prediction techniques can be used
- Based on a **multi-resolution wavelet** decomposition to predict the **trend evolution** oft the health status



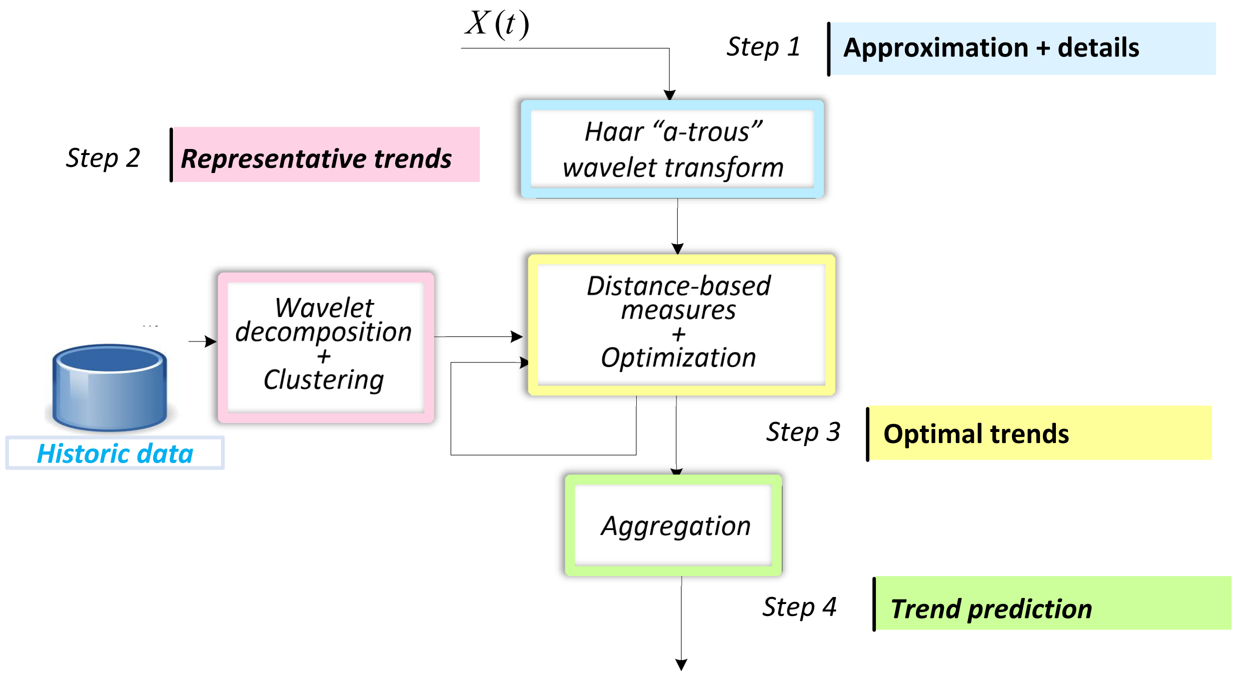
CISUC

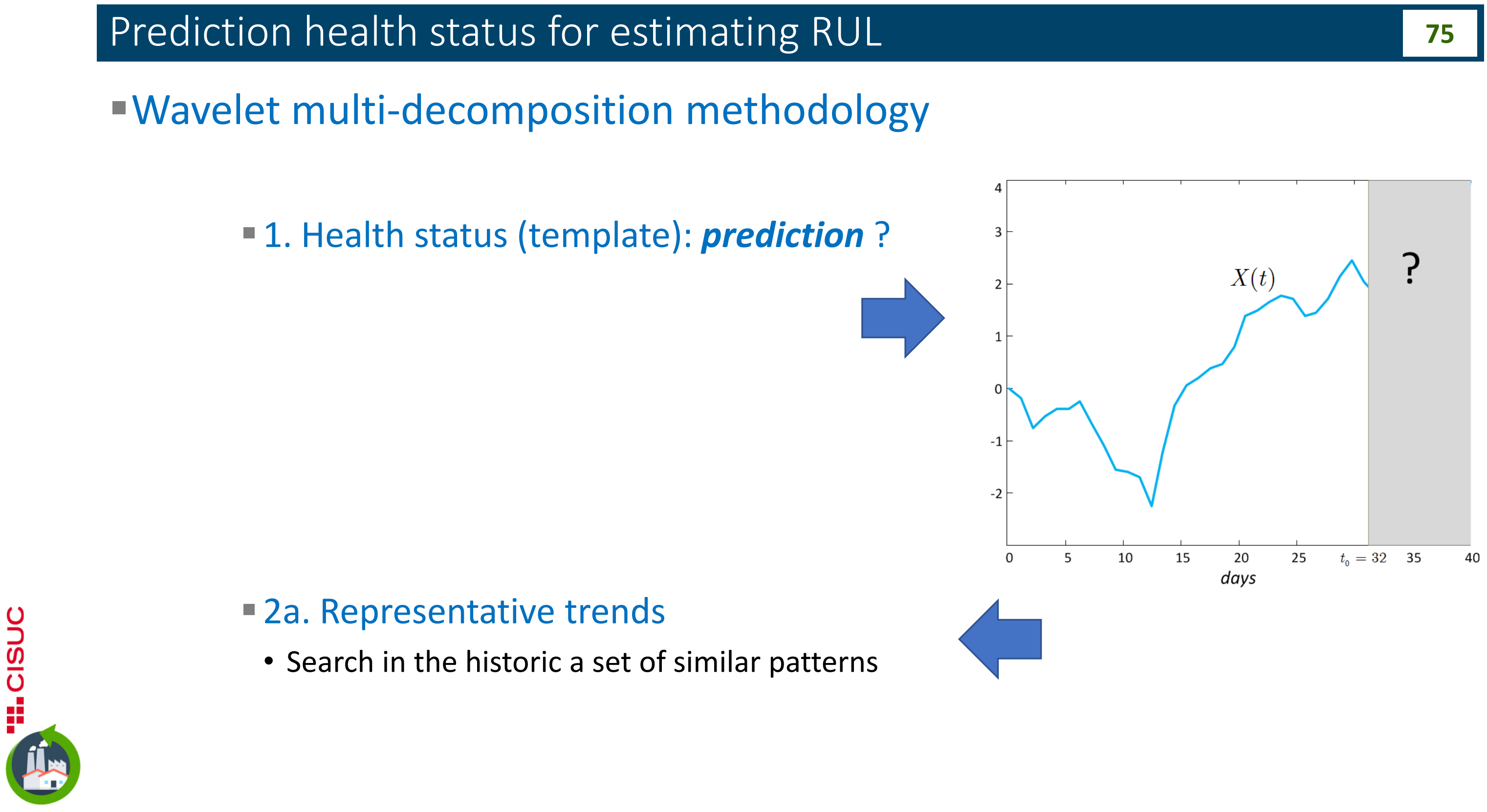
©MECO.net

Prediction health status for estimating RUL

74

- Wavelet multi-decomposition methodology





Prediction health status for estimating RUL

75

- Wavelet multi-decomposition methodology
  - 1. Health status (template): ***prediction*** ?
  - 2a. Representative trends
    - Search in the historic a set of similar patterns

4
3
2
1
0
-1
-2
0
5
10
15
20
25
$t_0 = 32$
35
40
days
$X(t)$
?
CISUC

Prediction health status for estimating RUL

76

Wavelet multi-decomposition methodology

2b. Representative trends

- For each level of decomposition a clustering process is employed

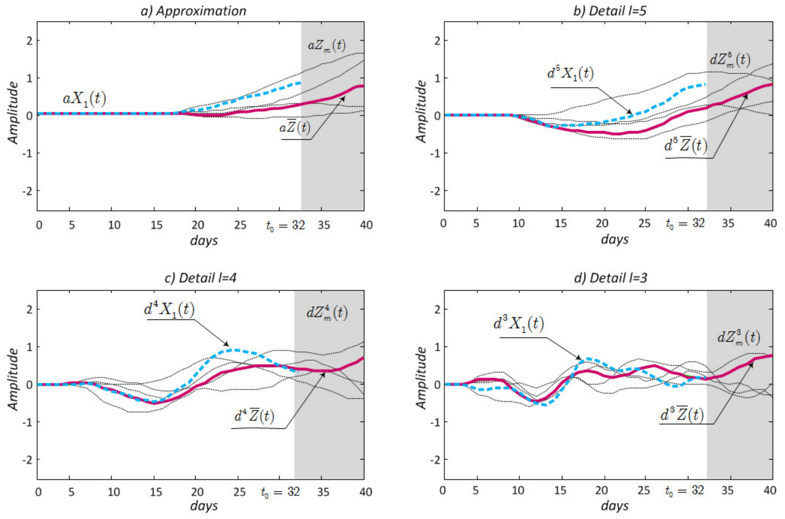
Template

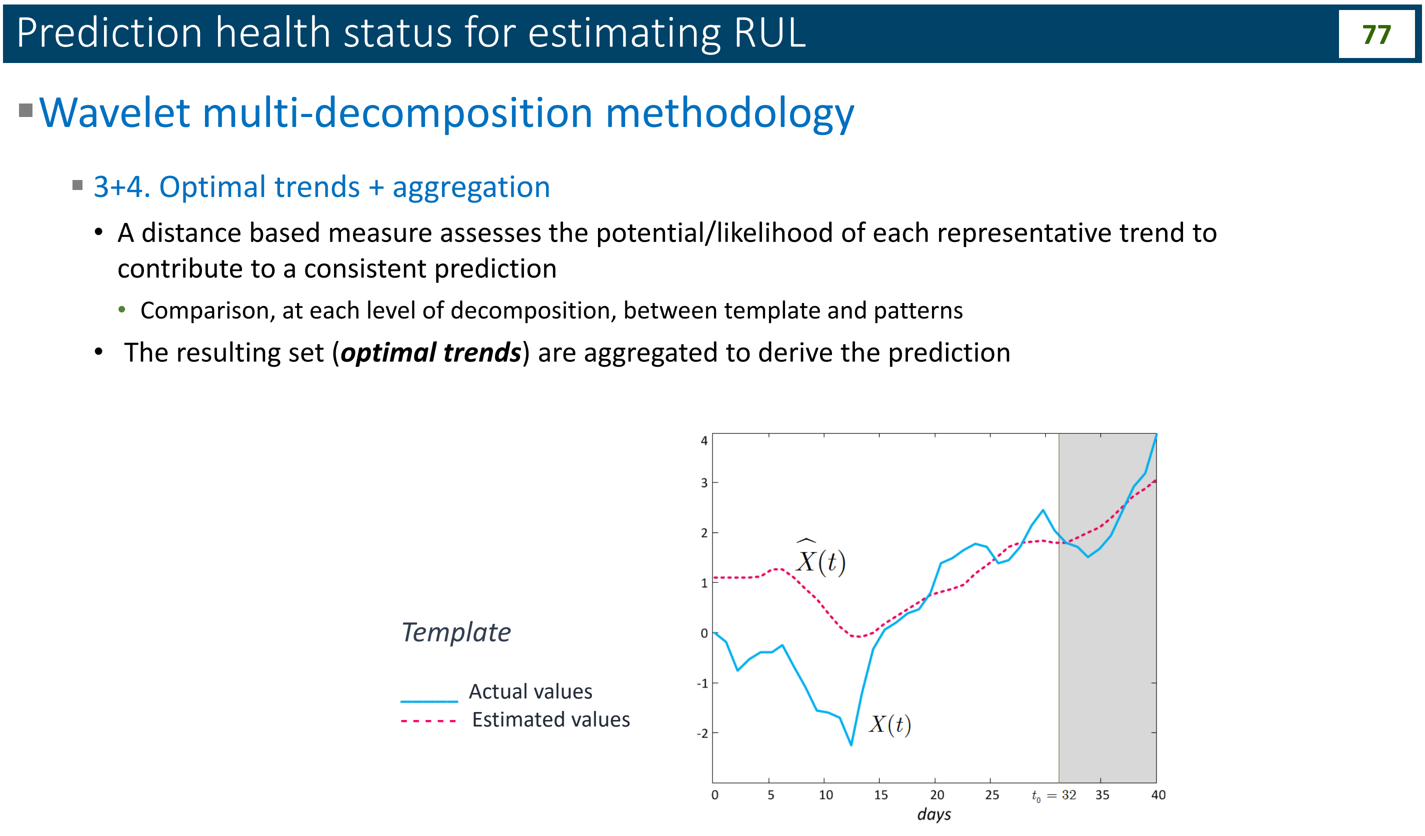
- - - - - wavelet decompostion

Patterns

______ wavelet decompostion

______ **Representative trend**





Prediction health status for estimating RUL

77

- Wavelet multi-decomposition methodology
  - 3+4. Optimal trends + aggregation
    - A distance based measure assesses the potential/likelihood of each representative trend to contribute to a consistent prediction
      - Comparison, at each level of decomposition, between template and patterns
    - The resulting set (***optimal trends***) are aggregated to derive the prediction

Prediction health status for estimating RUL

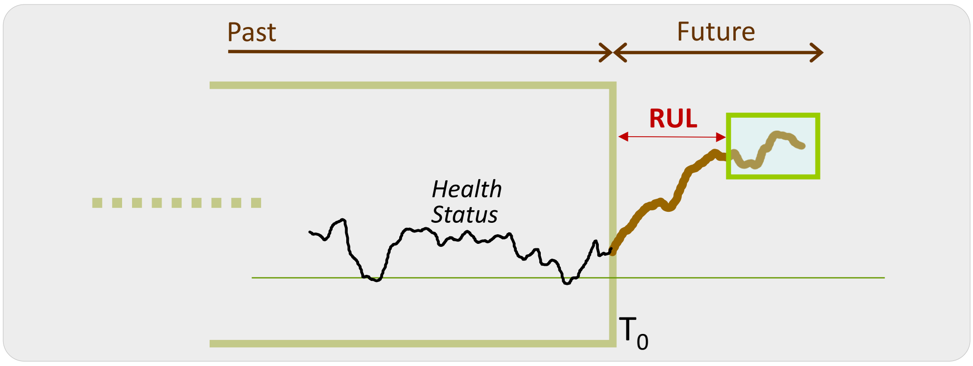
78

Conclusions

This work proposed a prediction based scheme to estimate the future evolution oh health status of equipment's

• **1|** Describe current health status	| Efficient description – wavelet approach
• **2|** Find in the historic similar behaviors	| Reduce number of operations - Iterative solution
• **3|** Prediction	| No explicit model - Weighted average – **Trends** wavelet decomposition

> RUL estimation



CISUC

5|

References and bibliography

References and bibliography

80

Atamuradov, V., Medjaher, K., Dersin, P., Lamoureux, B., & Zerhouni, N. (2017). Prognostics and health management for maintenance practitioners - review, implementation and tools evaluation. International Journal of Prognostics and Health Management, 8(Special Issue 7), 1–31.

Bing Li, J. Cui, K. He , L. Qian and Y. He (2019) A Method for Fault Diagnosis Based on Multidimensional Scaling (MDS) in Analog Circuits , 2019 *IOP Conf. Ser.: Mater. Sci. Eng.* 631 042037

Borg, I. and P. J. F. Groenen (2005), Modern Multidimensional Scaling, Theory and Aplications, Springer, 2005.

Chan et al. (2003); Haar wavelets for efficient similarity search of time-series: with and without time warping; IEEE Trans. Knowledge and Data Engineering, 15(3): 686-705.

Chappell, D. (2015). Introducing Azure Machine Learning – A guide for Technical Professionals, Microsoft Corporation, Chappelll & Associates.

Dourado A., E. Ferreira, P. Barbeiro (2007), VISRED –Numerical Data Mining with Linear and Nonlinear Techniques, P. Perner (Ed.): ICDM 2007, LNAI 4597, pp. 92–106, 2007. Springer-Verlag Berlin Heidelberg 2007

Geoffroy H., J. Berger, B. Colange, S. Lespinats, D. Dutykh, G. Sauce, B. Catherine (2019), Use of Multidimensional Scaling for Fault Detection or Monitoring Support In A Continuous Commissioning. Proceedings of the 16th IBPSA Conference, IBPSA, Sep 2019, Rome, Italy. pp.877-884, doi: 10.26868/25222708.2019.210699hal-02411240

Gil, P., H. Martins, and F. Januário, 'Outliers detection methods in wireless sensor networks', Artificial Intelligence Review, pp. 2411--2436, Feb. 2018, doi: 10.1007/s10462-018-9618-2.

References and bibliography 81

Hetland et al; A survey of recent methods for efficient retrieval of similar time sequences; Data Mining in Time Series Databases, World Scientific.

Huang, M., Z. Liu, Y. Tao (2020). Mechanical fault diagnosis and prediction in IoT based on multi-source sensing data fusion, Simulation Modelling Practice and Theory, Vol. 102, 2020, 101981, https://doi.org/10.1016/j.simpat.2019.101981

Jimenez, V.J., N. Bouhmala, A.H. Gausdal (2020). Developing a predictive maintenance model for vessel machinery, Journal of Ocean Engineering and Science, Vol. 5, Issue 4, pp. 358-386, https://doi.org/10.1016/j.joes.2020.03.003.

Kodali L. (2020), Extensions of Weighted Multidimensional Scaling with Statistics for Data Visualization and Process Monitoring, Dissertation submitted to the Faculty of the Virginia Polytechnic Institute and State University in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Statistics, August 2020.

Kruskal, Joseph B. & Wish, Myron (1978). *Multidimensional scaling*. Sage University Paper Series on Quantitative Applications in the Social Sciences. Beverly Hills, CA: Sage Publications.

Lei, Y., Li, N., Guo, L., Li, N., Yan, T., & Lin, J. (2018). Machinery health prognostics: A systematic review from data acquisition to RUL prediction. Mechanical Systems and Signal Processing, 104(December 2017), 799–834.

Matheus, J., A. Dourado, J. Henriques, M. Antónia, D. Nogueira (2006), Iterative Multidimensional Scaling for Industrial Process Monitoring, IEEEXplore, IEEE SMC Conf, 2006, DOI:10.1109/ICSMC.2006.384359

Matheus, J., A. Dourado and J. Henriques (2004), POM by Space Reduction for Intelligent Monitoring of Industrial Processes, Proc *IFAC-IEEE MCPL Management and Control of Production and Logistics*, 2004, Gaston Lefranc (Ed) Elsevier. ISBN 9780080444840.

References and bibliography 82

Radanliev, P., D. De Roure, M. Van Kleek, O. Santos, U. Ani (2020). Artificial intelligence in cyber physical systems. AI & Soc. https://doi.org/10.1007/s00146-020-01049-0

Rocha. T.; Similary Based Approaches for the Analysis and Prediction of Physiologic Times Series. PhD Thesis, Univ. of Coimbra.

Rocha, T., S. Paredes, P. Carvalho, J. Henriques; An effective wavelet strategy for the trend prediction of physiological time series with application to pHealth systems; in 35th Annual International IEEE EMBS Conference, Osaka, 2013.

Saeed N., H. Nam, M. I. Ul Haq, and Dost Muhammad Saqib Bhatti (2018). A Survey on Multidimensional Scaling. *ACM Comput. Surv.* 51, 3, Article 47 (May 2018). https://doi.org/10.1145/3178155

Shcherbakov M.V., A.V. Glotov, S.V. Cheremisinov (2020). Proactive and Predictive Maintenance of Cyber-Physical Systems. In: Kravets A., Bolshakov A., Shcherbakov M. (eds) Cyber-Physical Systems: Advances in Design & Modelling. Studies in Systems, Decision and Control, vol 259. Springer, Cham. https://doi.org/10.1007/978-3-030-32579-4_21

Yunus, M.Y.M. and J. Zhang (2010), Multivariate Process Monitoring Using Classical Multidimensional Scaling and Procrustes Analysis, 9th International Symposium on Dynamics and Control of Process Systems (DYCOPS 2010), Leuven, Belgium, July 5-7, 2010, doi: 10.3182/20100705-3-BE-2011.0145

Zhou, P.; D. Zuo, K.M. Hou, Z. Zhang, J. Dong, J. Li, H. Zhou (2019). A Comprehensive Technological Survey on the Dependable Self-Management CPS: From Self-Adaptive Architecture to Self-Management Strategies. Sensors 2019, 19, 1033. https://doi.org/10.3390/s19051033

SECURITY ENGINEERING FOR SMART FARMING – FROM AUTOMATED VEHICLES TO SENSOR NETWORKS.

CPS&IoT'2021 Summer School on Cyber-Physical Systems and Internet-of-Things

Christoph Schmittner

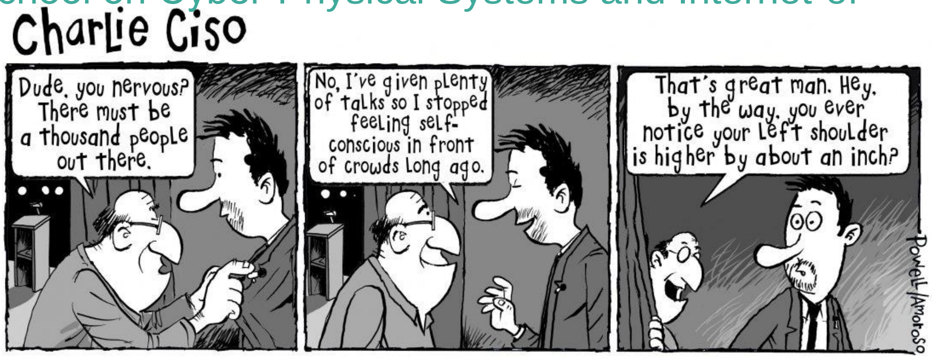
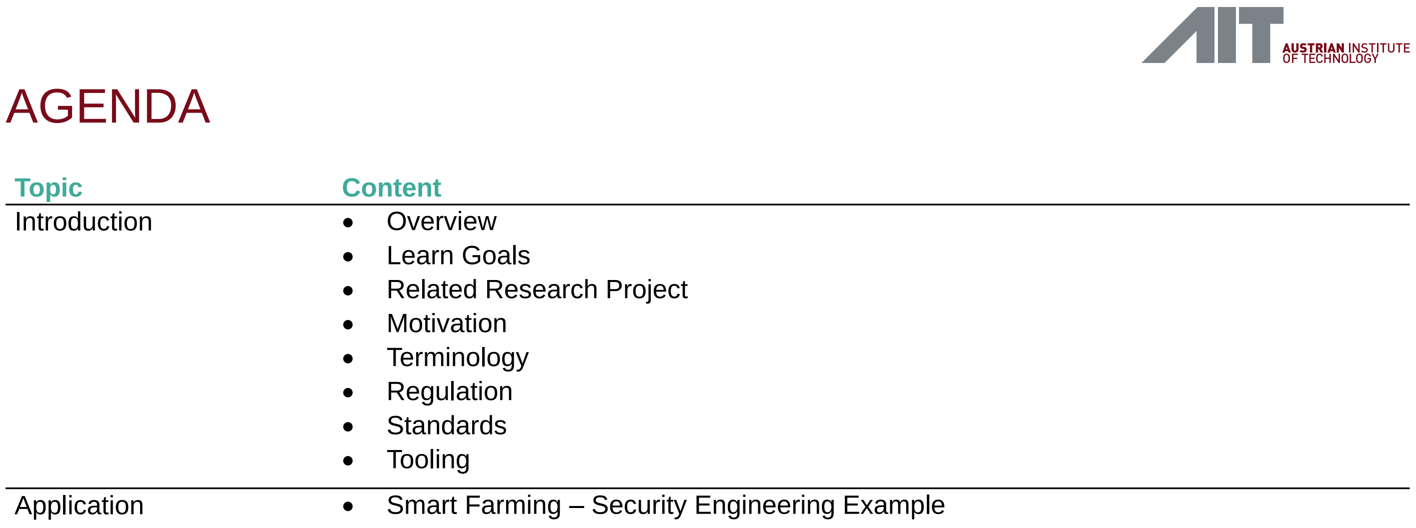

Charlie Ciso
Dude, you nervous? There must be a thousand people out there.
No, I've given plenty of talks so I stopped feeling self-conscious in front of crowds long ago.
That's great man. Hey, by the way, you ever notice your left shoulder is higher by about an inch?
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)



AGENDA

Topic	Content
Introduction	• Overview • Learn Goals • Related Research Project • Motivation • Terminology • Regulation • Standards • Tooling
Application	• Smart Farming – Security Engineering Example

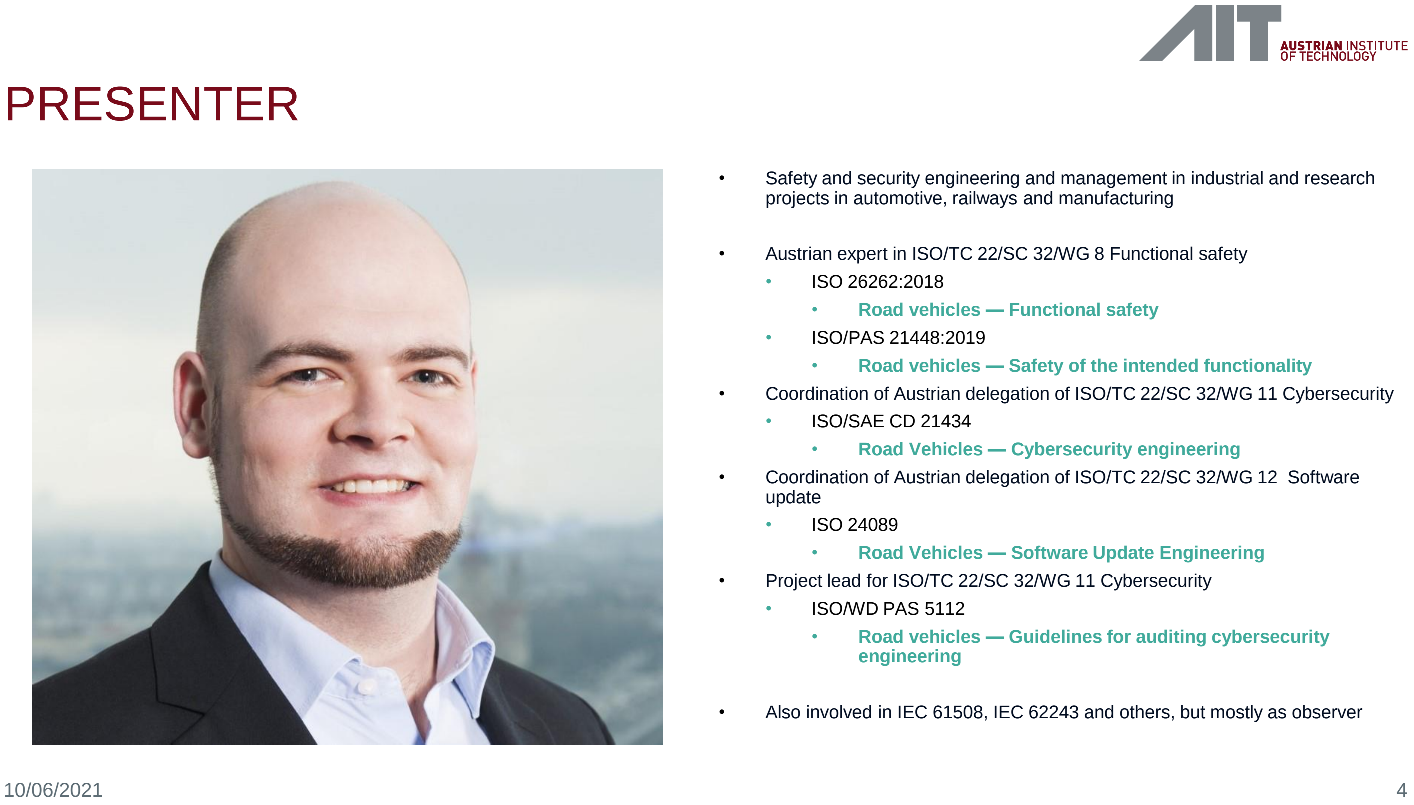
AUSTRIAN INSTITUTE OF TECHNOLOGY

LEARNING GOALS

- Insight in cybersecurity
  - Focus will be on automated vehicle for smart farming
  - Includes sensor networks and additional information from Industrial and railways
- Understand the topic and get an overview

Charlie Ciso
Why is it so DARK in this Data Center?
Hackers cant HACK what they can't SEE!!
Let's cut back on the Gartner Conferences.
Powell/Amoroso

10/06/2021 Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso) 3

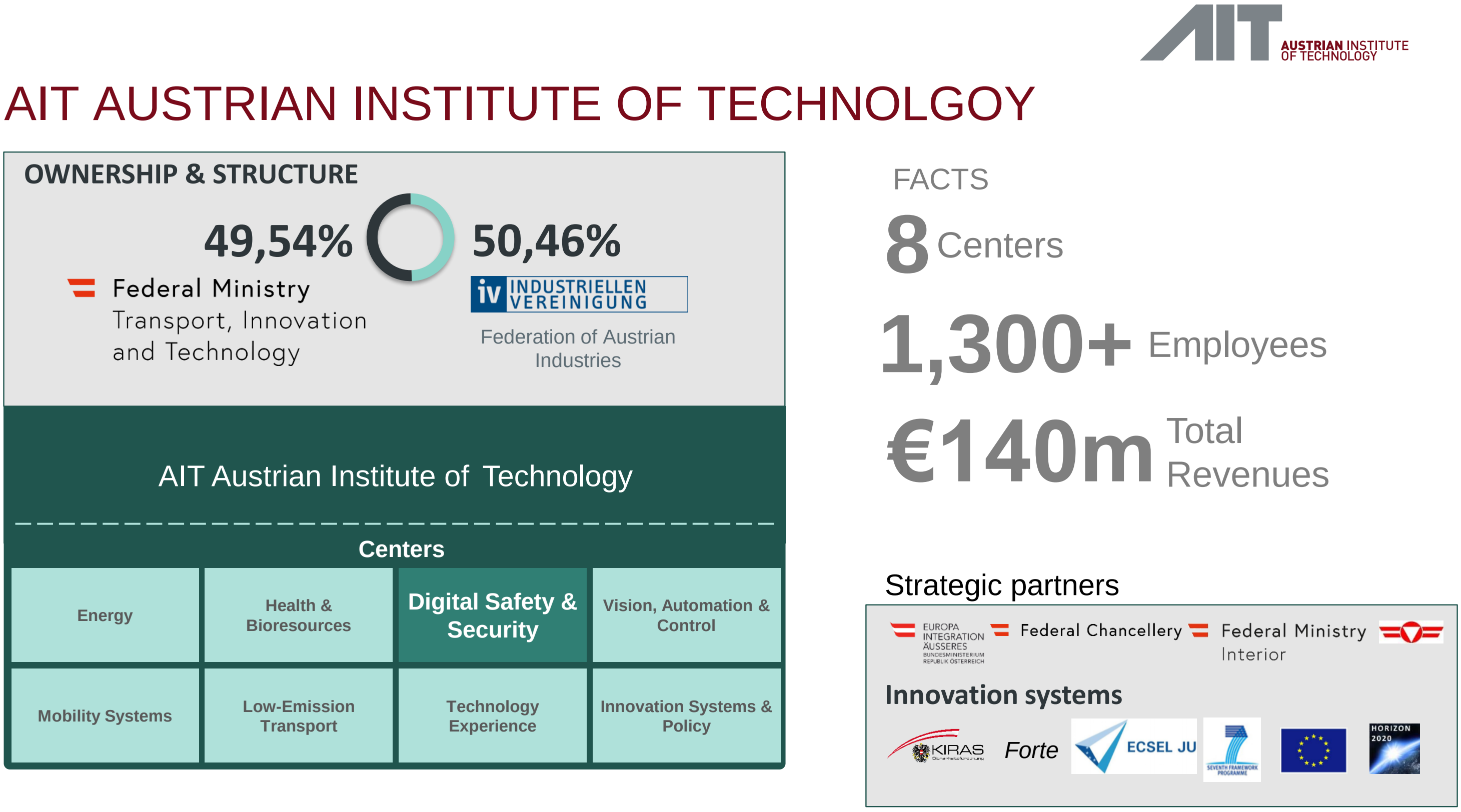


AUSTRIAN INSTITUTE OF TECHNOLOGY

PRESENTER

- Safety and security engineering and management in industrial and research projects in automotive, railways and manufacturing
- Austrian expert in ISO/TC 22/SC 32/WG 8 Functional safety
  - ISO 26262:2018
    - **Road vehicles — Functional safety**
  - ISO/PAS 21448:2019
    - **Road vehicles — Safety of the intended functionality**
- Coordination of Austrian delegation of ISO/TC 22/SC 32/WG 11 Cybersecurity
  - ISO/SAE CD 21434
    - **Road Vehicles — Cybersecurity engineering**
- Coordination of Austrian delegation of ISO/TC 22/SC 32/WG 12 Software update
  - ISO 24089
    - **Road Vehicles — Software Update Engineering**
- Project lead for ISO/TC 22/SC 32/WG 11 Cybersecurity
  - ISO/WD PAS 5112
    - **Road vehicles — Guidelines for auditing cybersecurity engineering**
- Also involved in IEC 61508, IEC 62243 and others, but mostly as observer

10/06/2021 4



AUSTRIAN INSTITUTE OF TECHNOLOGY

AIT AUSTRIAN INSTITUTE OF TECHNOLGOY

OWNERSHIP & STRUCTURE

49,54%
Federal Ministry
Transport, Innovation
and Technology

50,46%
INDUSTRIELLEN VEREINIGUNG
Federation of Austrian
Industries

AIT Austrian Institute of Technology

Centers

Energy	Health & Bioresources	Digital Safety & Security	Vision, Automation & Control
Mobility Systems	Low-Emission Transport	Technology Experience	Innovation Systems & Policy

FACTS

8 Centers

1,300+ Employees

€140m Total Revenues

Strategic partners

EUROPA INTEGRATION ÄUSSERES BUNDESMINISTERIUM REPUBLIK ÖSTERREICH
Federal Chancellery
Federal Ministry
Interior

Innovation systems

AUSTRIAN INSTITUTE OF TECHNOLOGY

TOMORROW TODAY

afarcloud

Aggregate Farming in the Cloud

FFG Forschung wirkt.

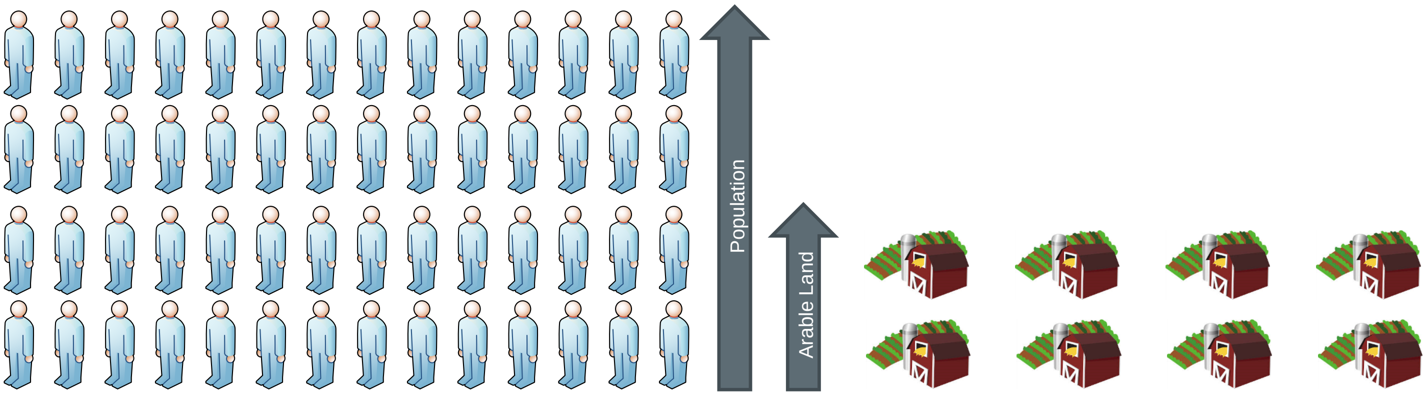
ECSEL Joint Undertaking

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 783221. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Finland, Germany, Greece, Italy, Latvia, Norway, Poland, Portugal, Spain, Sweden.

10/06/2021

AUSTRIAN INSTITUTE OF TECHNOLOGY

RISING WORLD POPULATION



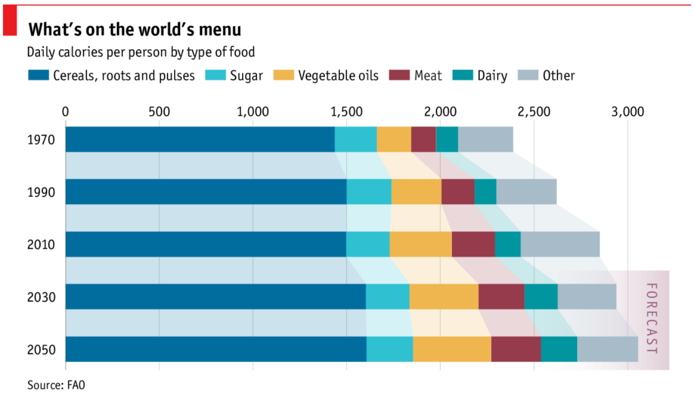
World population is increasing faster than arable land

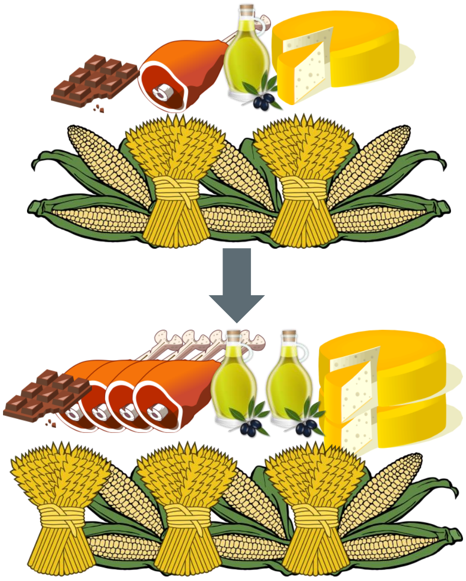
10/06/2021

7

AUSTRIAN INSTITUTE OF TECHNOLOGY

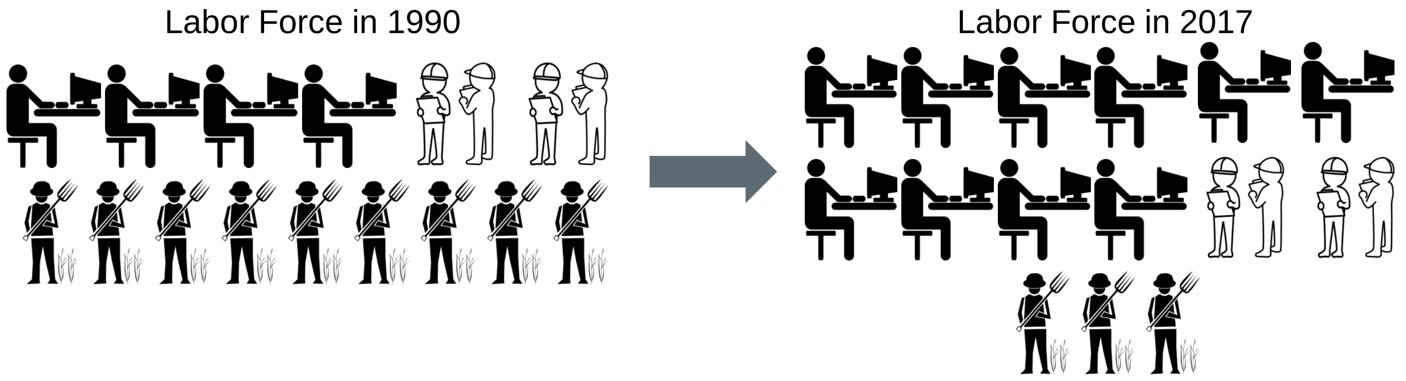
DIETARY CHANGES





AUSTRIAN INSTITUTE OF TECHNOLOGY

LABOR FORCE



Labor Force in 1990

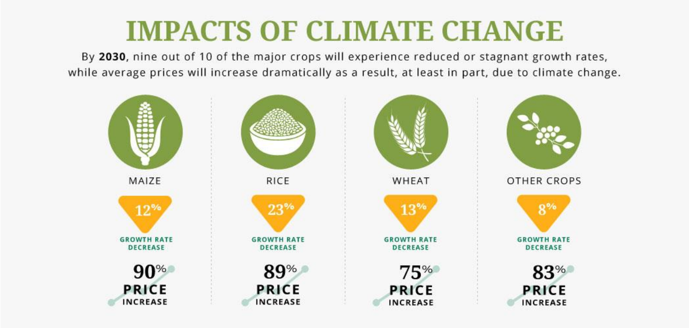
Labor Force in 2017

10/06/2021

9

AUSTRIAN INSTITUTE OF TECHNOLOGY

CLIMATE AND AGRICULTURE

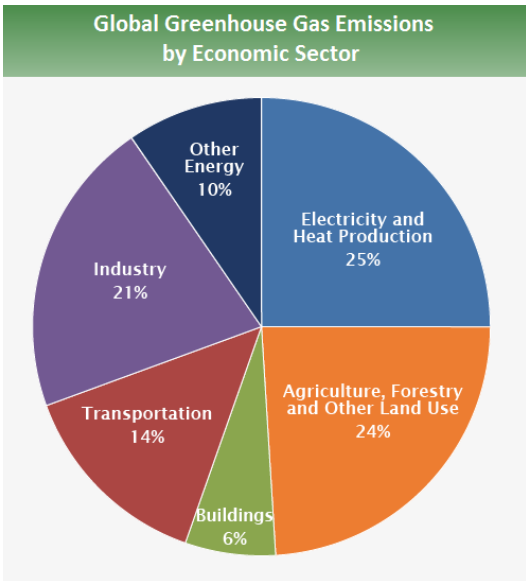


IMPACTS OF CLIMATE CHANGE

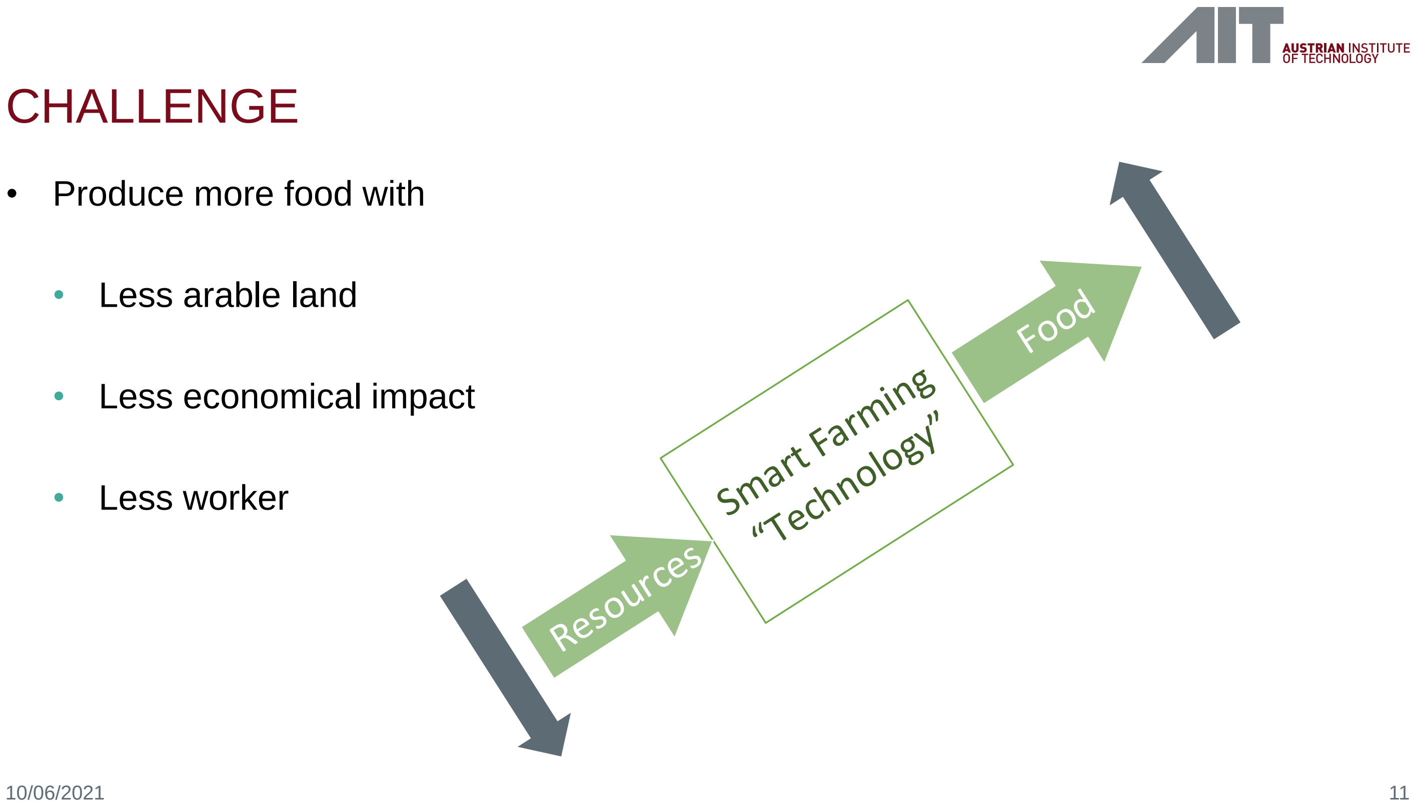
By **2030**, nine out of 10 of the major crops will experience reduced or stagnant growth rates, while average prices will increase dramatically as a result, at least in part, due to climate change.

MAIZE	RICE	WHEAT	OTHER CROPS
12% GROWTH RATE DECREASE	23% GROWTH RATE DECREASE	13% GROWTH RATE DECREASE	8% GROWTH RATE DECREASE
90% PRICE INCREASE	89% PRICE INCREASE	75% PRICE INCREASE	83% PRICE INCREASE

https://farmingfirst.org/sdg-toolkit#section_1


Global Greenhouse Gas Emissions by Economic Sector
Other Energy 10%
Electricity and Heat Production 25%
Industry 21%
Transportation 14%
Buildings 6%
Agriculture, Forestry and Other Land Use 24%

https://www.epa.gov/ghgemissions/global-greenhouse-gas-emissions-data



CHALLENGE

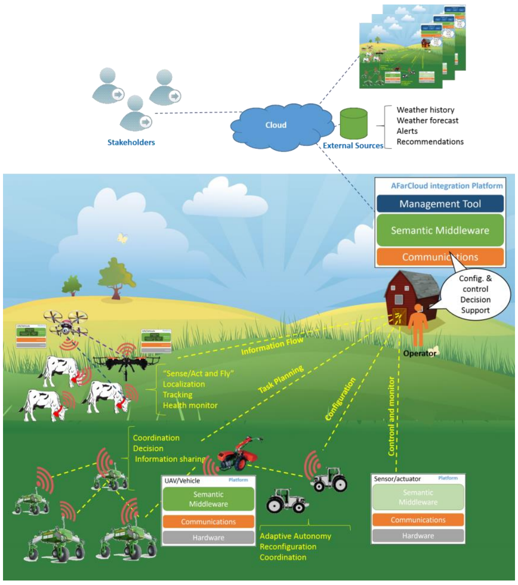
- Produce more food with
  - Less arable land
  - Less economical impact
  - Less worker

10/06/2021

11

AFARCLOUD - AGGREGATE FARMING IN THE CLOUD

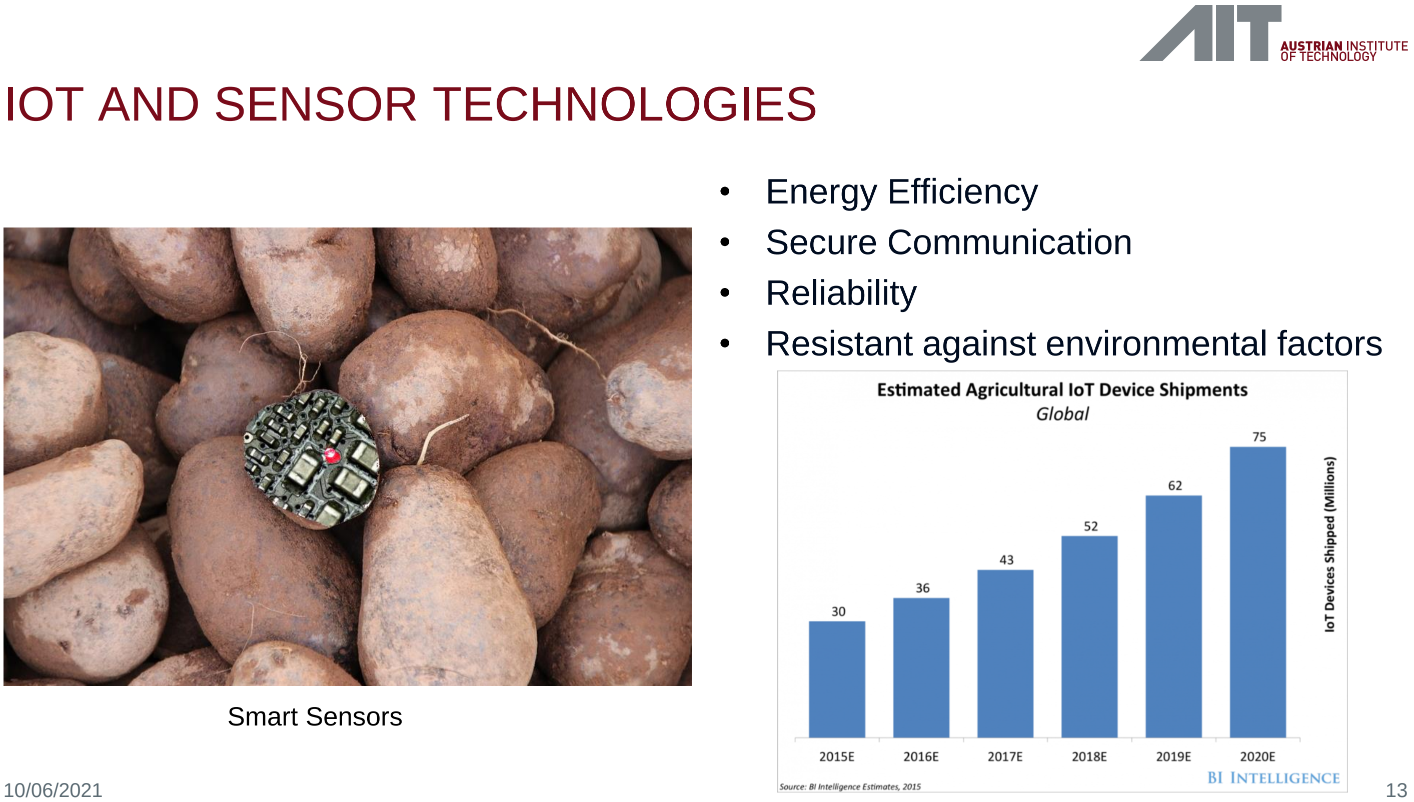
AUSTRIAN INSTITUTE OF TECHNOLOGY



- Ease and aggregate solutions for the agriculture environment characterization
- Facilitate the creation of hierarchical mission plans involving elements working in an autonomous manner
- Efficient use of the available farming vehicles by means of a "sensing-on-the-move" approach
- Improvement of traditional business models and development of new ones
- Demonstration of efficient and feasible solutions in real application scenarios

10/06/2021

12



AUSTRIAN INSTITUTE OF TECHNOLOGY

IOT AND SENSOR TECHNOLOGIES

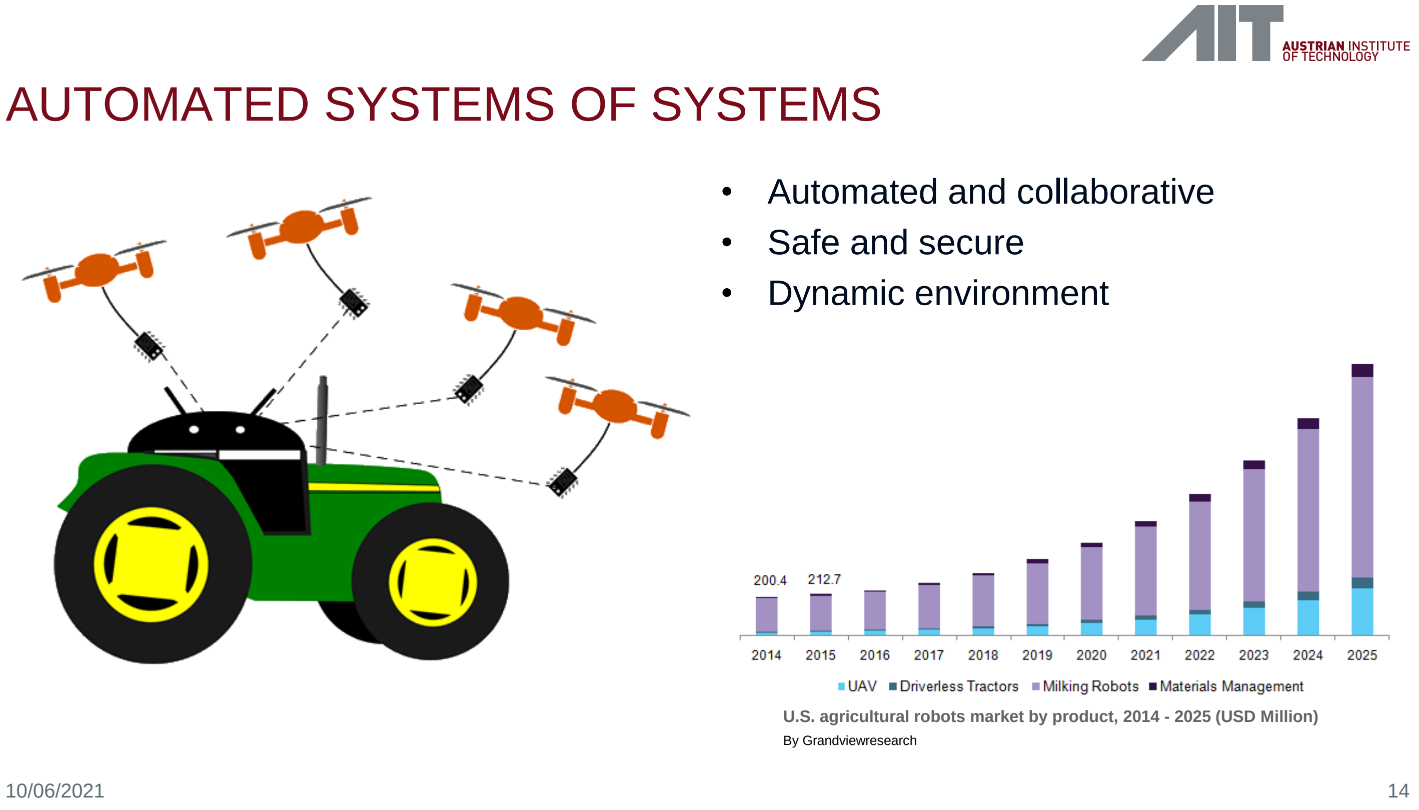
- Energy Efficiency
- Secure Communication
- Reliability
- Resistant against environmental factors

Smart Sensors

Estimated Agricultural IoT Device Shipments
Global
30
36
43
52
62
75
2015E
2016E
2017E
2018E
2019E
2020E
IoT Devices Shipped (Millions)
BI INTELLIGENCE
Source: BI Intelligence Estimates, 2015

10/06/2021

13



AUSTRIAN INSTITUTE OF TECHNOLOGY

AUTOMATED SYSTEMS OF SYSTEMS

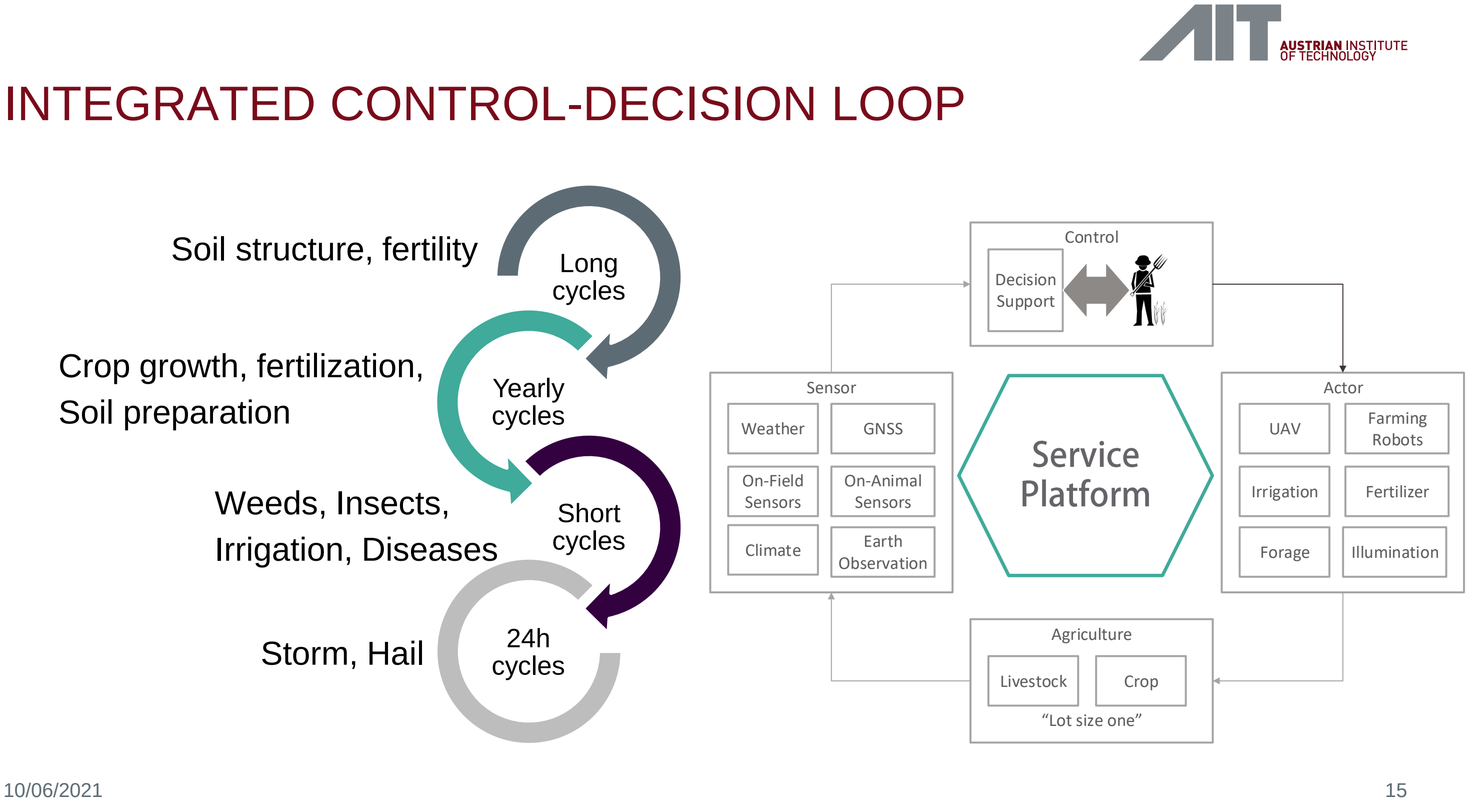
- Automated and collaborative
- Safe and secure
- Dynamic environment

U.S. agricultural robots market by product, 2014 - 2025 (USD Million)

By Grandviewresearch

10/06/2021

14

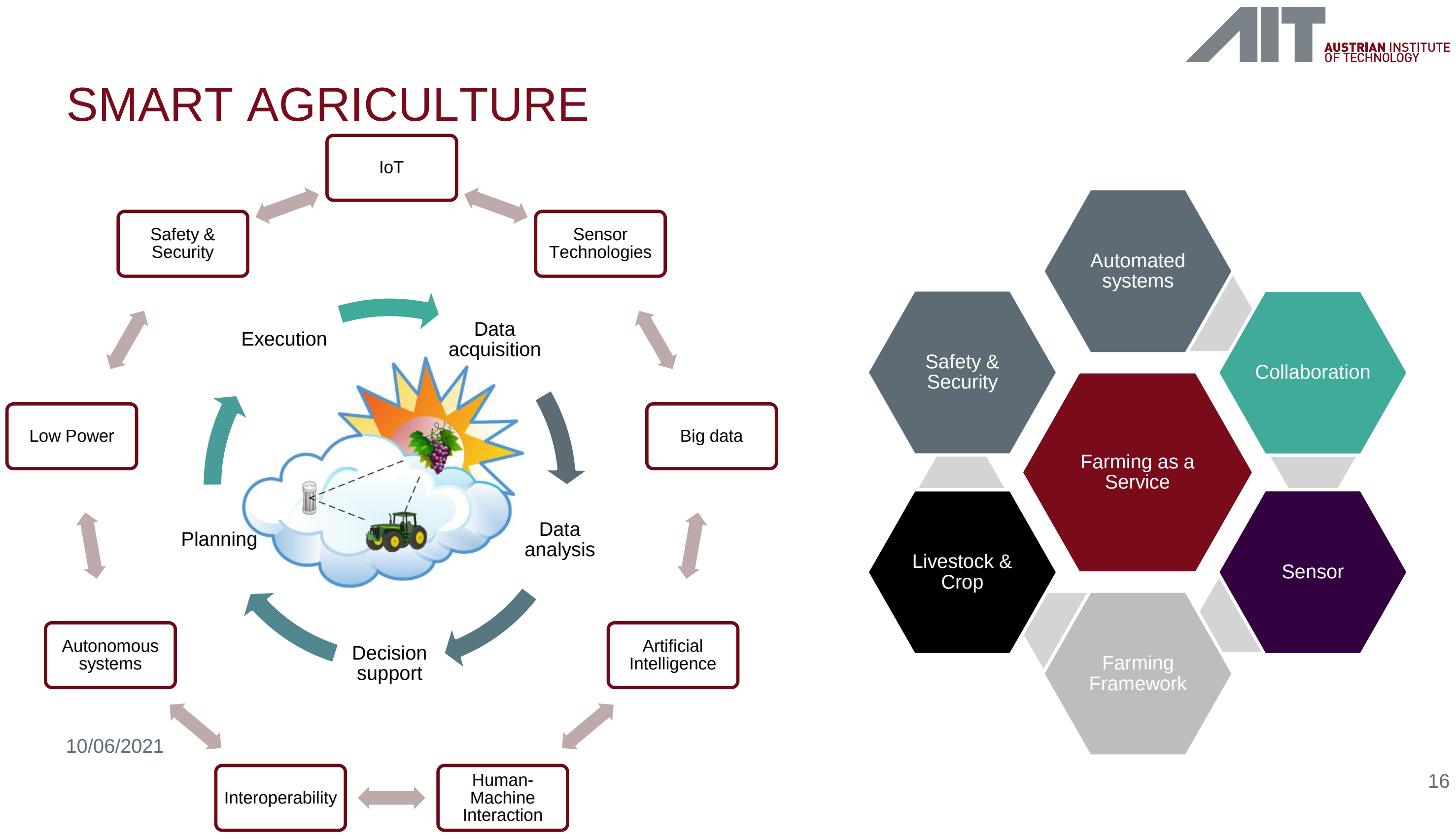


AUSTRIAN INSTITUTE OF TECHNOLOGY

INTEGRATED CONTROL-DECISION LOOP

10/06/2021

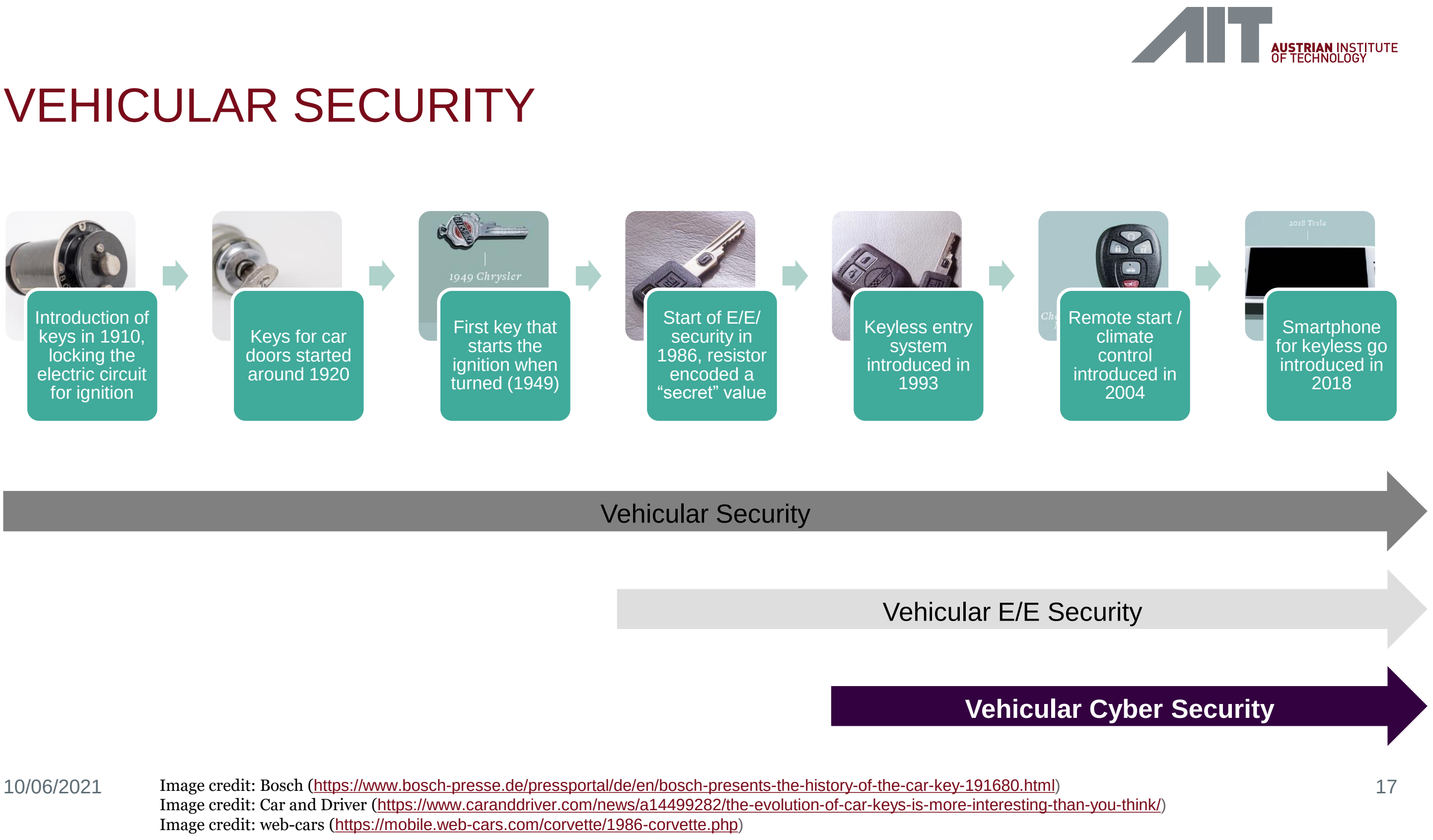
15



SMART AGRICULTURE

10/06/2021

16



VEHICULAR SECURITY

- Introduction of keys in 1910, locking the electric circuit for ignition
- Keys for car doors started around 1920
- First key that starts the ignition when turned (1949)
- Start of E/E/ security in 1986, resistor encoded a "secret" value
- Keyless entry system introduced in 1993
- Remote start / climate control introduced in 2004
- Smartphone for keyless go introduced in 2018

Vehicular Security

Vehicular E/E Security

Vehicular Cyber Security

10/06/2021

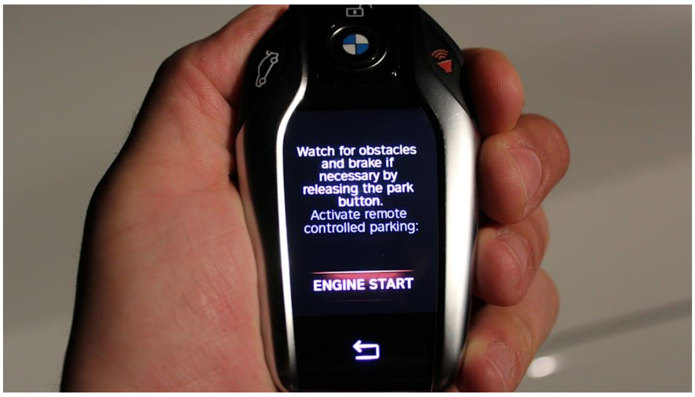
Image credit: Bosch (https://www.bosch-presse.de/pressportal/de/en/bosch-presents-the-history-of-the-car-key-191680.html)
Image credit: Car and Driver (https://www.caranddriver.com/news/a14499282/the-evolution-of-car-keys-is-more-interesting-than-you-think/)
Image credit: web-cars (https://mobile.web-cars.com/corvette/1986-corvette.php)

17

AUSTRIAN INSTITUTE OF TECHNOLOGY

VEHICULAR SECURITY

- In the past the main concern was **vehicle theft**
- With the introduction of new features concerns were extended to
  - **Safety**
  - **Financial**
  - **Operational**
  - **Privacy**


Watch for obstacles and brake if necessary by releasing the park button.
Activate remote controlled parking:
ENGINE START

10/06/2021 Image credit: Autoblog (https://www.autoblog.com/2017/07/07/bmw-display-key-technology-nobody-asked-for/#slide-1366051) 18

VEHICULAR SECURITY

- In the past the main concern was **vehicle theft**
- With the introduction of new features concerns were extended to
  - **Safety**
  - **Financial**
  - **Operational**
  - **Privacy**
- **Theft of Intellectual Property** is also a topic

Charlie Ciso
How come our Research VP just got fired?
I heard that our CEO was humiliated during some industry meeting at the FBI.
Apparently, everyone in the room had their IP stolen by the Chinese... except us!
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

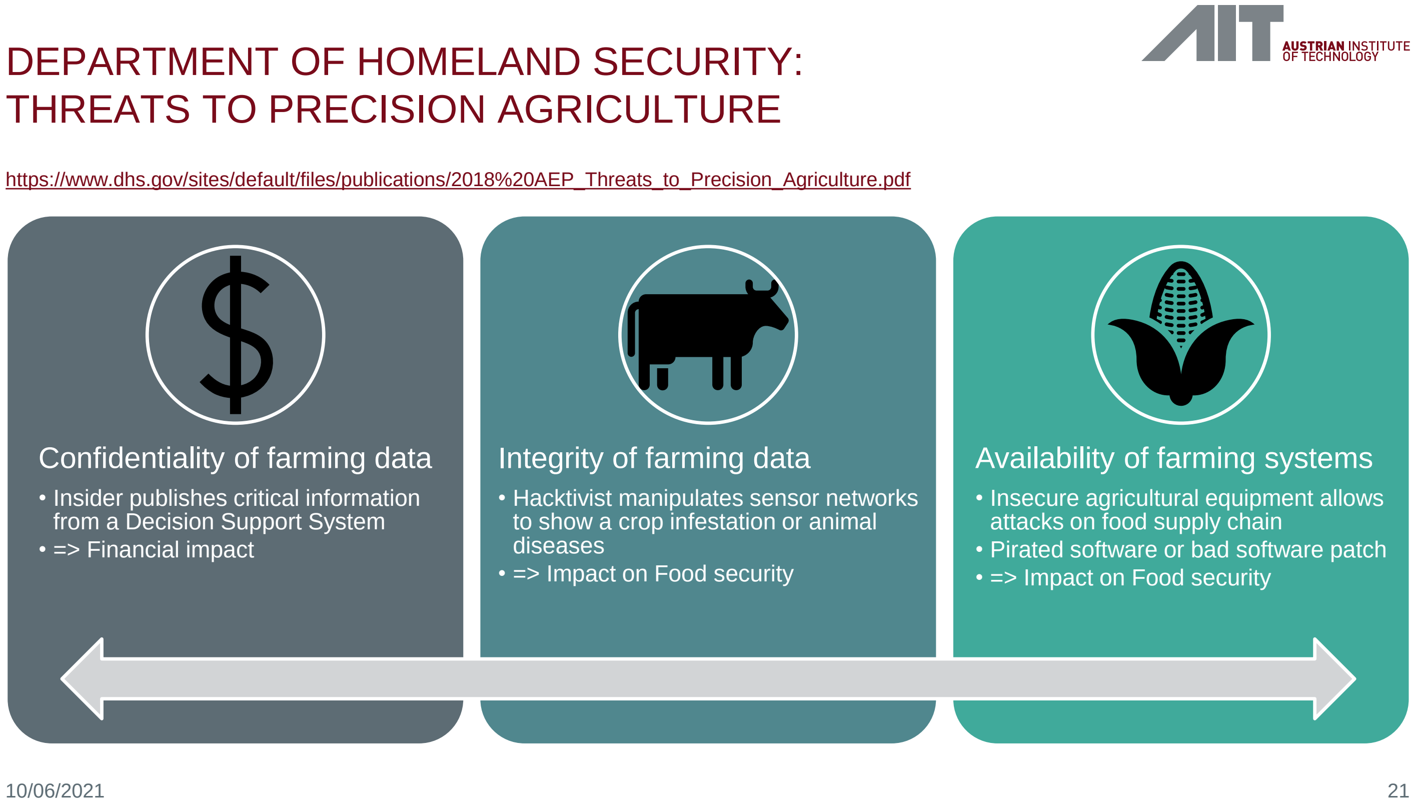
AUSTRIAN INSTITUTE OF TECHNOLOGY

PRIVACY

- Difference between
  - protection of personally identifiable data against hacking
  - Ensuring data minimization and lawful basis for data collection

Charlie Ciso
I want to talk to You about GDPR.
Marketing already showed me! Just think...
... A Giant Database of Personal Records!
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)



AUSTRIAN INSTITUTE OF TECHNOLOGY

DEPARTMENT OF HOMELAND SECURITY: THREATS TO PRECISION AGRICULTURE

https://www.dhs.gov/sites/default/files/publications/2018%20AEP_Threats_to_Precision_Agriculture.pdf

Confidentiality of farming data

- Insider publishes critical information from a Decision Support System
- => Financial impact

Integrity of farming data

- Hacktivist manipulates sensor networks to show a crop infestation or animal diseases
- => Impact on Food security

Availability of farming systems

- Insecure agricultural equipment allows attacks on food supply chain
- Pirated software or bad software patch
- => Impact on Food security

10/06/2021

21

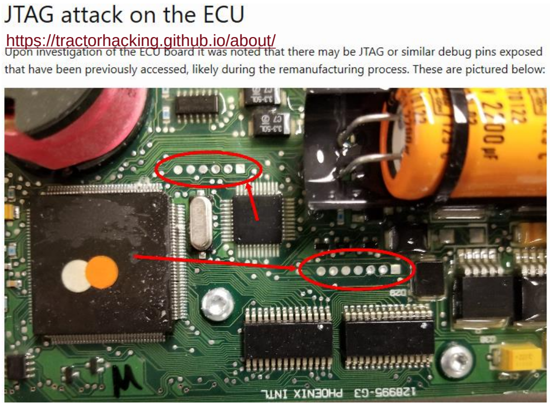
AUSTRIAN INSTITUTE OF TECHNOLOGY

PIRATED SOFTWARE

https://www.vice.com/en_us/article/xykkkd/why-american-farmers-are-hacking-their-tractors-with-ukrainian-firmware

MOTHERBOARD
TECH BY VICE

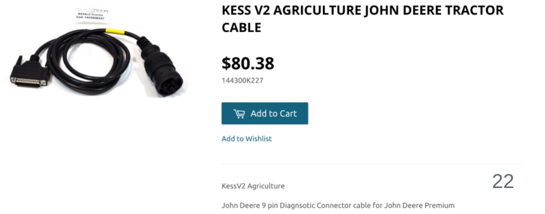
Why American Farmers Are Hacking Their Tractors With Ukrainian Firmware



JTAG attack on the ECU

https://tractorhacking.github.io/about/

Upon investigation of the ECU board it was noted that there may be JTAG or similar debug pins exposed that have been previously accessed, likely during the remanufacturing process. These are pictured below:



KESS V2 AGRICULTURE JOHN DEERE TRACTOR CABLE

$80.38

144300K227

Add to Cart

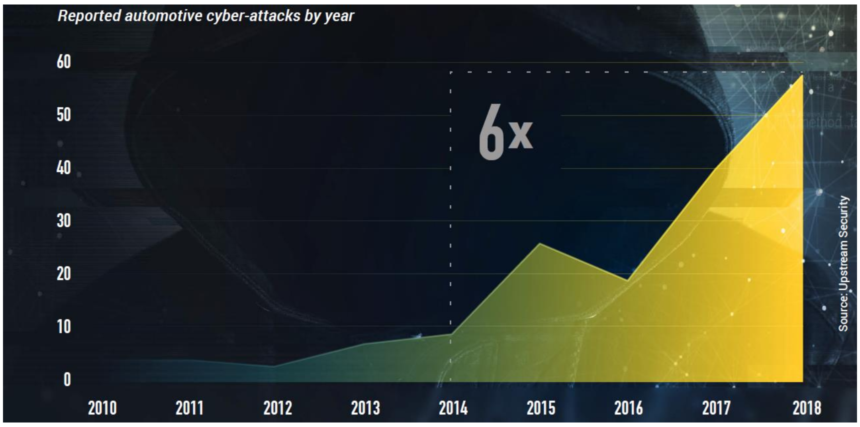
Add to Wishlist

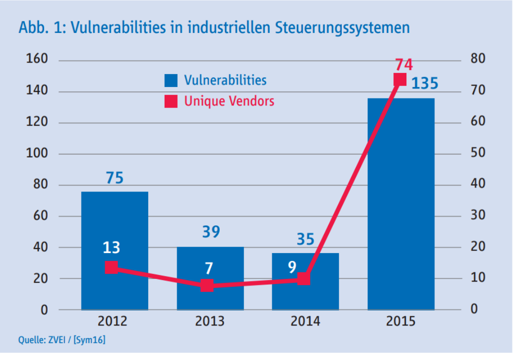
KessV2 Agriculture

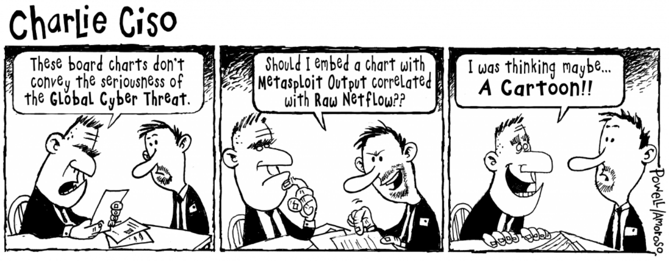
John Deere 9 pin Diagnsotic Connector cable for John Deere Premium

ATTACKS ON VEHICLES AND CONTROL SYSTEMS

AUSTRIAN INSTITUTE OF TECHNOLOGY






Charlie Ciso
These board charts don't convey the seriousness of the Global Cyber Threat.
Should I embed a chart with Metasploit Output correlated with Raw Netflow??
I was thinking maybe... A Cartoon!!
Powell/Amoroso

10/06/2021

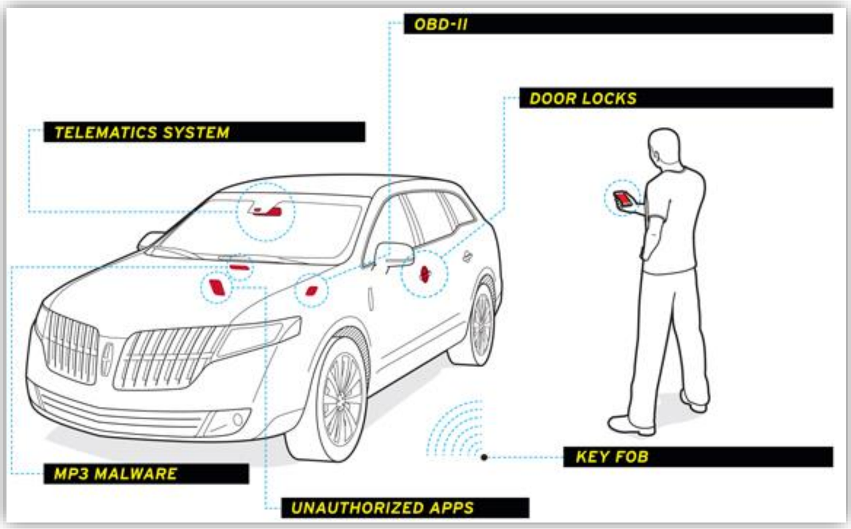
Image credit: Upstream Auto (https://www.upstream.auto/blog/q1-2018-automotive-cyber-hacks/)
Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)
Image credit: zvei: (Orientierungsleitfaden für Hersteller zur IEC 62443)

23

AUSTRIAN INSTITUTE OF TECHNOLOGY

RISING AWARENESS

- **Vulnerable** architectures
- Increasing **connectivity**
- Standards and regulation **without security**

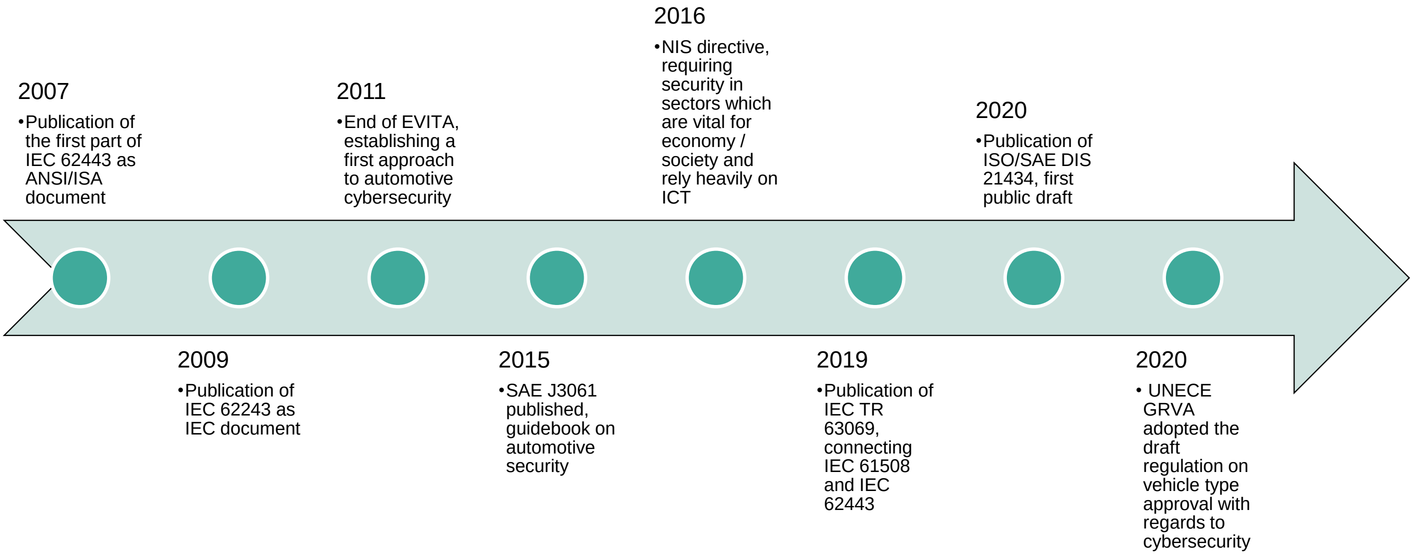


10/06/2021

Image credit: Car and Driver (https://www.caranddriver.com/features/a15124906/can-your-car-be-hacked-feature/

24

VEHICULAR (AND INDUSTRIAL) SECURITY



2007

- Publication of the first part of IEC 62443 as ANSI/ISA document

2009

- Publication of IEC 62243 as IEC document

2011

- End of EVITA, establishing a first approach to automotive cybersecurity

2015

- SAE J3061 published, guidebook on automotive security

2016

- NIS directive, requiring security in sectors which are vital for economy / society and rely heavily on ICT

2019

- Publication of IEC TR 63069, connecting IEC 61508 and IEC 62443

2020

- Publication of ISO/SAE DIS 21434, first public draft

2020

- UNECE GRVA adopted the draft regulation on vehicle type approval with regards to cybersecurity

10/06/2021 25

AUSTRIAN INSTITUTE OF TECHNOLOGY

TOMORROW TODAY

TERMINOLOGY

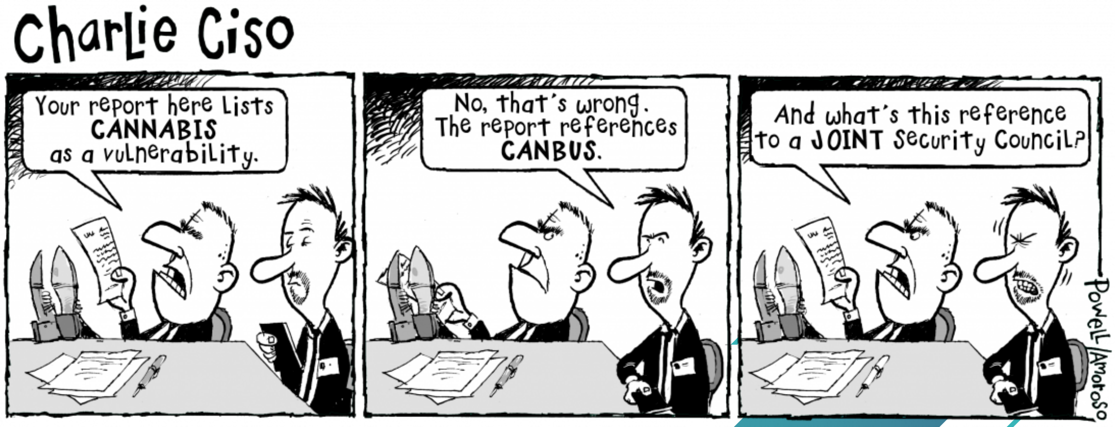
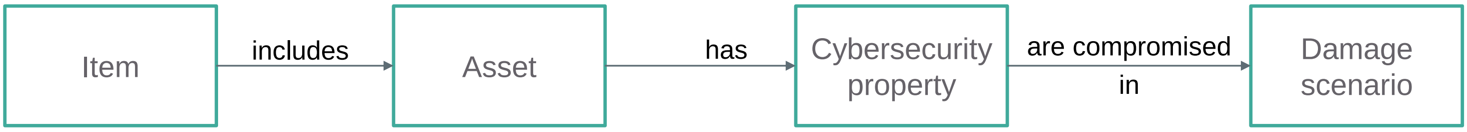

Charlie Ciso
Your report here lists CANNABIS as a vulnerability.
No, that's wrong. The report references CANBUS.
And what's this reference to a JOINT Security Council?
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

AUSTRIAN INSTITUTE OF TECHNOLOGY

VEHICULAR CYBERSECURITY

What do we protect



Item

includes

Asset

has

Cybersecurity property

are compromised in

Damage scenario

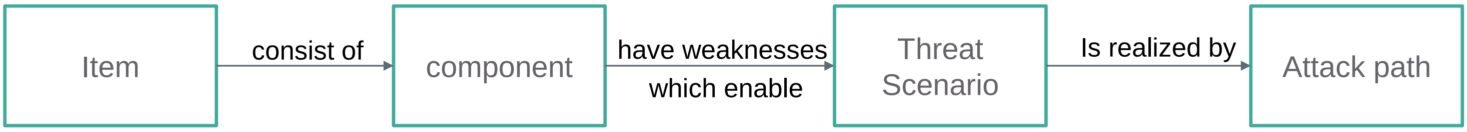
- Item: something which implements a function at vehicle level
- Asset: something of value
- Cybersecurity Property: attribute (CIA) of an asset which is important
- Damage scenario: violation of that property, causing an impact

Charlie Ciso
How do we recognize a DDoS attack?
Trust me, you'll know.
Charlie Ciso
Sorry, this panel is having trouble loading.
OK
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

VEHICULAR CYBERSECURITY

What could attack us



Item

consist of

component

have weaknesses which enable

Threat Scenario

Is realized by

Attack path

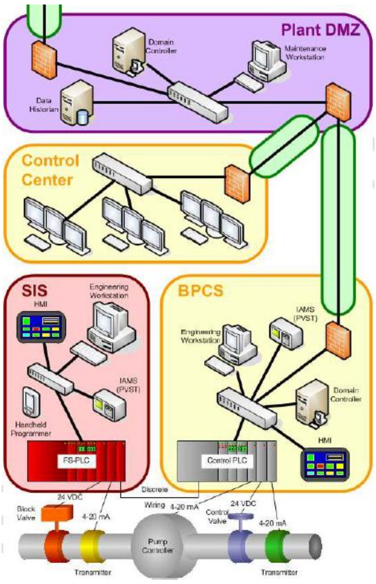
- Item: something which implements a function at vehicle level
- Components: part of the item
- Threat Scenario: something which exploits a weakness in an component
- Attack path: set of action which realize a threat scenario with a certain feasability

Charlie Ciso
You can't hold open the door. That's bad physical security.
Why? What's the Big Deal??
CIRCUS

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

AUSTRIAN INSTITUTE OF TECHNOLOGY

INDUSTRIAL CYBERSECURITY



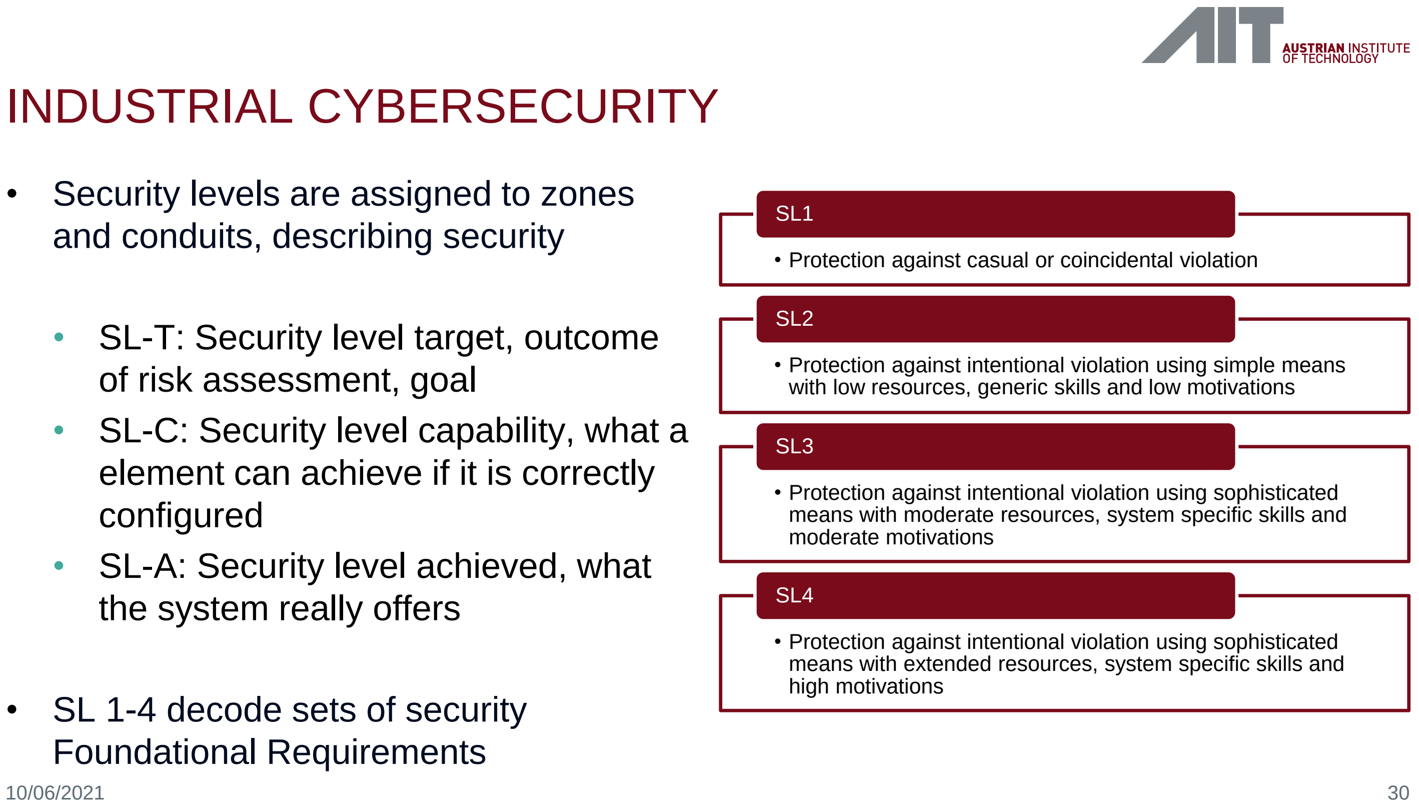
- Systems are divided into zones which groups elements with similar security needs
- Conduits are the only allowed connection between zones

Charlie Ciso
Why are there no windows in our Data Center?
Evil hackers might tunnel attacks over photons of light from outside.
Last month I told him Antivirus was stored in glass vials!!
Powell/Amoroso

10/06/2021

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)
Image credit: Slideshare (https://www.slideshare.net/Yokogawa1/secure-systems-security-and-isa99-iec62443)

29



INDUSTRIAL CYBERSECURITY

- Security levels are assigned to zones and conduits, describing security
  - SL-T: Security level target, outcome of risk assessment, goal
  - SL-C: Security level capability, what a element can achieve if it is correctly configured
  - SL-A: Security level achieved, what the system really offers
- SL 1-4 decode sets of security Foundational Requirements

SL1

- Protection against casual or coincidental violation

SL2

- Protection against intentional violation using simple means with low resources, generic skills and low motivations

SL3

- Protection against intentional violation using sophisticated means with moderate resources, system specific skills and moderate motivations

SL4

- Protection against intentional violation using sophisticated means with extended resources, system specific skills and high motivations

10/06/2021

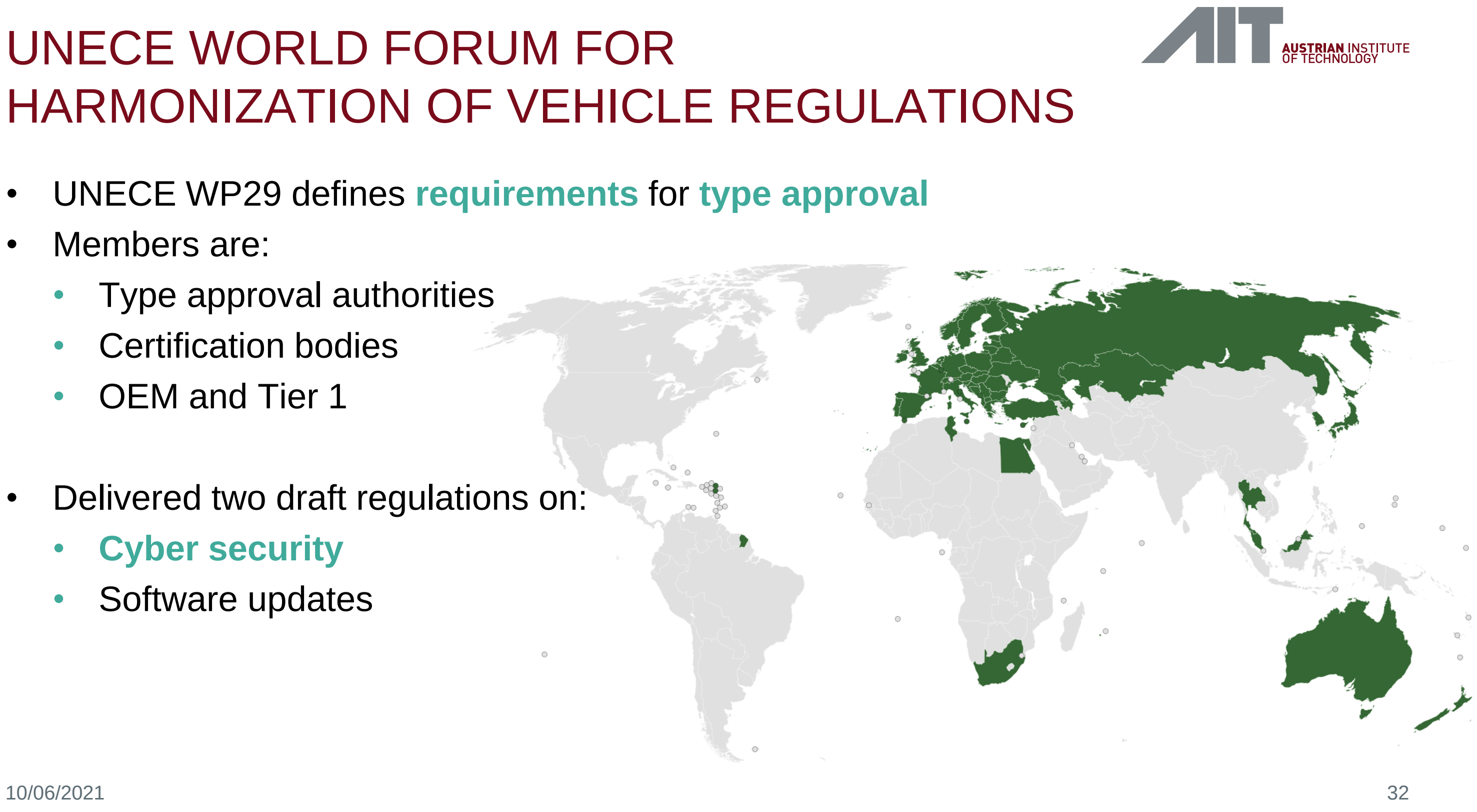
30

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

CYBERSECURITY REGULATION

Charlie Ciso
I wish Marketing would stop parading us in front of customers to make sales.
I think you're exaggerating, Charlie.
Ding!
Third Floor! Cyber Security!
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)



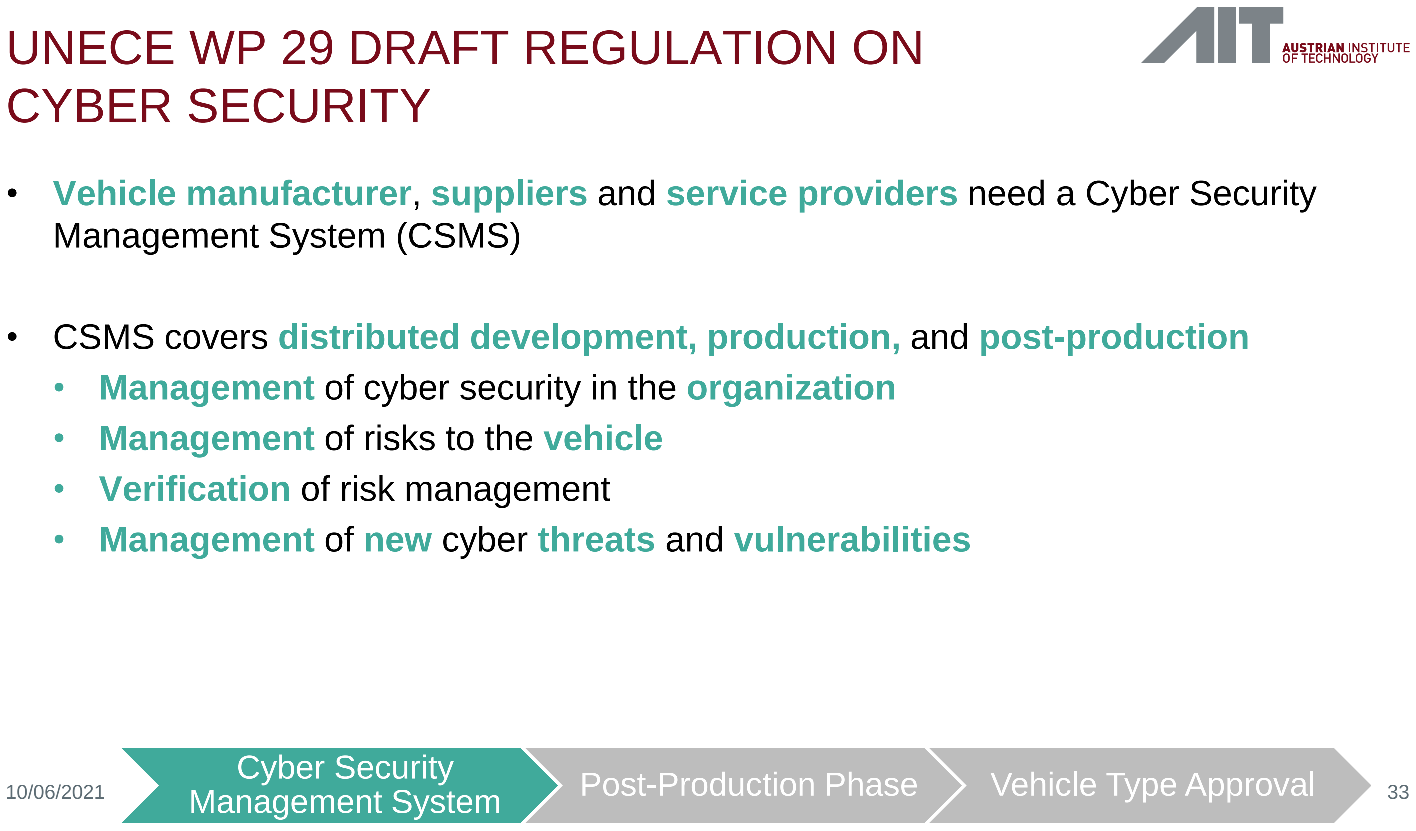
UNECE WORLD FORUM FOR HARMONIZATION OF VEHICLE REGULATIONS

AUSTRIAN INSTITUTE OF TECHNOLOGY

- UNECE WP29 defines **requirements** for **type approval**
- Members are:
  - Type approval authorities
  - Certification bodies
  - OEM and Tier 1
- Delivered two draft regulations on:
  - **Cyber security**
  - Software updates

10/06/2021

32



UNECE WP 29 DRAFT REGULATION ON CYBER SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

- **Vehicle manufacturer**, **suppliers** and **service providers** need a Cyber Security Management System (CSMS)

- CSMS covers **distributed development, production,** and **post-production**
  - **Management** of cyber security in the **organization**
  - **Management** of risks to the **vehicle**
  - **Verification** of risk management
  - **Management** of **new** cyber **threats** and **vulnerabilities**

10/06/2021

Cyber Security Management System → Post-Production Phase → Vehicle Type Approval

33

UNECE WP 29 DRAFT REGULATION ON CYBER SECURITY

- **Compliance** with the regulation is **maintained** through the **vehicle lifecycle**
  - **Monitoring** of changes in the **threat landscape** and vulnerabilities.
  - **Implemented** security measures need to be **monitored** for **effectiveness**.
  - **Changing** circumstances should **not impact safety** and **availability**.

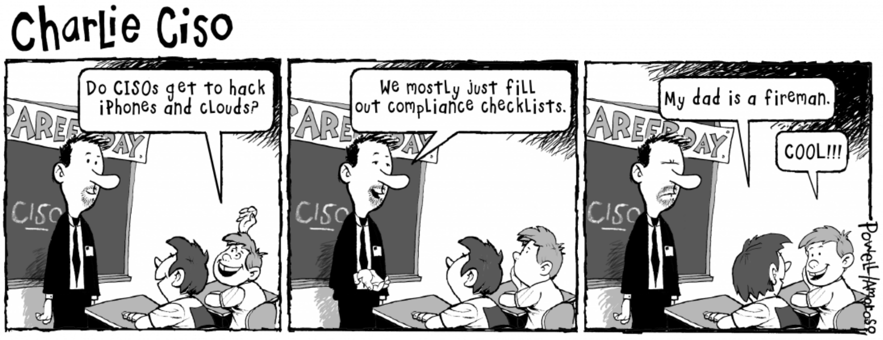
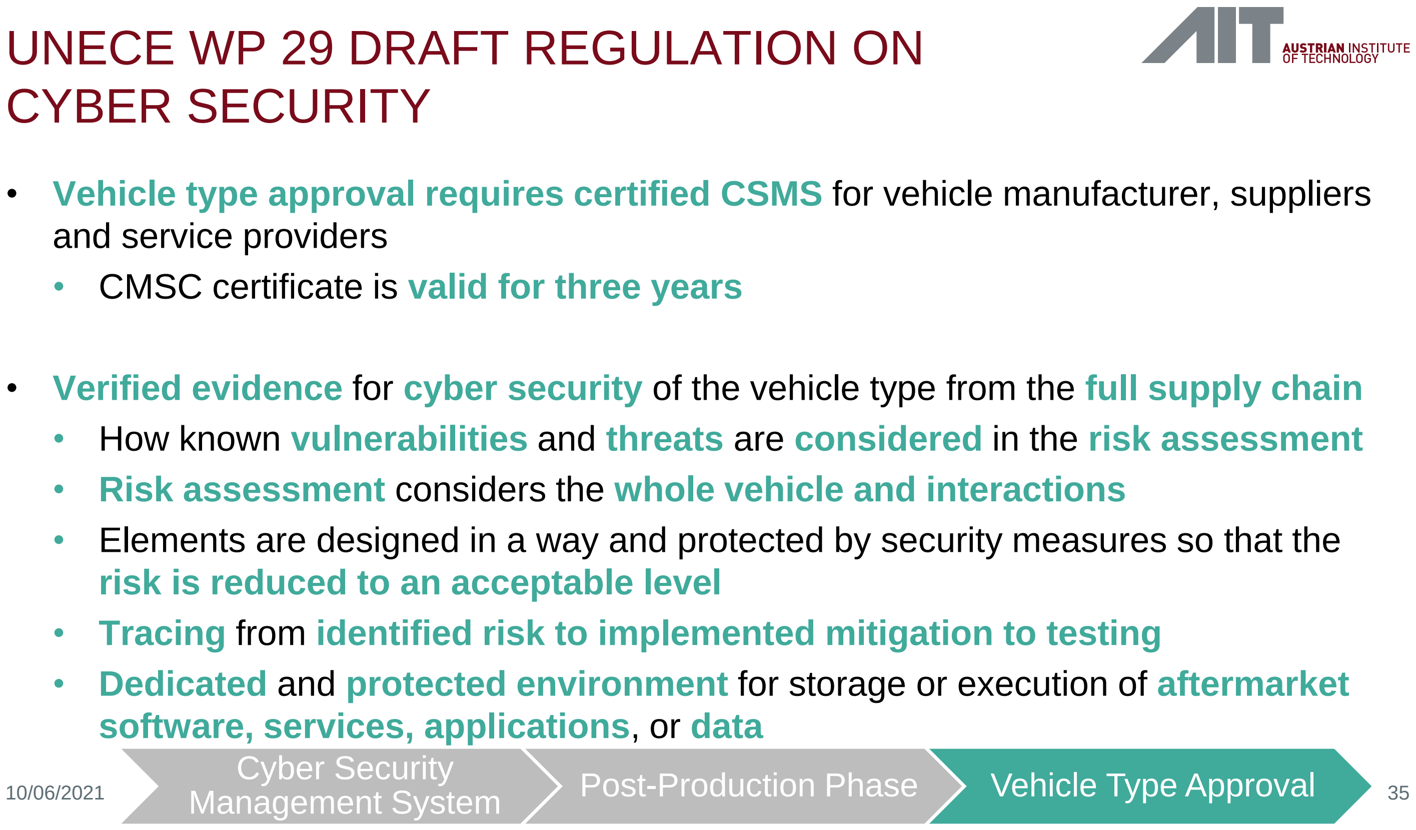

Charlie Ciso
Do CISOs get to hack iPhones and clouds?
We mostly just fill out compliance checklists.
My dad is a fireman.
COOL!!!
CAREER DAY
CISO
Powell/Amoroso

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)

Cyber Security Management System → Post-Production Phase → Vehicle Type Approval



UNECE WP 29 DRAFT REGULATION ON CYBER SECURITY

AUSTRIAN INSTITUTE OF TECHNOLOGY

- **Vehicle type approval requires certified CSMS** for vehicle manufacturer, suppliers and service providers
  - CMSC certificate is **valid for three years**

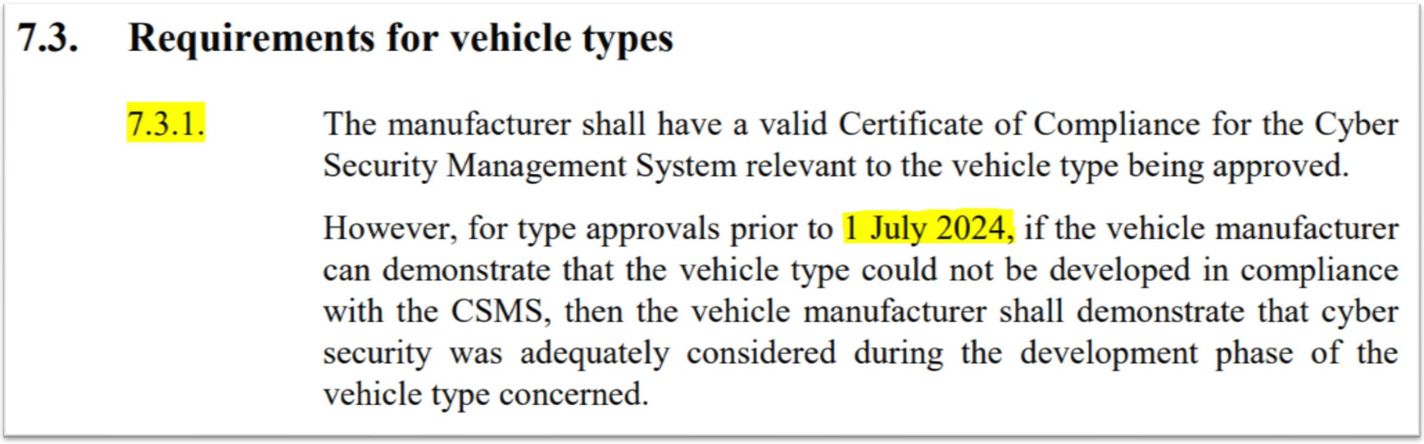
- **Verified evidence** for **cyber security** of the vehicle type from the **full supply chain**
  - How known **vulnerabilities** and **threats** are **considered** in the **risk assessment**
  - **Risk assessment** considers the **whole vehicle and interactions**
  - Elements are designed in a way and protected by security measures so that the **risk is reduced to an acceptable level**
  - **Tracing** from **identified risk to implemented mitigation to testing**
  - **Dedicated** and **protected environment** for storage or execution of **aftermarket software, services, applications**, or **data**

10/06/2021

Cyber Security Management System | Post-Production Phase | Vehicle Type Approval

35

TIMELINE - VEHICLES



7.3. Requirements for vehicle types

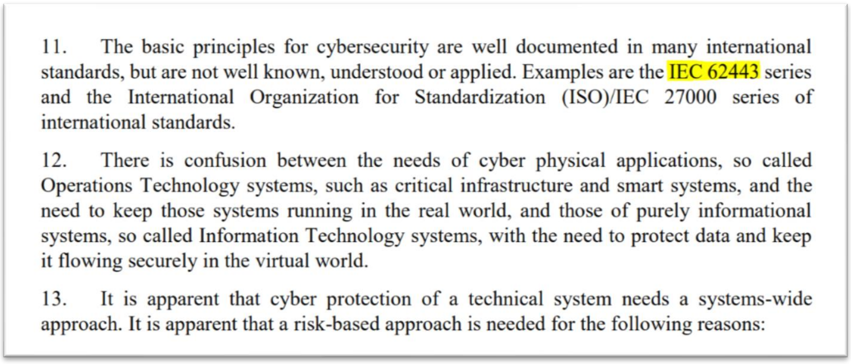
7.3.1. The manufacturer shall have a valid Certificate of Compliance for the Cyber Security Management System relevant to the vehicle type being approved.

However, for type approvals prior to 1 July 2024, if the vehicle manufacturer can demonstrate that the vehicle type could not be developed in compliance with the CSMS, then the vehicle manufacturer shall demonstrate that cyber security was adequately considered during the development phase of the vehicle type concerned.

Image credit: UNECE (https://www.unece.org/fileadmin/DAM/trans/doc/2020/wp29grva/GRVA-06-19r1e.pdf)

TIMELINE - INDUSTRIAL

- United Nations Economic Commission for Europe (UNECE) confirmed in 2018 to integrate ISA/IEC 62443 series of standards into its forthcoming Common Regulatory Framework (CRF).
- The CRF will serve as an official UN policy position statement for Europe, establishing a common legislative basis for cybersecurity practices within the European Union trade markets.



11. The basic principles for cybersecurity are well documented in many international standards, but are not well known, understood or applied. Examples are the IEC 62443 series and the International Organization for Standardization (ISO)/IEC 27000 series of international standards.

12. There is confusion between the needs of cyber physical applications, so called Operations Technology systems, such as critical infrastructure and smart systems, and the need to keep those systems running in the real world, and those of purely informational systems, so called Information Technology systems, with the need to protect data and keep it flowing securely in the virtual world.

13. It is apparent that cyber protection of a technical system needs a systems-wide approach. It is apparent that a risk-based approach is needed for the following reasons:

Image credit: UNECE (https://www.unece.org/fileadmin/DAM/trade/wp6/documents/2018/ECE_CTCS_WP.6_2018_9E_Cybersecurity.pdf)

AUSTRIAN INSTITUTE OF TECHNOLOGY

TOMORROW TODAY

CYBERSECURITY STANDARDS

Overview

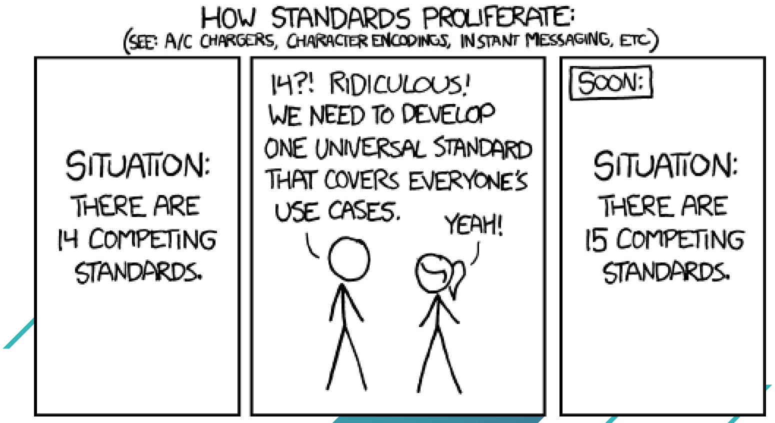
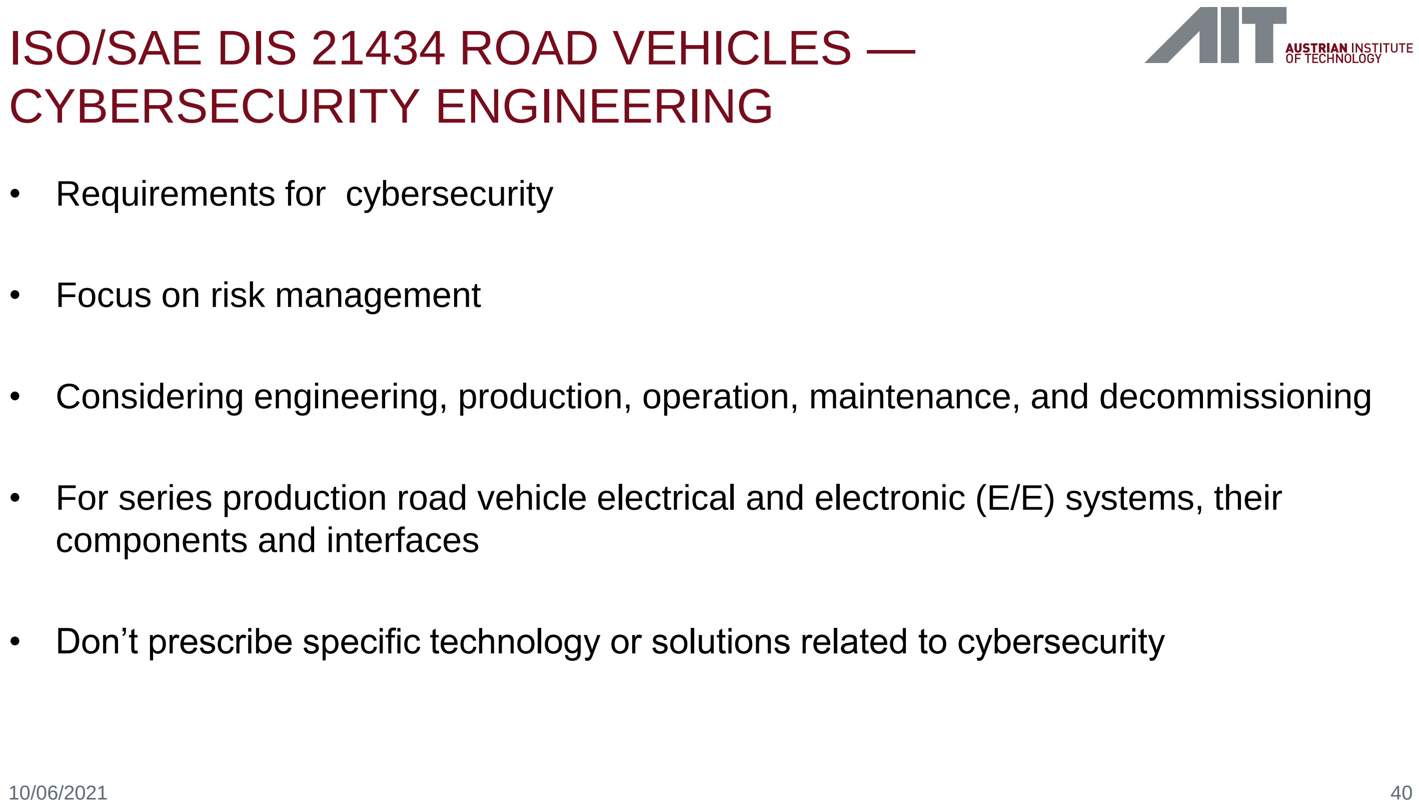

HOW STANDARDS PROLIFERATE:
(SEE: A/C CHARGERS, CHARACTER ENCODINGS, INSTANT MESSAGING, ETC.)
SITUATION: THERE ARE 14 COMPETING STANDARDS.
14?! RIDICULOUS! WE NEED TO DEVELOP ONE UNIVERSAL STANDARD THAT COVERS EVERYONE'S USE CASES.
YEAH!
SOON:
SITUATION: THERE ARE 15 COMPETING STANDARDS.

Image credit: XCKD (https://xkcd.com/927/)

AUSTRIAN INSTITUTE
OF TECHNOLOGY
TOMORROW TODAY

VEHICULAR

Cybersecurity Standards



ISO/SAE DIS 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING

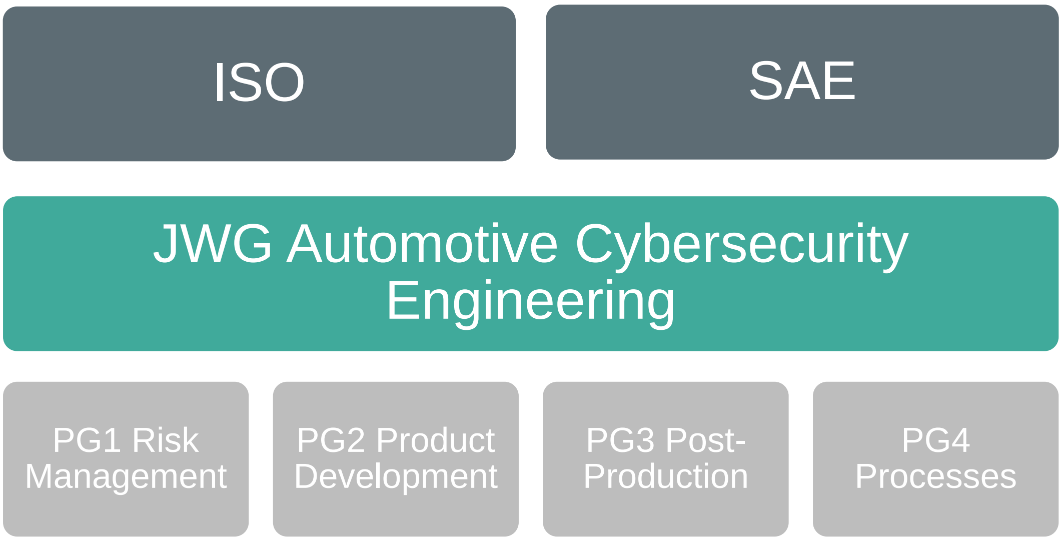
AUSTRIAN INSTITUTE OF TECHNOLOGY

- Requirements for cybersecurity
- Focus on risk management
- Considering engineering, production, operation, maintenance, and decommissioning
- For series production road vehicle electrical and electronic (E/E) systems, their components and interfaces
- Don't prescribe specific technology or solutions related to cybersecurity

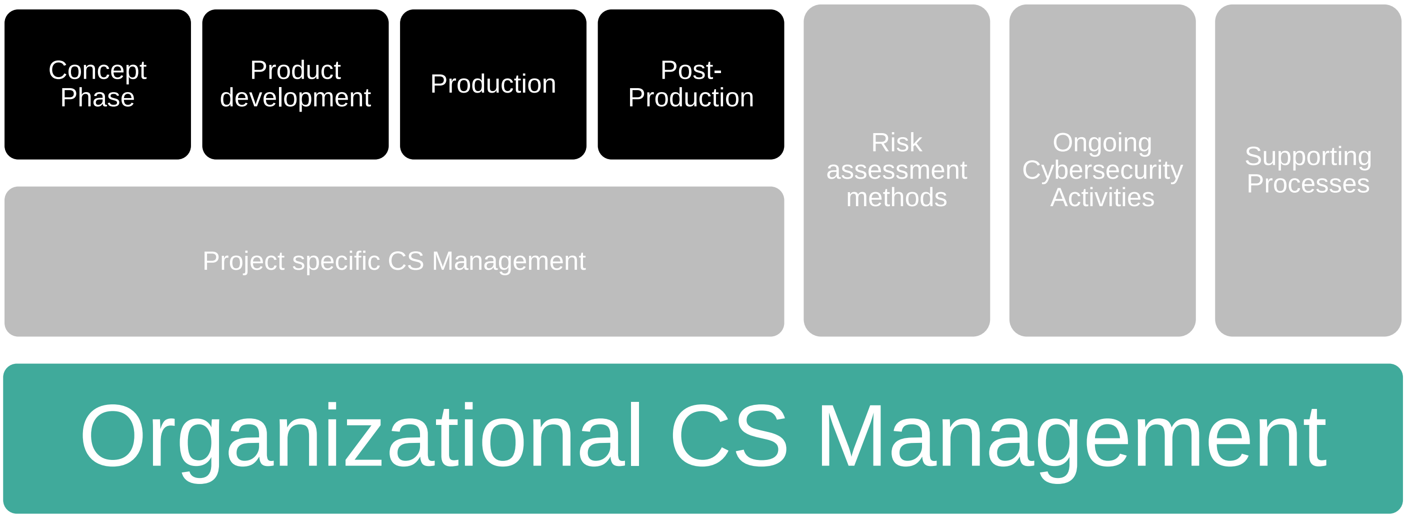
10/06/2021 40

ISO/SAE CD 21434 Road Vehicles — Cybersecurity engineering

- Standard is developed in cooperation between ISO and SAE



ISO/SAE CD 21434 ROAD VEHICLES — CYBERSECURITY ENGINEERING



Concept Phase

Product development

Production

Post-Production

Project specific CS Management

Risk assessment methods

Ongoing Cybersecurity Activities

Supporting Processes

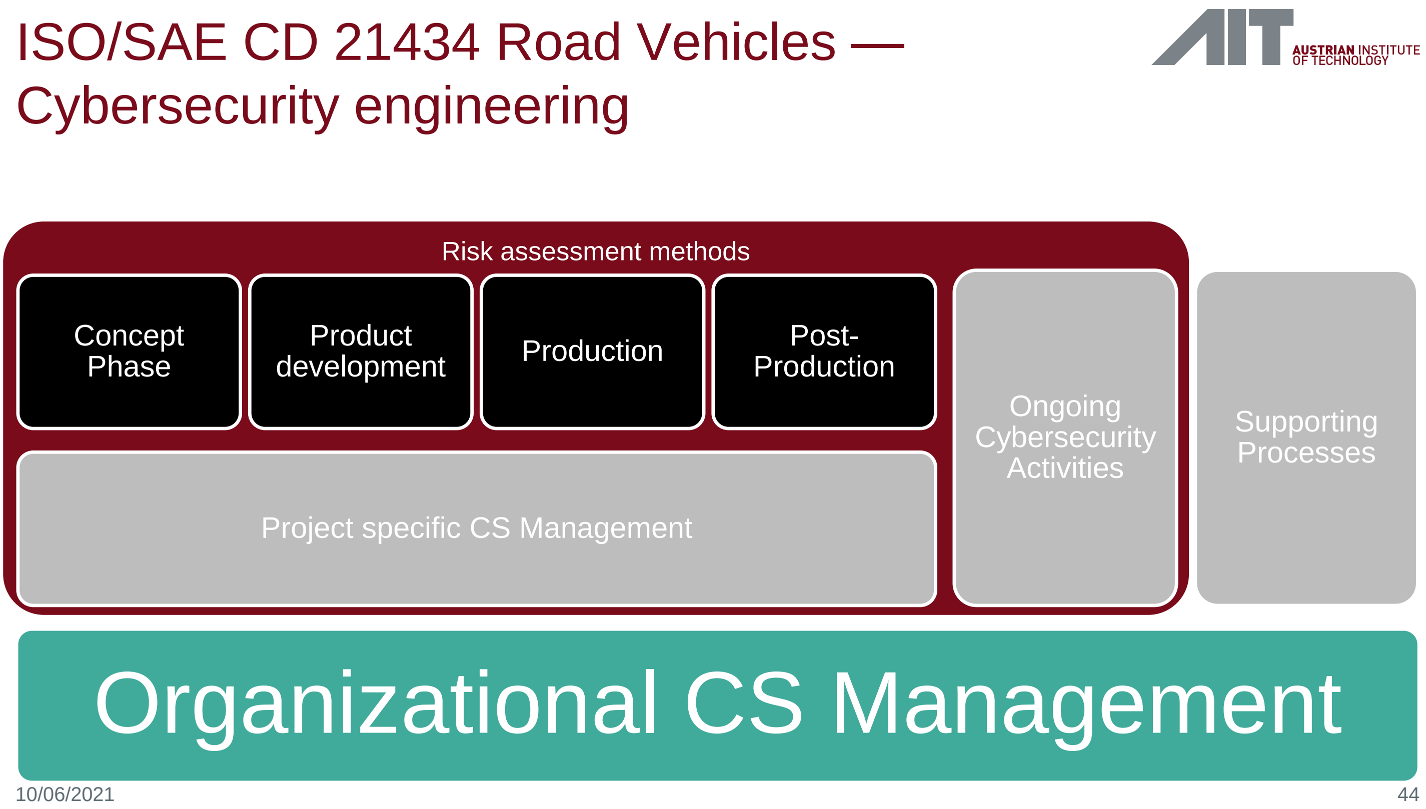
Organizational CS Management

CS = Cybersecurity

ISO/SAE CD 21434 Road Vehicles — Cybersecurity engineering

- **Risk Assessment methods**
  - Phase / Detail independent modules which can be called
  - Risk management for Safety, Financial, Operational and
- **Concept, Product development, Production, Post-Production**
  - Item to component level
  - Production and Post-Production is covered
- **Project specific CS Management**
  - CS planning, CS Case, CS assessment
- **Ongoing CS Activities**
  - Monitoring, Knowledge Base
- **Supporting Processes**
  - Quality, Information Security, Competence Management
- **Organizational CS Management**
  - CS culture, Information sharing

CS = Cybersecurity



ISO/SAE CD 21434 Road Vehicles — Cybersecurity engineering

Risk assessment methods

Concept Phase

Product development

Production

Post-Production

Project specific CS Management

Ongoing Cybersecurity Activities

Supporting Processes

Organizational CS Management

10/06/2021

44

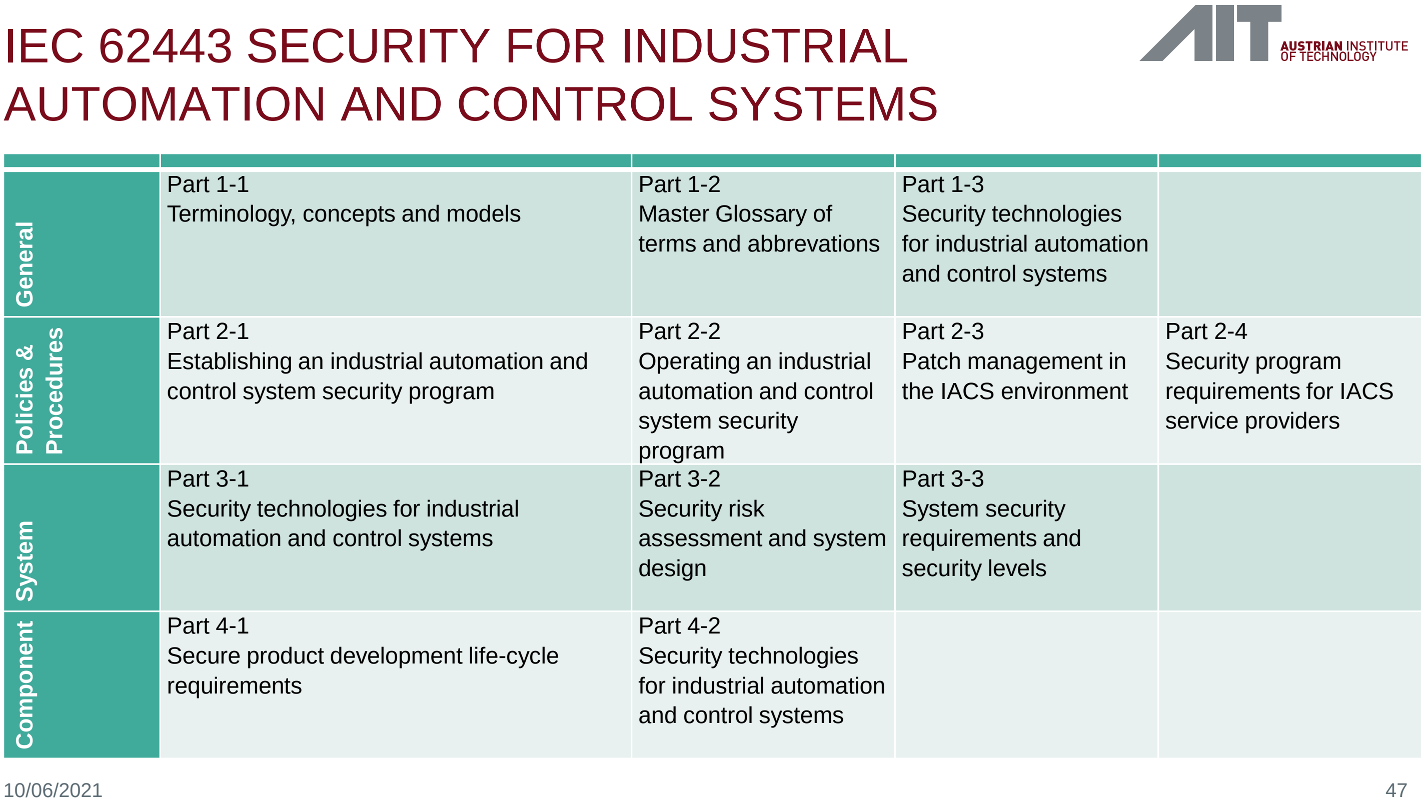
ONGOING DEVELOPMENTS

Automotive

- ISO/AWI 24089 Road vehicles — Software update engineering
  - Upcoming standard for automotive software updates
- ISO/WD PAS 5112 Road vehicles — Guidelines for auditing cybersecurity engineering
  - New development, describing how to audit a cybersecurity process

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

INDUSTRIAL
Cybersecurity Standards



IEC 62443 SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

AUSTRIAN INSTITUTE OF TECHNOLOGY

General	Part 1-1 Terminology, concepts and models	Part 1-2 Master Glossary of terms and abbrevations	Part 1-3 Security technologies for industrial automation and control systems	
Policies & Procedures	Part 2-1 Establishing an industrial automation and control system security program	Part 2-2 Operating an industrial automation and control system security program	Part 2-3 Patch management in the IACS environment	Part 2-4 Security program requirements for IACS service providers
System	Part 3-1 Security technologies for industrial automation and control systems	Part 3-2 Security risk assessment and system design	Part 3-3 System security requirements and security levels	
Component	Part 4-1 Secure product development life-cycle requirements	Part 4-2 Security technologies for industrial automation and control systems		

10/06/2021

47

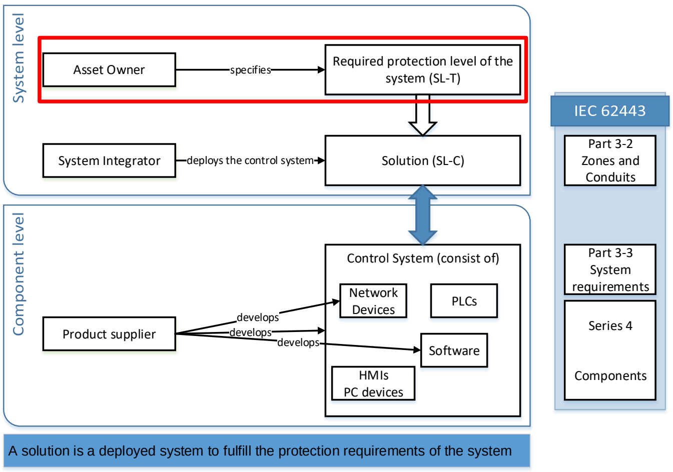
IEC62443 - PARTS

- Set 1 described generic concepts
- Set 2 describes management of security
- Set 3 describes approach from system owner / integrator point of view
- Set 4 describes approach from component developer point of view

AUSTRIAN INSTITUTE OF TECHNOLOGY

APPROACH - ASSET OWNER

- Asset owner uses Part 3-2 to determine the security needs of his system
  - Considering safety and business criticality
  - Consider logical and functional specialties
- Develops a security architecture
  - Divide system into zones
  - A zone collects systems with a similar criticality level or security needs
    - Everything safety-critical, everything wireless, …
    - Zones share a target security level (SL-T)
    - Target security level is a vector, describing security properties

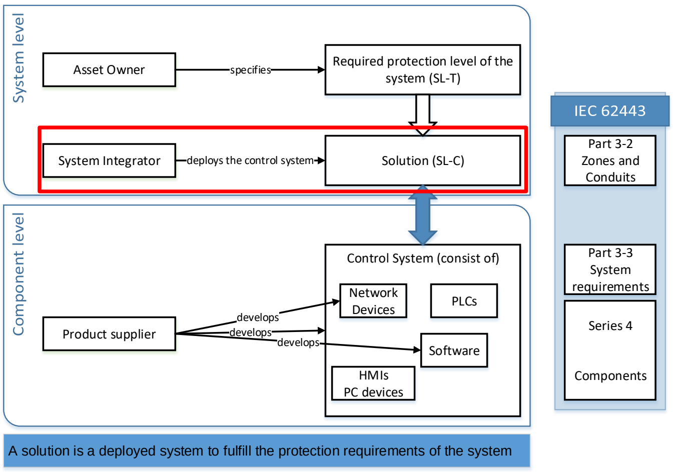


A solution is a deployed system to fulfill the protection requirements of the system

AUSTRIAN INSTITUTE OF TECHNOLOGY

APPROACH – SYSTEM INTEGRATOR

- System Integrator uses Part 3-3 to design a system, fulfilling the target security level
- Utilizes elements with inbuilt security properties
- Need also to consider required safety, availability, timeliness and other requirements
- System possess Security Level Capabilities (SL-C)

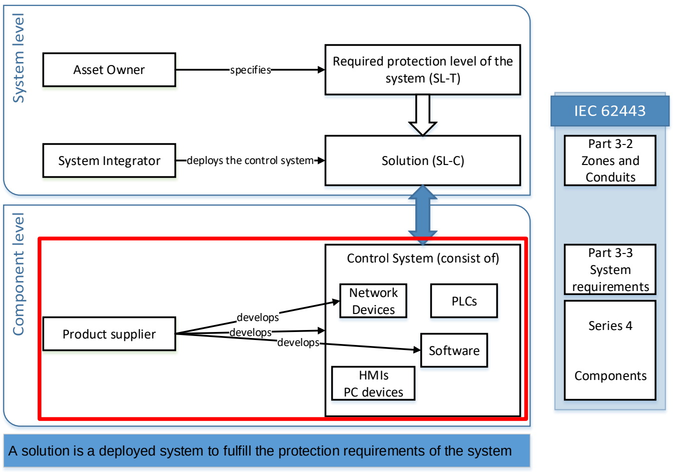


A solution is a deployed system to fulfill the protection requirements of the system

AUSTRIAN INSTITUTE OF TECHNOLOGY

APPROACH – PRODUCT SUPPLIER

- Product supplier uses Set 4 to develop secure components
- Part 4-1 describes secure development lifecycles, required capabilities => process
- Part 4-2 describe security measures which can be inbuilt into the system
- Components are developed independent of system level
    - Components are developed by product supplier based on assumed usage and security measures are chosen
    - Fulfillment of security requirements depend on solutions
    - => Components can be reused for multiple systems



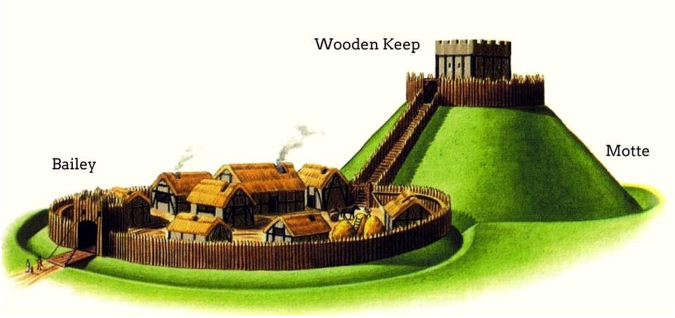
A solution is a deployed system to fulfill the protection requirements of the system

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THREAT MODELING FOR VEHICLES

WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses

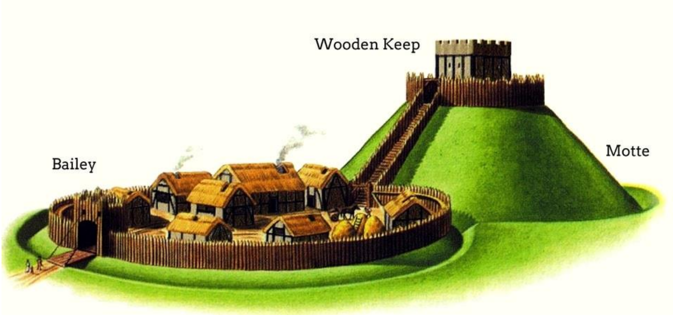


https://www.castlesworld.com/tools/motte-and-bailey-castles.php

AUSTRIAN INSTITUTE OF TECHNOLOGY

WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats



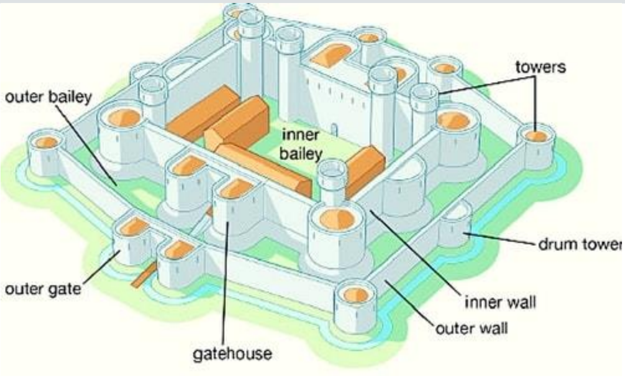
https://www.castlesworld.com/tools/motte-and-bailey-castles.php

https://deadliestwarrior.fandom.com/wiki/Huo_Chien

AUSTRIAN INSTITUTE OF TECHNOLOGY

WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
  - Resolving identified weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats

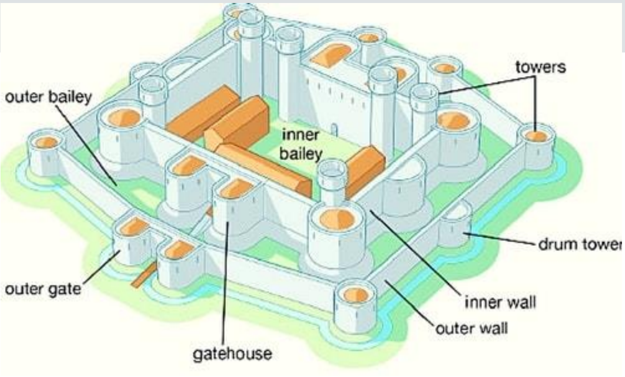


https://www.castlesworld.com/tools/concentric-castles.php

https://deadliestwarrior.fandom.com/wiki/Huo_Chien

WHAT IS THREAT MODELING

- **Structured Process**
  - Examination of a system for potential weaknesses
  - Resolving identified weaknesses
- **Systematic approach**
  - Based on a conceptual model of weaknesses and threats
  - Keeping the model of weaknesses and threats current



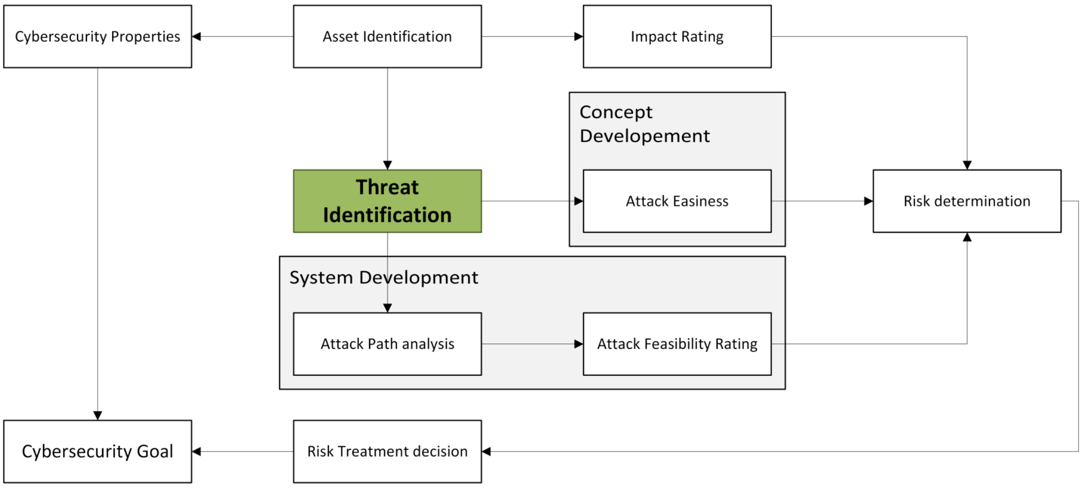
https://www.castlesworld.com/tools/concentric-castles.php

https://www.pbs.org/video/1812-niagara-frontier-fort-george-cannon-firing/

AUSTRIAN INSTITUTE OF TECHNOLOGY

THREAT MODELING AND AUTOMOTIVE

Threat Identification is included in ISO/SAE 21434 and UNECE WP29 Draft Regulation



57

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

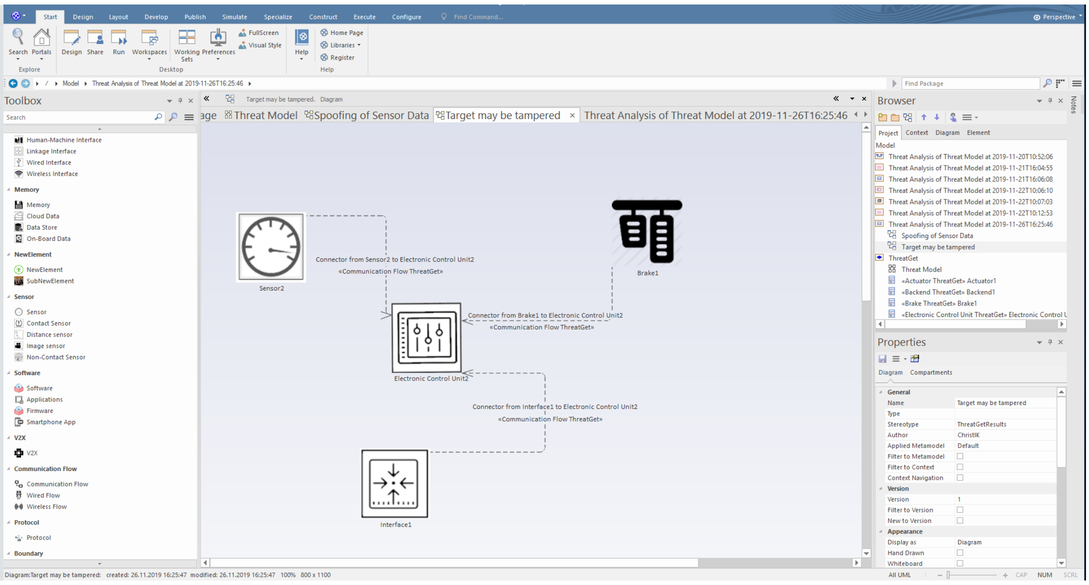
AIT APPROACH FOR THREAT MODELING

Developed for embedded systems and integrated in model-based engineering

MODEL-BASED ENGINEERING

Security Model

- **ThreatGet is integrated into Enterprise Architect Tool**
- **Security model and system model are connected**



Model
- Threat Analysis of Threat Model at 2019-11-20T10:52:06
- Threat Analysis of Threat Model at 2019-11-21T16:04:55
- Threat Analysis of Threat Model at 2019-11-21T16:06:08
- Threat Analysis of Threat Model at 2019-11-22T10:06:10
- Threat Analysis of Threat Model at 2019-11-22T10:07:03
- Threat Analysis of Threat Model at 2019-11-22T10:12:53
- Threat Analysis of Threat Model at 2019-11-26T16:25:46
  - Spoofing of Sensor Data
  - Target may be tampered
- ThreatGet
  - Threat Model
  - «Actuator ThreatGet» Actuator1
  - «Backend ThreatGet» Backend1
  - «Brake ThreatGet» Brake1
  - «Electronic Control Unit ThreatGet» Electronic Control U

General	
Name	Target may be tampered
Type	
Stereotype	ThreatGetResults
Author	ChristlK
Applied Metamodel	Default
Filter to Metamodel	□
Filter to Context	□
Context Navigation	□
Version	
Version	1
Filter to Version	□
New to Version	□
Appearance	
Display as	Diagram
Hand Drawn	□
Whiteboard	□

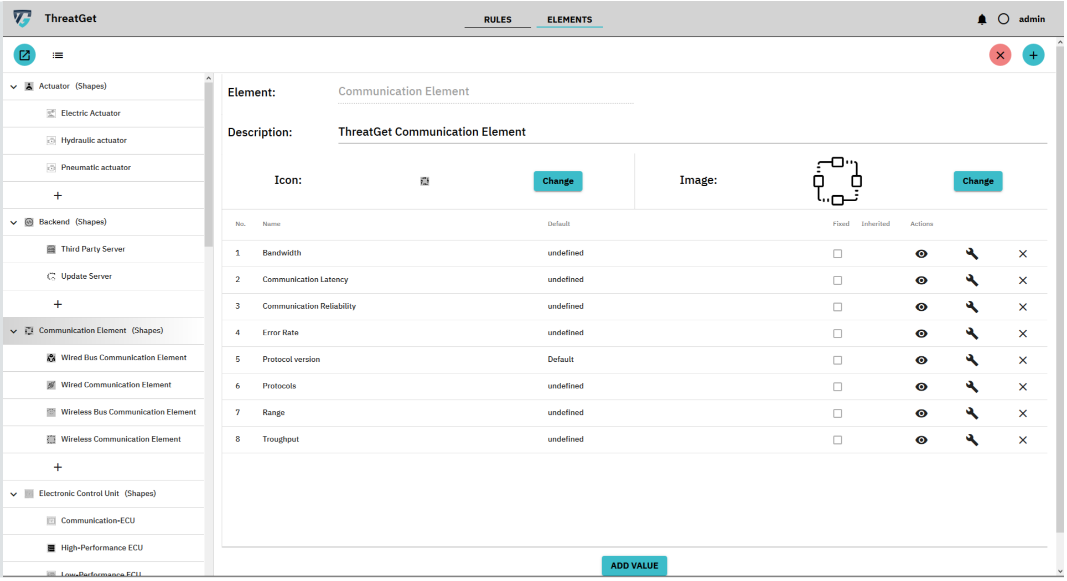
Diagram:Target may be tampered: created: 26.11.2019 16:25:47 modified: 26.11.2019 16:25:47 100% 800 x 1100

AUSTRIAN INSTITUTE OF TECHNOLOGY

DOMAIN ELEMENTS

Domain Elements

- Set of common elements for a domain
- Inheritance and Refinement
- Customizable



- Actuator (Shapes)
  - Electric Actuator
  - Hydraulic actuator
  - Pneumatic actuator
  - +
- Backend (Shapes)
  - Third Party Server
  - Update Server
  - +
- Communication Element (Shapes)
  - Wired Bus Communication Element
  - Wired Communication Element
  - Wireless Bus Communication Element
  - Wireless Communication Element
  - +
- Electronic Control Unit (Shapes)
  - Communication-ECU
  - High-Performance ECU
  - Low-Performance ECU

Element: Communication Element

Description: ThreatGet Communication Element

Icon:

Image:

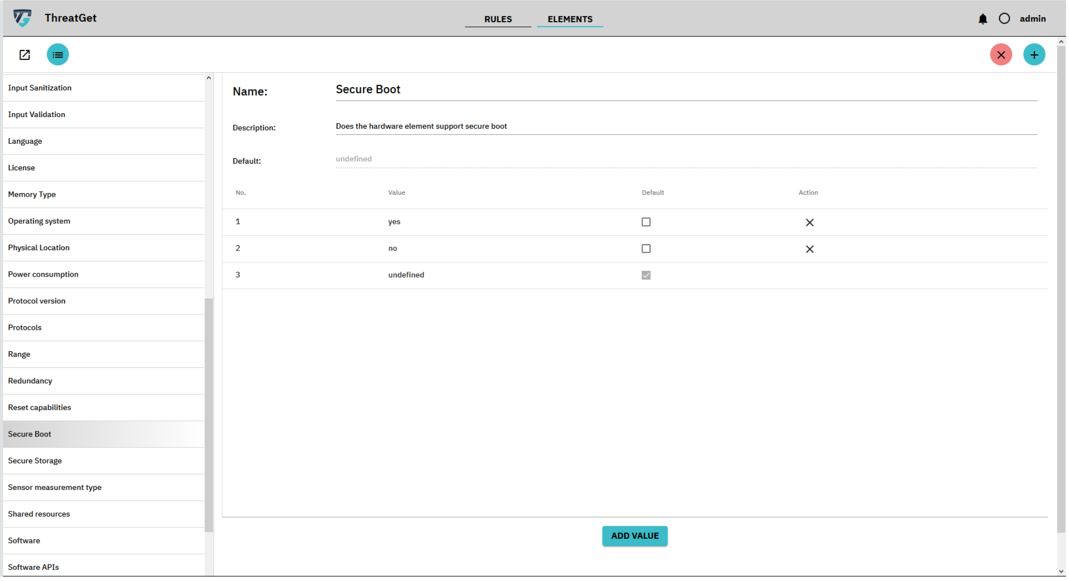
No.	Name	Default	Fixed	Inherited	Actions		
1	Bandwidth	undefined	□		👁	🔧	×
2	Communication Latency	undefined	□		👁	🔧	×
3	Communication Reliability	undefined	□		👁	🔧	×
4	Error Rate	undefined	□		👁	🔧	×
5	Protocol version	Default	□		👁	🔧	×
6	Protocols	undefined	□		👁	🔧	×
7	Range	undefined	□		👁	🔧	×
8	Troughput	undefined	□		👁	🔧	×

AUSTRIAN INSTITUTE OF TECHNOLOGY

SECURITY PROPERTIES

Security Properties

- **Relevant security properties, including assets**
- **Assignable to elements**
- **Customizable**



Name: Secure Boot

Description: Does the hardware element support secure boot

Default: undefined

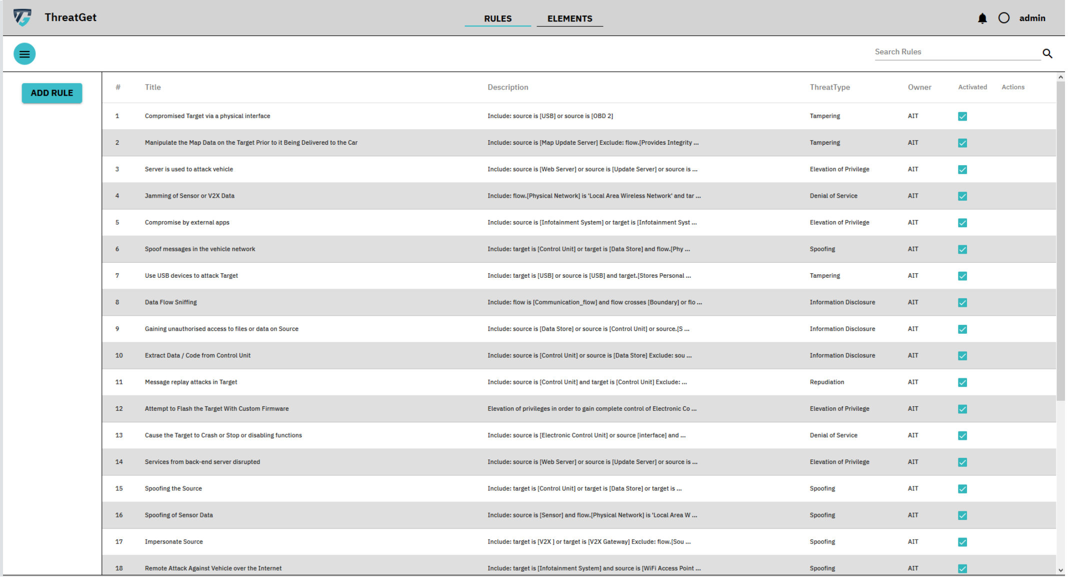
No.	Value	Default	Action
1	yes	□	×
2	no	□	×
3	undefined	☑	

AUSTRIAN INSTITUTE OF TECHNOLOGY

AUTOMATED SECURITY ASSESSMENT

Rule Engine

- Rules describe potential weaknesses
- Multi-hops attack and attack flows
- Risk evaluation based on weakness and assets

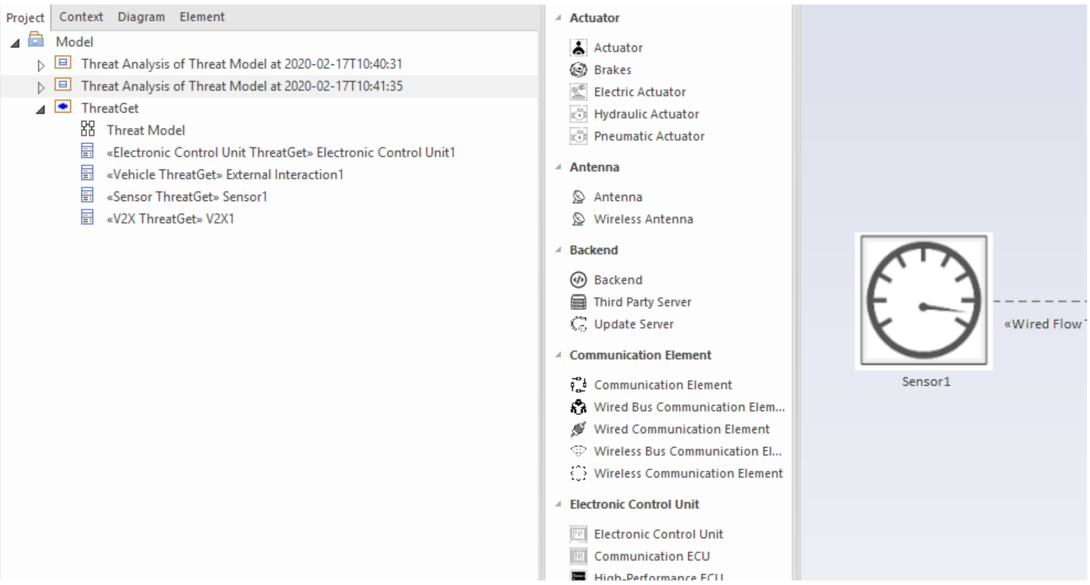


#	Title	Description	ThreatType	Owner	Activated	Actions
1	Compromised Target via a physical interface	Include: source is [USB] or source is [OBD 2]	Tampering	AIT	☑	
2	Manipulate the Map Data on the Target Prior to it Being Delivered to the Car	Include: source is [Map Update Server] Exclude: flow.[Provides Integrity ...	Tampering	AIT	☑	
3	Server is used to attack vehicle	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	☑	
4	Jamming of Sensor or V2X Data	Include: flow.[Physical Network] is 'Local Area Wireless Network' and tar ...	Denial of Service	AIT	☑	
5	Compromise by external apps	Include: source is [Infotainment System] or target is [Infotainment Syst ...	Elevation of Privilege	AIT	☑	
6	Spoof messages in the vehicle network	Include: target is [Control Unit] or target is [Data Store] and flow.[Phy ...	Spoofing	AIT	☑	
7	Use USB devices to attack Target	Include: target is [USB] or source is [USB] and target.[Stores Personal ...	Tampering	AIT	☑	
8	Data Flow Sniffing	Include: flow is [Communication_flow] and flow crosses [Boundary] or flo ...	Information Disclosure	AIT	☑	
9	Gaining unauthorised access to files or data on Source	Include: source is [Data Store] or source is [Control Unit] or source.[S ...	Information Disclosure	AIT	☑	
10	Extract Data / Code from Control Unit	Include: source is [Control Unit] or source is [Data Store] Exclude: sou ...	Information Disclosure	AIT	☑	
11	Message replay attacks in Target	Include: source is [Control Unit] and target is [Control Unit] Exclude: ...	Repudiation	AIT	☑	
12	Attempt to Flash the Target With Custom Firmware	Elevation of privileges in order to gain complete control of Electronic Co ...	Elevation of Privilege	AIT	☑	
13	Cause the Target to Crash or Stop or disabling functions	Include: source is [Electronic Control Unit] or source [interface] and ...	Denial of Service	AIT	☑	
14	Services from back-end server disrupted	Include: source is [Web Server] or source is [Update Server] or source is ...	Elevation of Privilege	AIT	☑	
15	Spoofing the Source	Include: target is [Control Unit] or target is [Data Store] or target is ...	Spoofing	AIT	☑	
16	Spoofing of Sensor Data	Include: source is [Sensor] and flow.[Physical Network] is 'Local Area W ...	Spoofing	AIT	☑	
17	Impersonate Source	Include: target is [V2X] or target is [V2X Gateway] Exclude: flow.[Sou ...	Spoofing	AIT	☑	
18	Remote Attack Against Vehicle over the Internet	Include: target is [Infotainment System] and source is [WiFi Access Point ...	Spoofing	AIT	☑	

VERSIONING

Traceability of Analysis

- **For each analysis a snapshot of the model is generated**
- **Snapshot + analysis reports is marked with date and time**
- **Stored in the model**

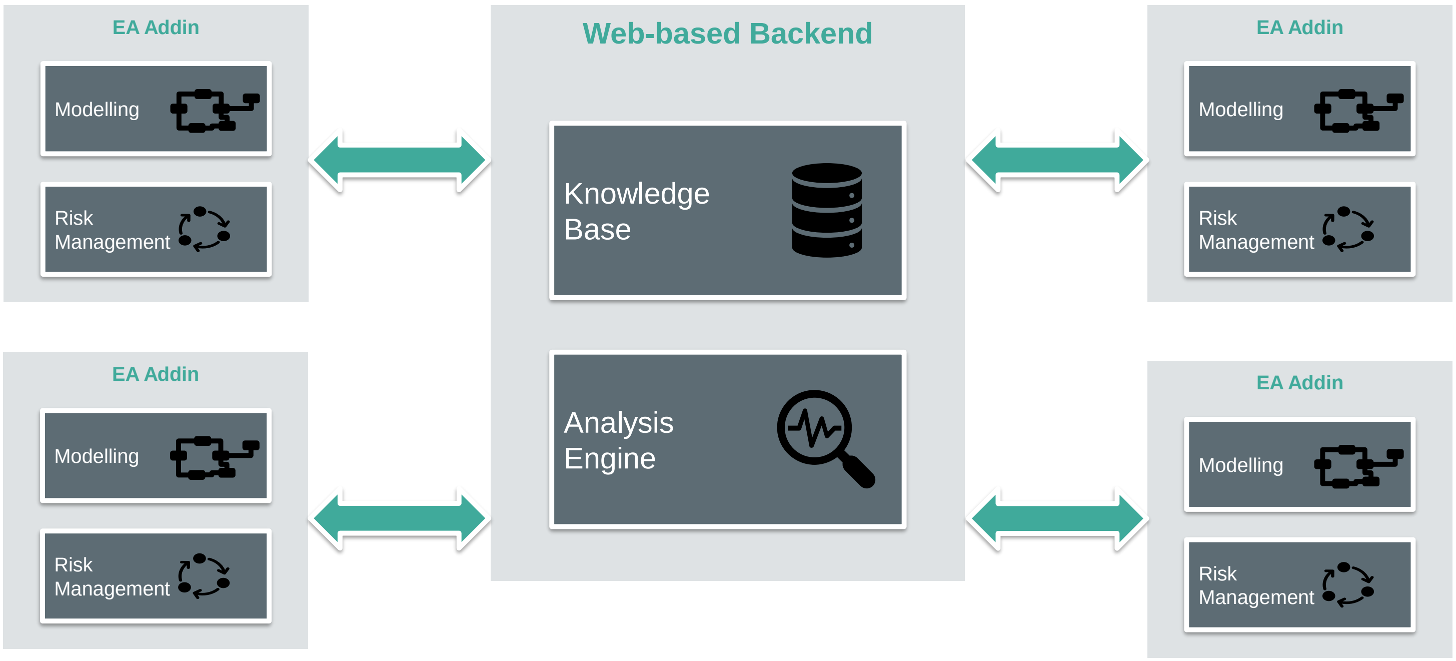


Project Context Diagram Element

- Model
  - Threat Analysis of Threat Model at 2020-02-17T10:40:31
  - Threat Analysis of Threat Model at 2020-02-17T10:41:35
  - ThreatGet
    - Threat Model
    - «Electronic Control Unit ThreatGet» Electronic Control Unit1
    - «Vehicle ThreatGet» External Interaction1
    - «Sensor ThreatGet» Sensor1
    - «V2X ThreatGet» V2X1

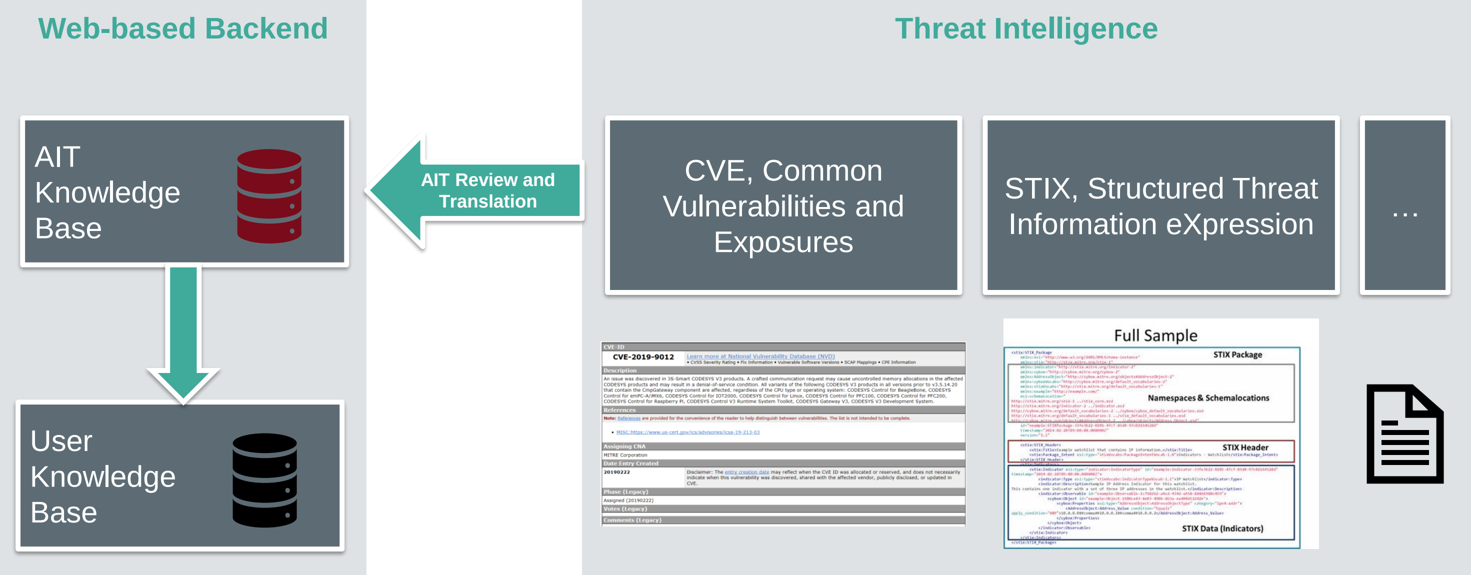
AUSTRIAN INSTITUTE OF TECHNOLOGY

ARCHITECTURE



AUTOMATED THREAT INTELLIGENCE UPDATES

AUSTRIAN INSTITUTE OF TECHNOLOGY

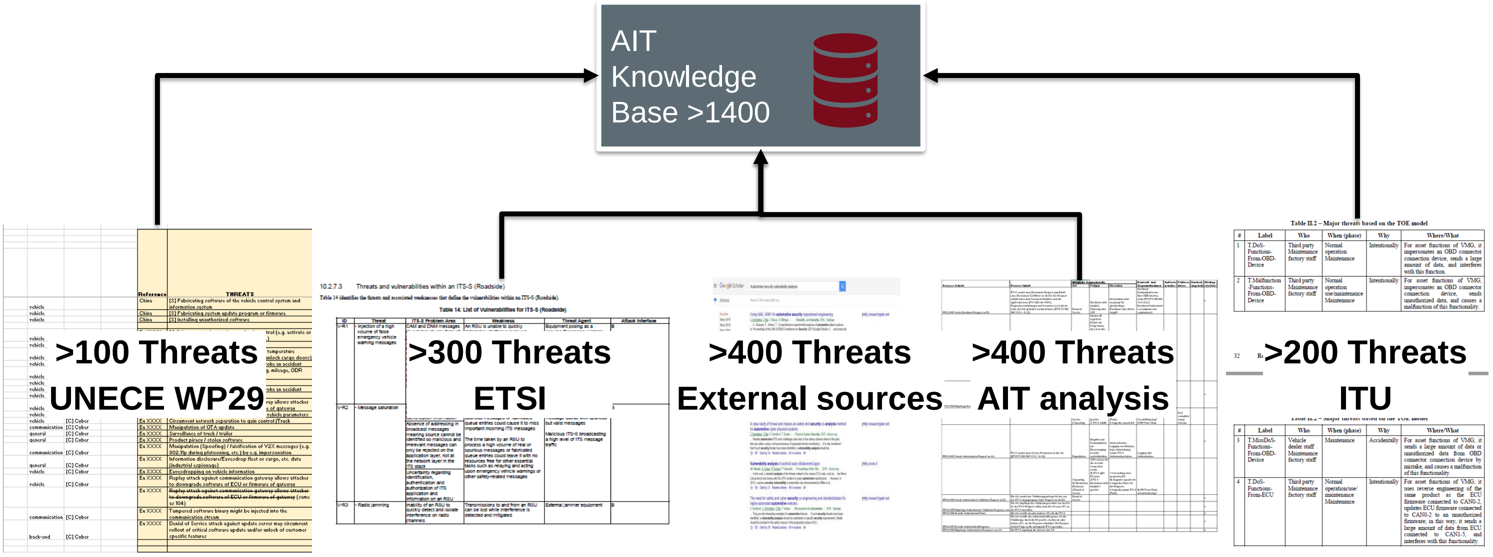

Web-based Backend
AIT Knowledge Base
User Knowledge Base
AIT Review and Translation
Threat Intelligence
CVE, Common Vulnerabilities and Exposures
STIX, Structured Threat Information eXpression
…
Full Sample
STIX Package
Namespaces & Schemalocations
STIX Header
STIX Data (Indicators)

CVE-ID	
CVE-2019-9012	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
An issue was discovered in 3S-Smart CODESYS V3 products. A crafted communication request may cause uncontrolled memory allocations in the affected CODESYS products and may result in a denial-of-service condition. All variants of the following CODESYS V3 products in all versions prior to v3.5.14.20 that contain the CmpGateway component are affected, regardless of the CPU type or operating system: CODESYS Control for BeagleBone, CODESYS Control for emPC-A/iMX6, CODESYS Control for IOT2000, CODESYS Control for Linux, CODESYS Control for PFC100, CODESYS Control for PFC200, CODESYS Control for Raspberry Pi, CODESYS Control V3 Runtime System Toolkit, CODESYS Gateway V3, CODESYS V3 Development System.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete. • MISC:https://www.us-cert.gov/ics/advisories/icsa-19-213-03	
Assigning CNA	
MITRE Corporation	
Date Entry Created	
20190222	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.
Phase (Legacy)	
Assigned (20190222)	
Votes (Legacy)	
Comments (Legacy)	

```
<stix:STIX_Package
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:stix="http://stix.mitre.org/stix-1"
    xmlns:indicator="http://stix.mitre.org/Indicator-2"
    xmlns:cybox="http://cybox.mitre.org/cybox-2"
    xmlns:AddressObject="http://cybox.mitre.org/objects#AddressObject-2"
    xmlns:cyboxVocabs="http://cybox.mitre.org/default_vocabularies-2"
    xmlns:stixVocabs="http://stix.mitre.org/default_vocabularies-1"
    xmlns:example="http://example.com/"
    xsi:schemaLocation="
http://stix.mitre.org/stix-1 ../stix_core.xsd
http://stix.mitre.org/Indicator-2 ../indicator.xsd
http://cybox.mitre.org/default_vocabularies-2 ../cybox/cybox_default_vocabularies.xsd
http://stix.mitre.org/default_vocabularies-1 ../stix_default_vocabularies.xsd
http://cybox.mitre.org/objects#AddressObject-2 ../cybox/objects/Address_Object.xsd"
    id="example:STIXPackage-33fe3b22-0201-47cf-85d0-97c02164528d"
    timestamp="2014-02-20T09:00:00.000000Z"
    version="1.1"
    >
    <stix:STIX_Header>
        <stix:Title>Example watchlist that contains IP information.</stix:Title>
        <stix:Package_Intent xsi:type="stixVocabs:PackageIntentVocab-1.0">Indicators - Watchlist</stix:Package_Intent>
    </stix:STIX_Header>
    <stix:Indicators>
        <stix:Indicator xsi:type="indicator:IndicatorType" id="example:Indicator-33fe3b22-0201-47cf-85d0-97c02164528d"
timestamp="2014-02-20T09:00:00.000000Z">
            <indicator:Type xsi:type="stixVocabs:IndicatorTypeVocab-1.1">IP Watchlist</indicator:Type>
            <indicator:Description>Sample IP Address Indicator for this watchlist.
This contains one indicator with a set of three IP addresses in the watchlist.</indicator:Description>
            <indicator:Observable id="example:Observable-1c798262-a4cd-434d-a958-884d6980c459">
                <cybox:Object id="example:Object-1980ce43-8e03-490b-863a-ea404d12242e">
                    <cybox:Properties xsi:type="AddressObject:AddressObjectType" category="ipv4-addr">
                        <AddressObject:Address_Value condition="Equals"
apply_condition="ANY">10.0.0.0##comma##10.0.0.1##comma##10.0.0.2</AddressObject:Address_Value>
                    </cybox:Properties>
                </cybox:Object>
            </indicator:Observable>
        </stix:Indicator>
    </stix:Indicators>
</stix:STIX_Package>
```

THREAT INTELLIGENCE – AUTOMOTIVE EXAMPLE

AUSTRIAN INSTITUTE OF TECHNOLOGY



AIT Knowledge Base >1400

>100 Threats UNECE WP29

>300 Threats ETSI

>400 Threats External sources

>400 Threats AIT analysis

>200 Threats ITU

UNECE WP29: World Forum for Harmonization of Vehicle Regulations

ETSI: European Telecommunications Standards Institute (V2X in Europe)

ITU: International Telecommunication Union

AUSTRIAN INSTITUTE OF TECHNOLOGY

THREATGET - AWARDS

Winner eAward 2020 in the categorie Industrie 4.0

Participation as Austrian contribution in iLAB at EXPO 2020

https://www.threatget.com/

67

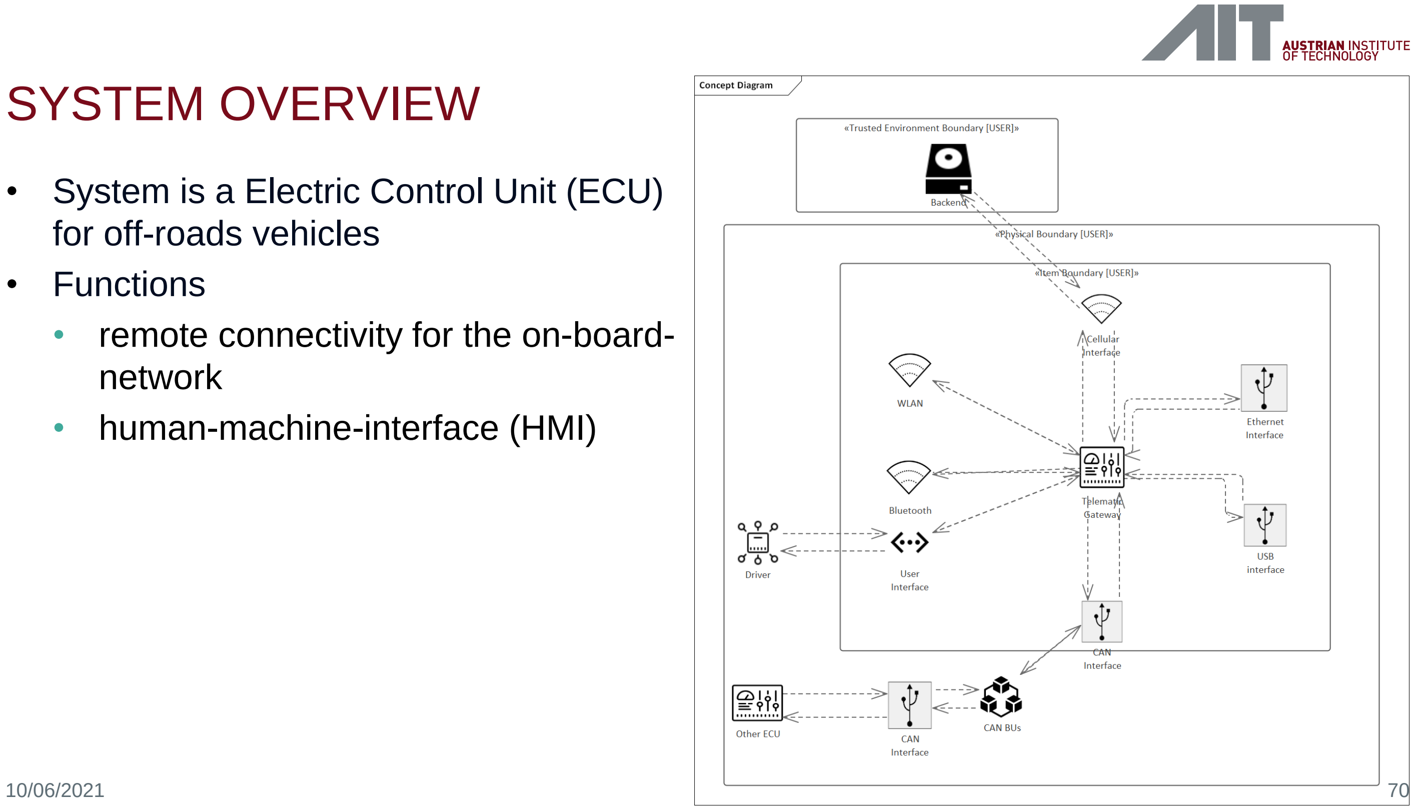
AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

TOMORROW TODAY

SMART FARMING – SECURITY ENGINEERING EXAMPLE

Communication Gateway and Human-Machine Interface for agricultural vehicles

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 783221. The JU receives support from the European Union’s Horizon 2020 research and innovation programme and Austria, Belgium, Czech Republic, Finland, Germany, Greece, Italy, Latvia, Norway, Poland, Portugal, Spain, Sweden.



AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW

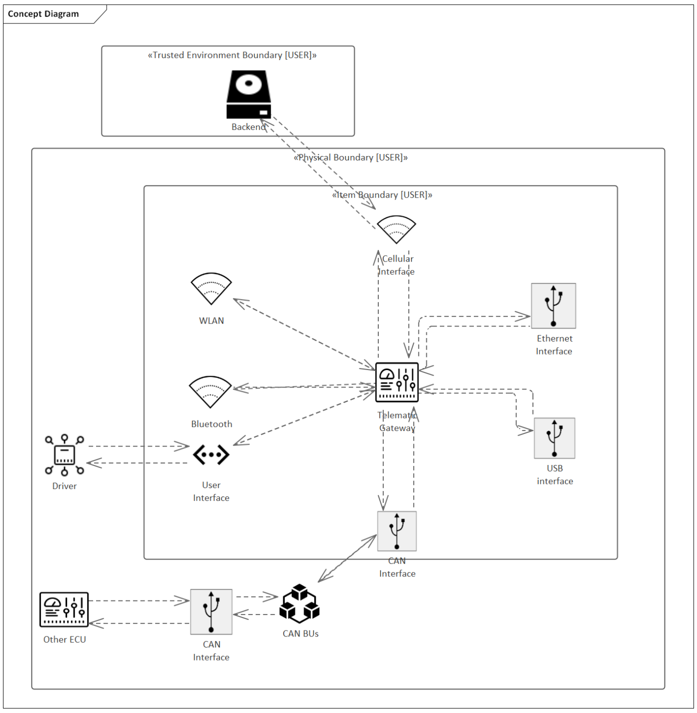
- System is a Electric Control Unit (ECU) for off-roads vehicles
- Functions
  - remote connectivity for the on-board-network
  - human-machine-interface (HMI)

10/06/2021

70

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW

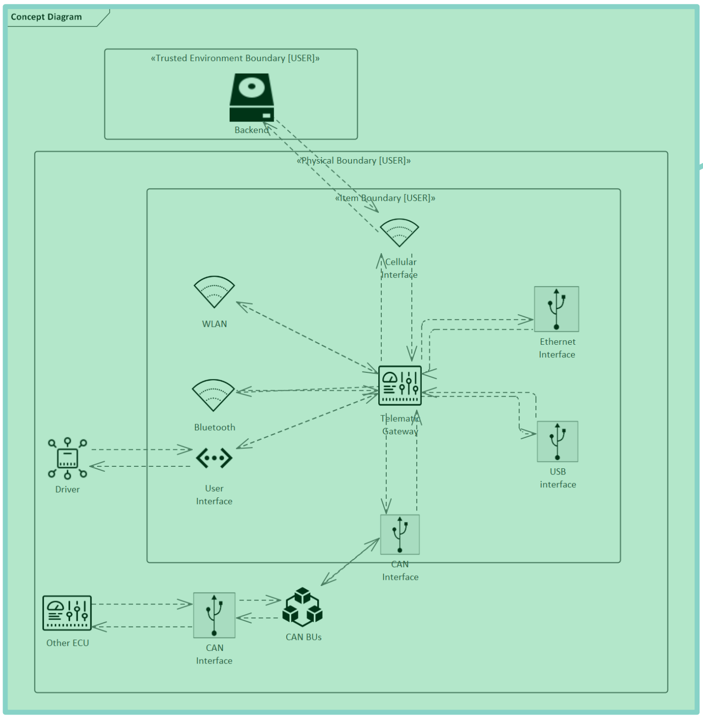


10/06/2021

71

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW

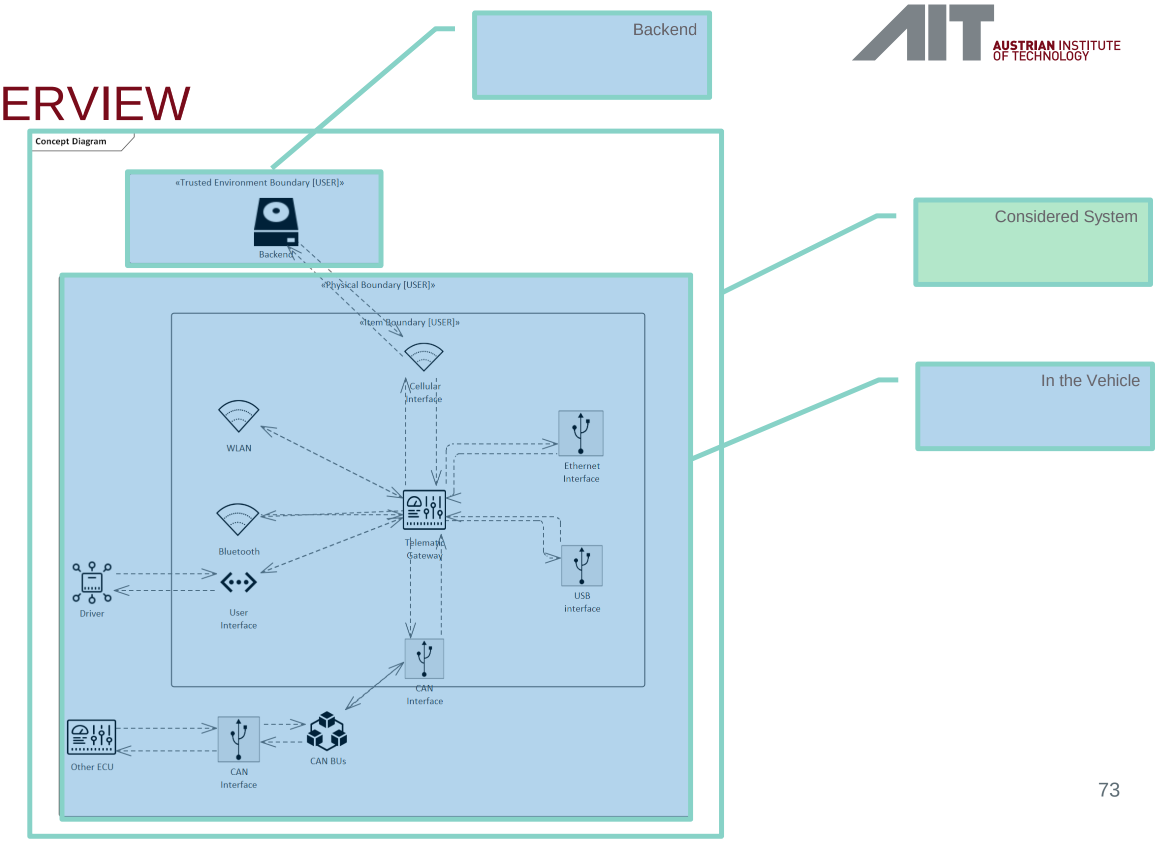


Considered System

10/06/2021

72

SYSTEM OVERVIEW

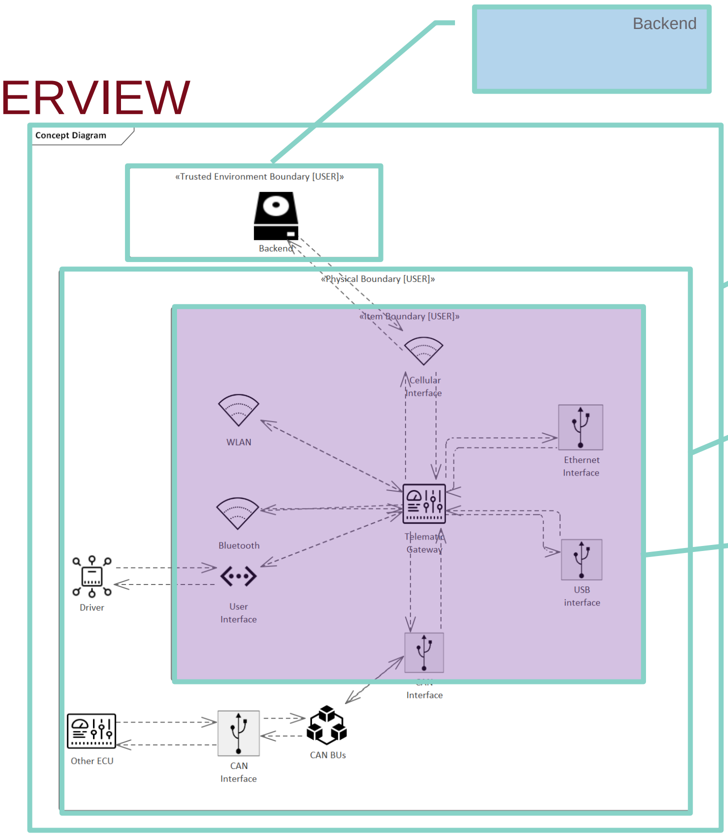


10/06/2021

73

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW



Considered System

In the Vehicle

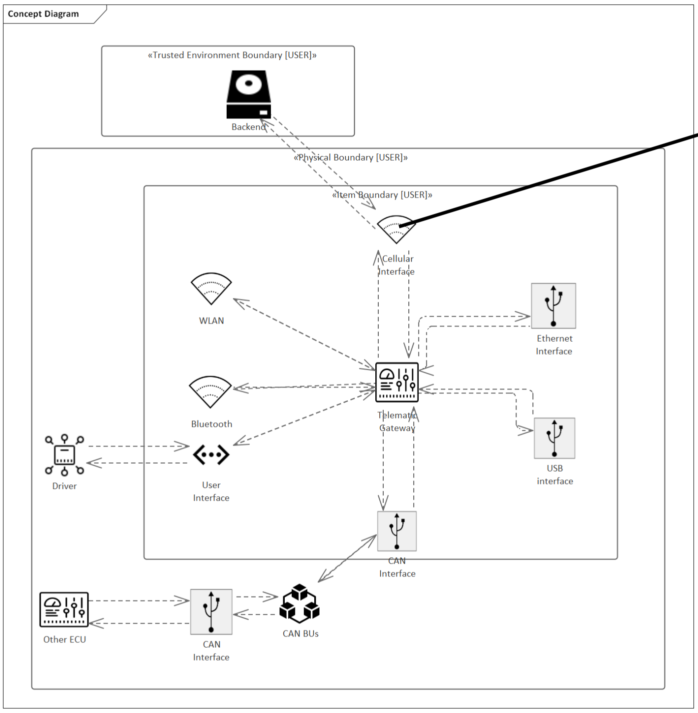
Item, what we are developing

10/06/2021

74

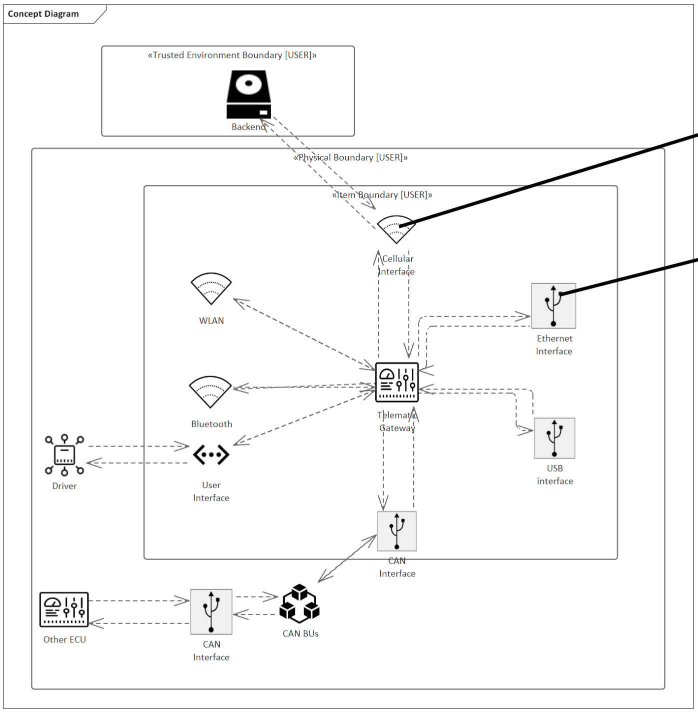
AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

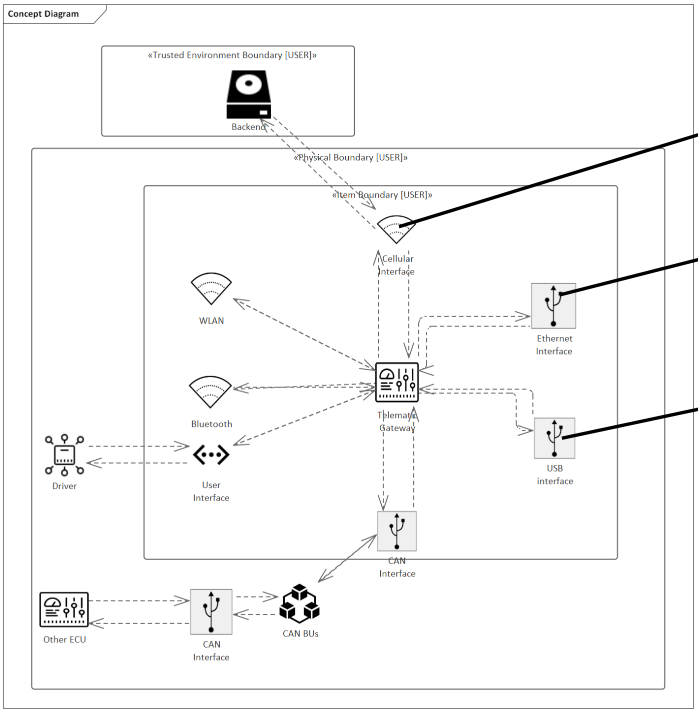
Ethernet for development and programming and for future-proofing (automotive Ethernet)

10/06/2021

76

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

Ethernet for development and programming and for future-proofing (automotive Ethernet)

Physically protected USB interface for OEM programming and updates in the field

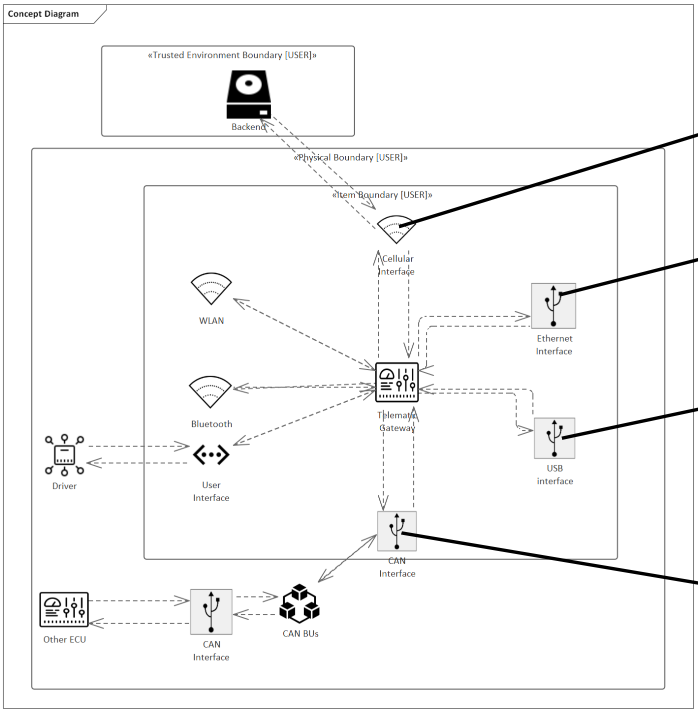
10/06/2021

77

©MECO.net

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

Ethernet for development and programming and for future-proofing (automotive Ethernet)

Physically protected USB interface for OEM programming and updates in the field

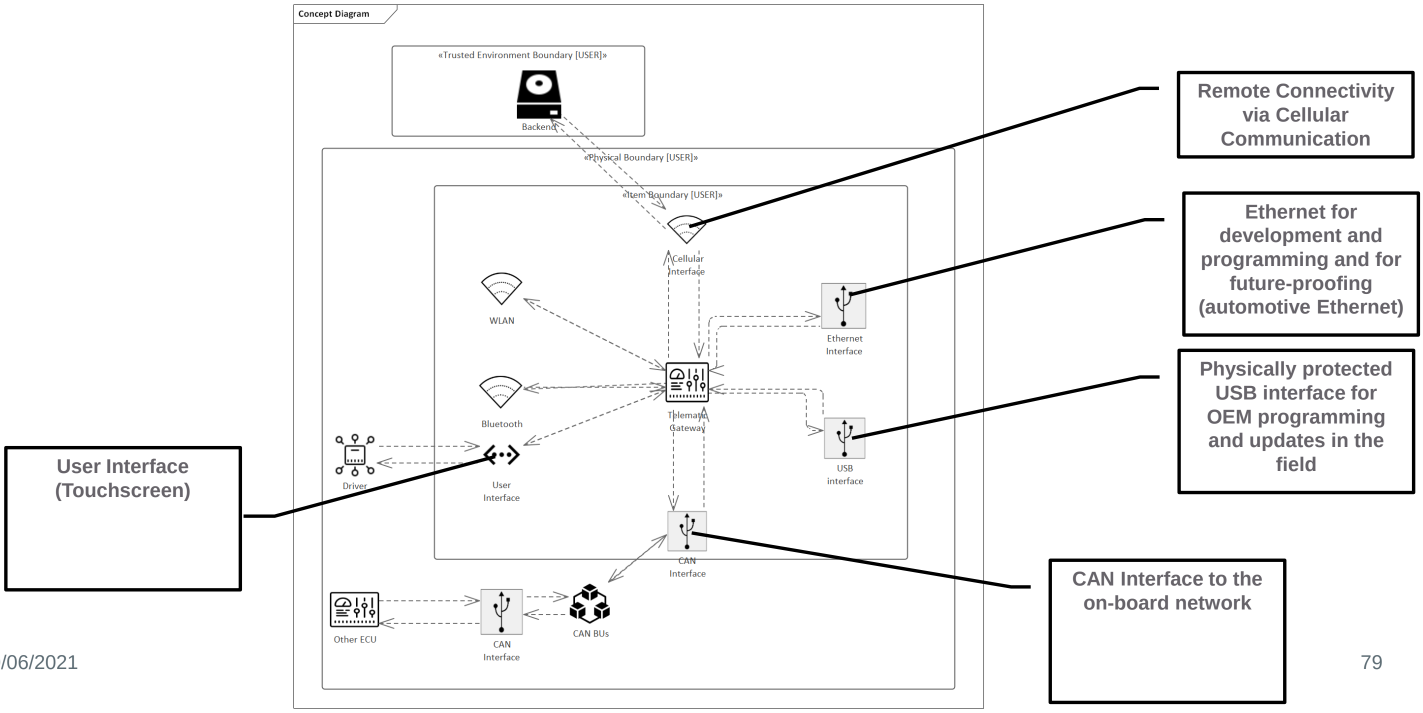
CAN Interface to the on-board network

10/06/2021

78

©MECO.net

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

Ethernet for development and programming and for future-proofing (automotive Ethernet)

Physically protected USB interface for OEM programming and updates in the field

User Interface (Touchscreen)

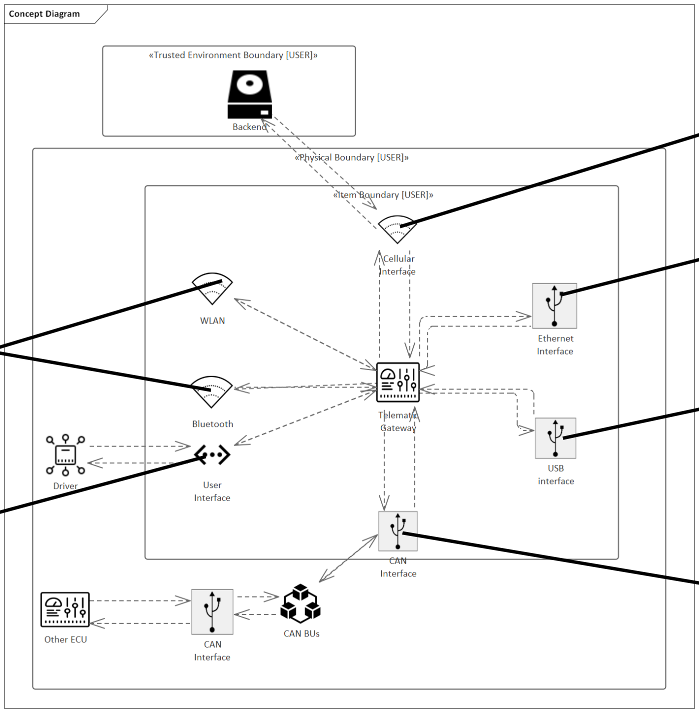
CAN Interface to the on-board network

10/06/2021

79

AUSTRIAN INSTITUTE OF TECHNOLOGY

SYSTEM OVERVIEW



Remote Connectivity via Cellular Communication

Ethernet for development and programming and for future-proofing (automotive Ethernet)

Physically protected USB interface for OEM programming and updates in the field

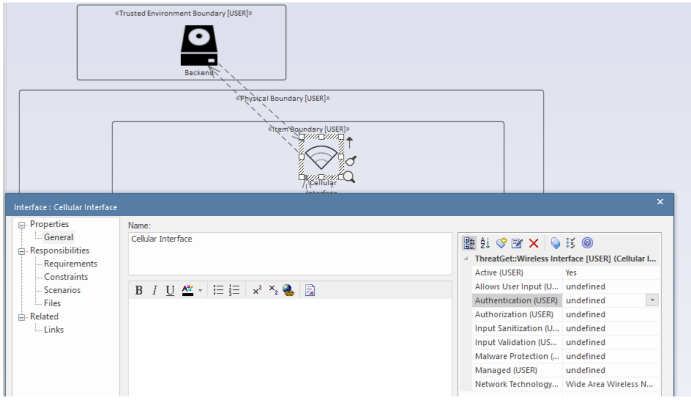
CAN Interface to the on-board network

WLAN and Bluetooth Interface for local connectivity

User Interface (Touchscreen)

10/06/2021

SYSTEM PROPERTIES



Interface : Cellular Interface

Name: Cellular Interface

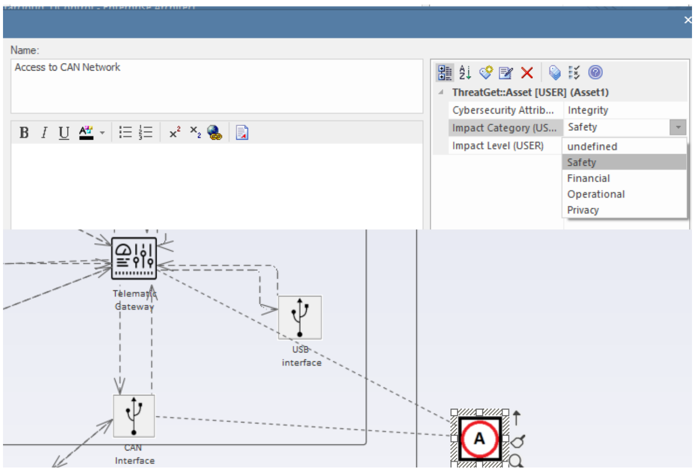
ThreatGet::Wireless Interface [USER] (Cellular I...

Active (USER)	Yes
Allows User Input (U...	undefined
Authentication (USER)	undefined
Authorization (USER)	undefined
Input Sanitization (U...	undefined
Input Validation (US...	undefined
Malware Protection (...	undefined
Managed (USER)	undefined
Network Technology...	Wide Area Wireless N...

- All Elements can be configured to denote:
  - Security related System Properties
  - Existing Security Controls

ASSET DEFINITION

- Process based on brainstorming or pre-existing knowledge
  - What are valuable elements in the system
  - Different viewpoints
    - User
      - Access to CAN Network due to potential of Safety Impact
    - Customer
    - Producer



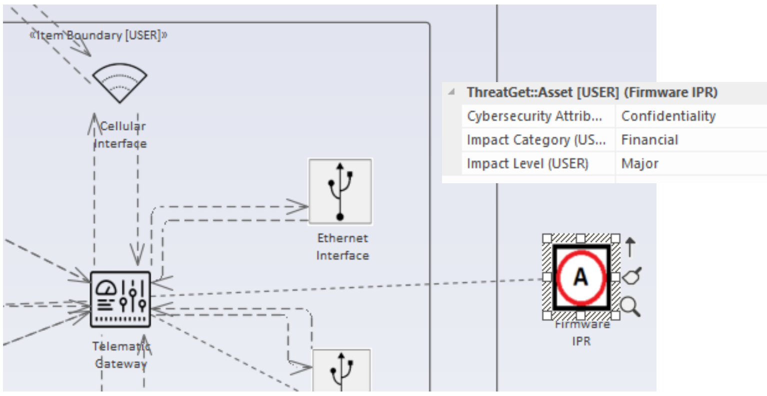
Name:
Access to CAN Network

ThreatGet::Asset [USER] (Asset1)

Cybersecurity Attrib...	Integrity
Impact Category (US...	Safety
Impact Level (USER)	

ASSET DEFINITION

- Process based on brainstorming or pre-existing knowledge
  - What are valuable elements in the system
  - Different viewpoints
    - User
      - Access to CAN Network due to potential of Safety Impact
    - Customer
    - Producer
      - Confidentiality of IPR of Firmware due to potential Financial Impact



ThreatGet::Asset [USER] (Firmware IPR)

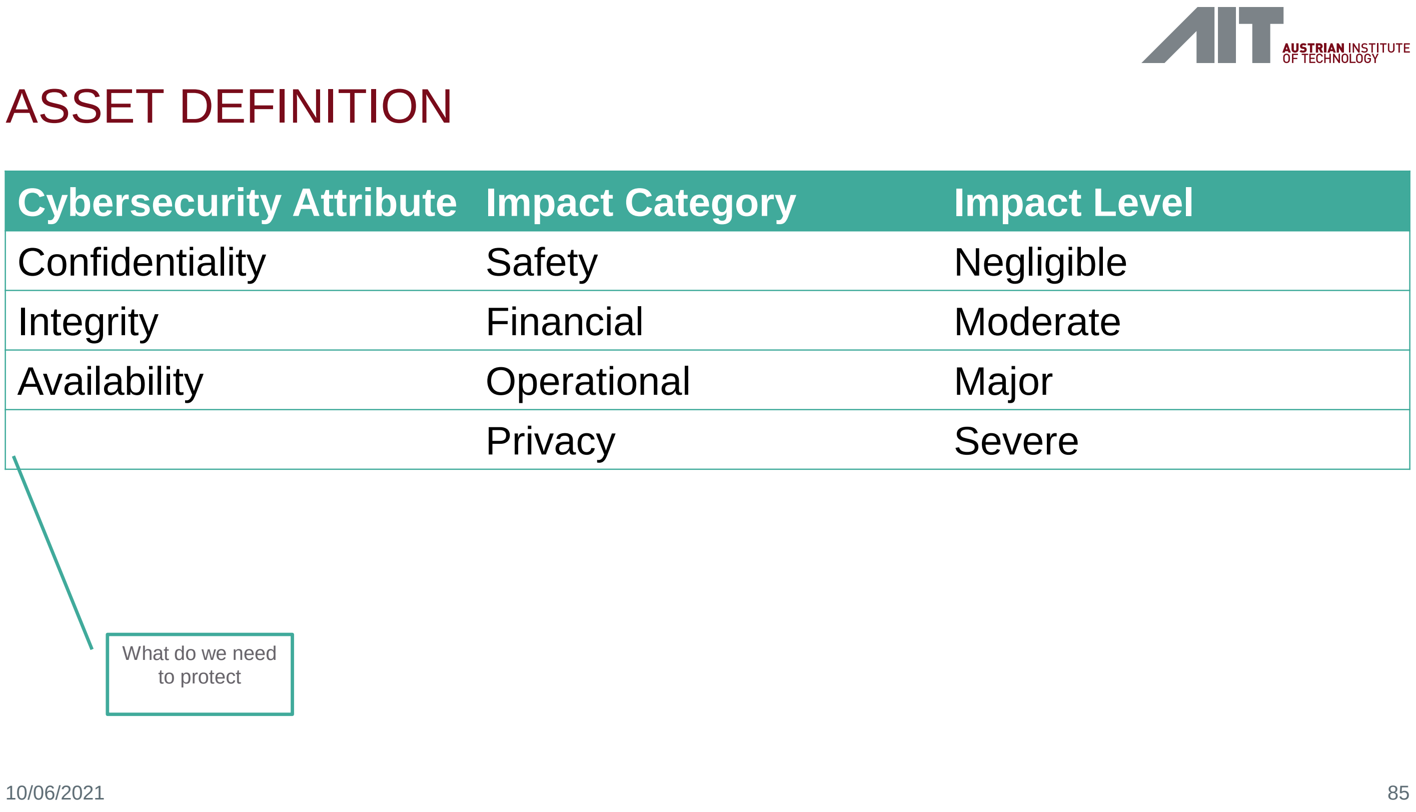
Cybersecurity Attrib...	Confidentiality
Impact Category (US...	Financial
Impact Level (USER)	Major

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

ASSET DEFINITION

Cybersecurity Attribute	Impact Category	Impact Level
Confidentiality	Safety	Negligible
Integrity	Financial	Moderate
Availability	Operational	Major
	Privacy	Severe

10/06/2021 84



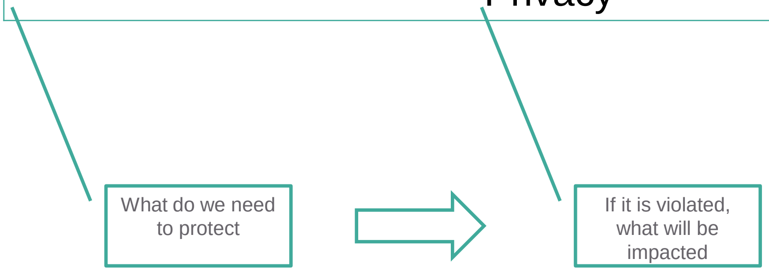
ASSET DEFINITION

Cybersecurity Attribute	Impact Category	Impact Level
Confidentiality	Safety	Negligible
Integrity	Financial	Moderate
Availability	Operational	Major
	Privacy	Severe

What do we need to protect

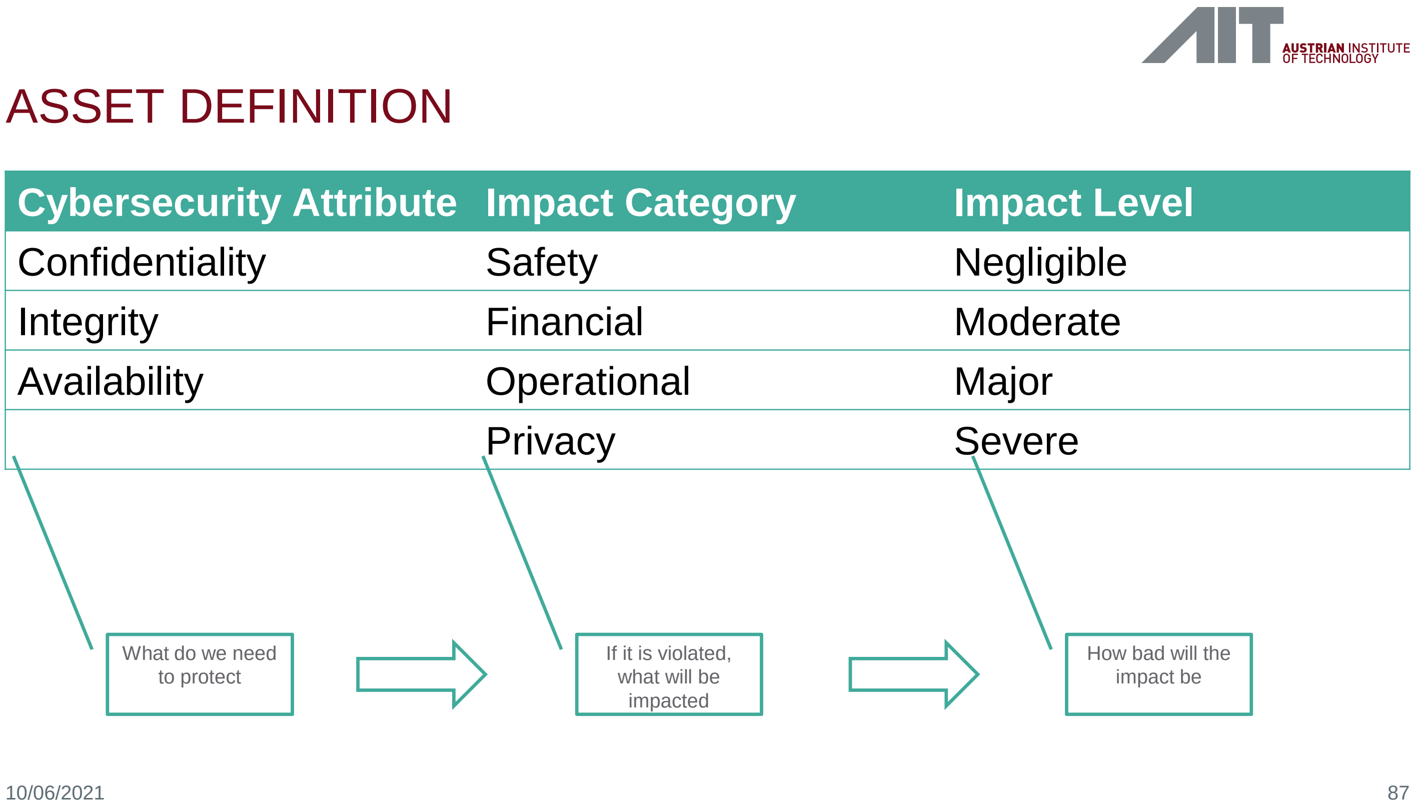
ASSET DEFINITION

Cybersecurity Attribute	Impact Category	Impact Level
Confidentiality	Safety	Negligible
Integrity	Financial	Moderate
Availability	Operational	Major
	Privacy	Severe



What do we need to protect

If it is violated, what will be impacted



ASSET DEFINITION

Cybersecurity Attribute	Impact Category	Impact Level
Confidentiality	Safety	Negligible
Integrity	Financial	Moderate
Availability	Operational	Major
	Privacy	Severe

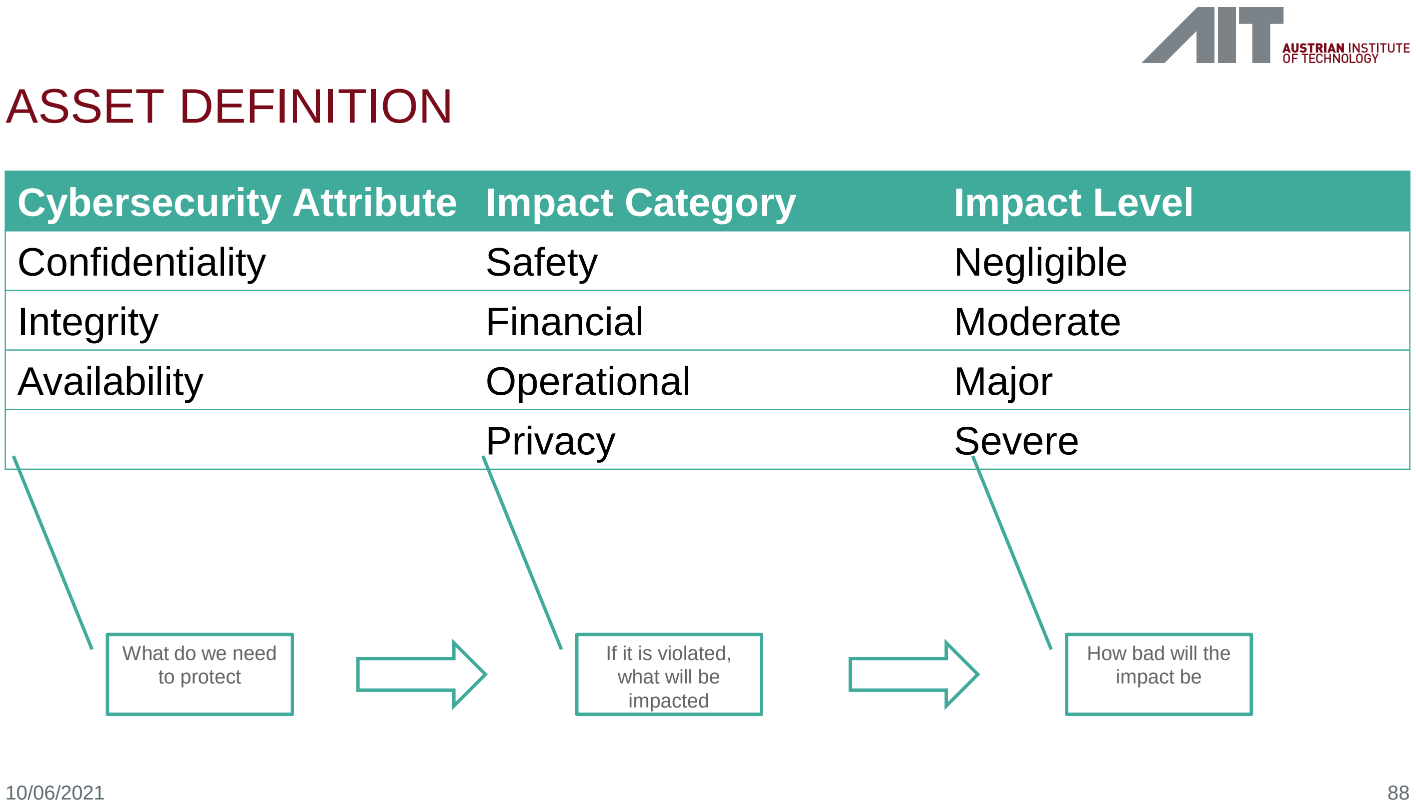
What do we need to protect

If it is violated, what will be impacted

How bad will the impact be

10/06/2021

87



ASSET DEFINITION

Cybersecurity Attribute	Impact Category	Impact Level
Confidentiality	Safety	Negligible
Integrity	Financial	Moderate
Availability	Operational	Major
	Privacy	Severe

What do we need to protect

If it is violated, what will be impacted

How bad will the impact be

10/06/2021

88

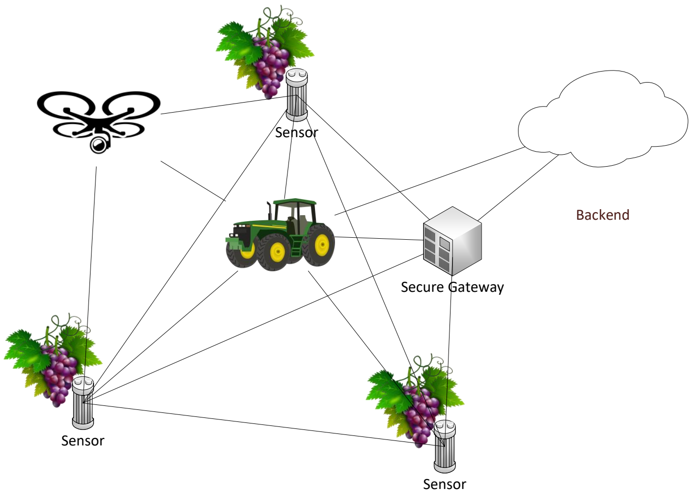
LIVE DEMO

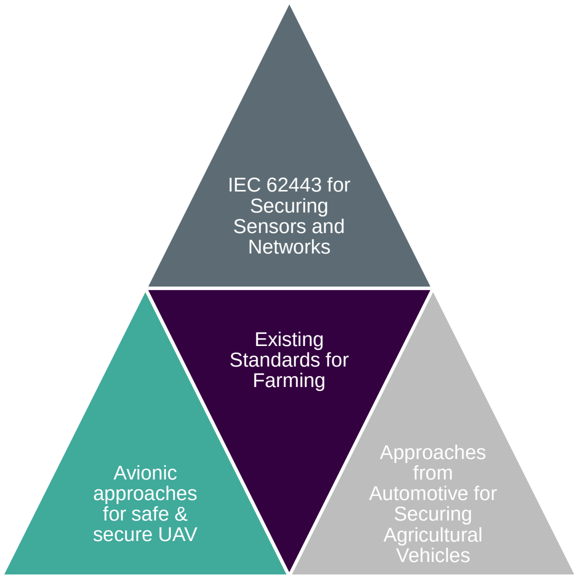
- (If it works)

AUSTRIAN INSTITUTE OF TECHNOLOGY

SAFETY & SECURITY FRAMEWORK

- **Reliable** and **safe** food supply depends on **trustworthy systems**




IEC 62443 for Securing Sensors and Networks
Existing Standards for Farming
Avionic approaches for safe & secure UAV
Approaches from Automotive for Securing Agricultural Vehicles

10/06/2021

90

AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

SUMMARY

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY

SUMMARY

- Security is still a novel topic for many domains
- Standards are existing, but practical experience, methods and processes are missing
- Topic is important due to upcoming regulations
- First tools for embedded system / CPS / IoT are in development

10/06/2021

92

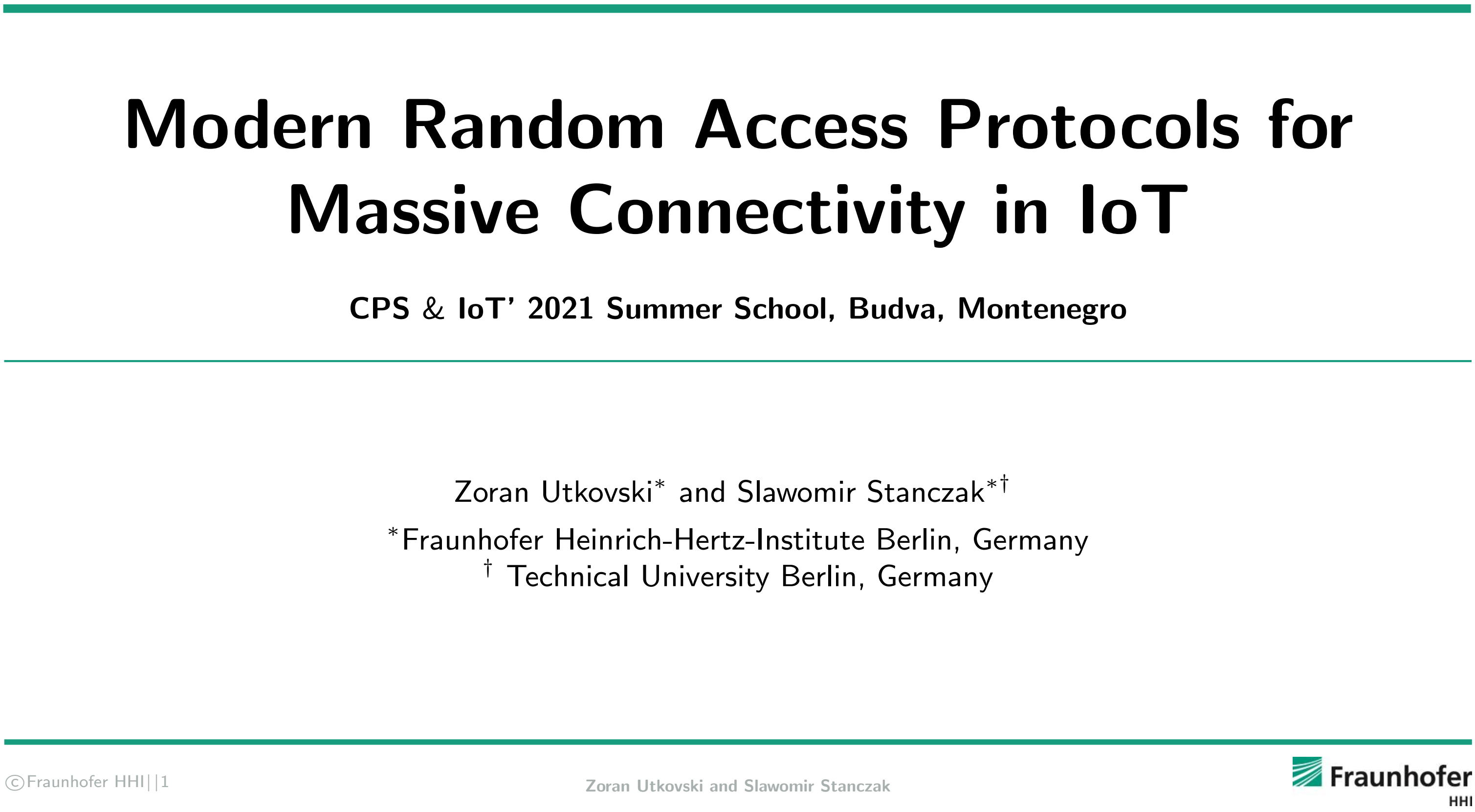
AUSTRIAN INSTITUTE OF TECHNOLOGY
TOMORROW TODAY

THANK YOU!

Christoph Schmittner

Charlie Ciso
I need one brave volunteer to go take a new security training course.
Me!!
Pick Me!
Ooooh!!
I'LL Go!!!
Over here!!
Its kind of disorienting when security training is actually better than work.

Image credit: tag-cyber (https://www.tag-cyber.com/media/charlie-ciso)



Modern Random Access Protocols for Massive Connectivity in IoT

CPS & IoT' 2021 Summer School, Budva, Montenegro

Zoran Utkovski* and Slawomir Stanczak*†

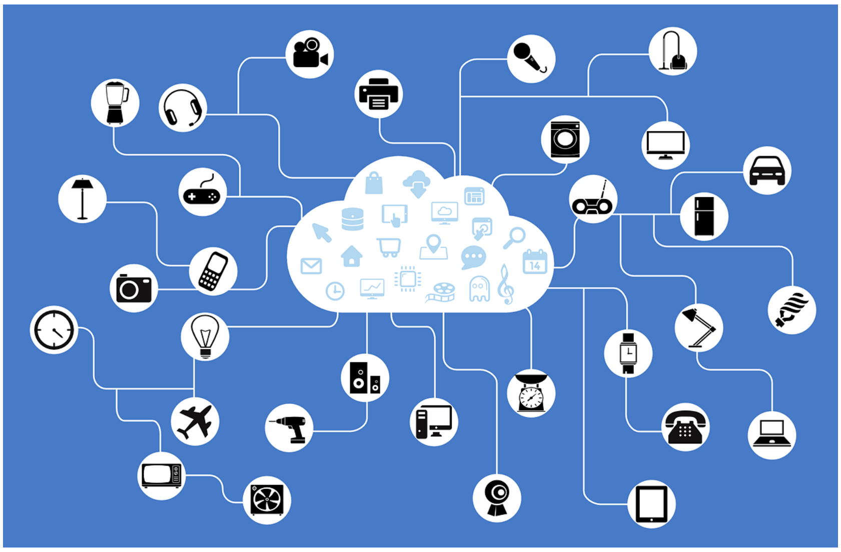
*Fraunhofer Heinrich-Hertz-Institute Berlin, Germany
† Technical University Berlin, Germany

Outline

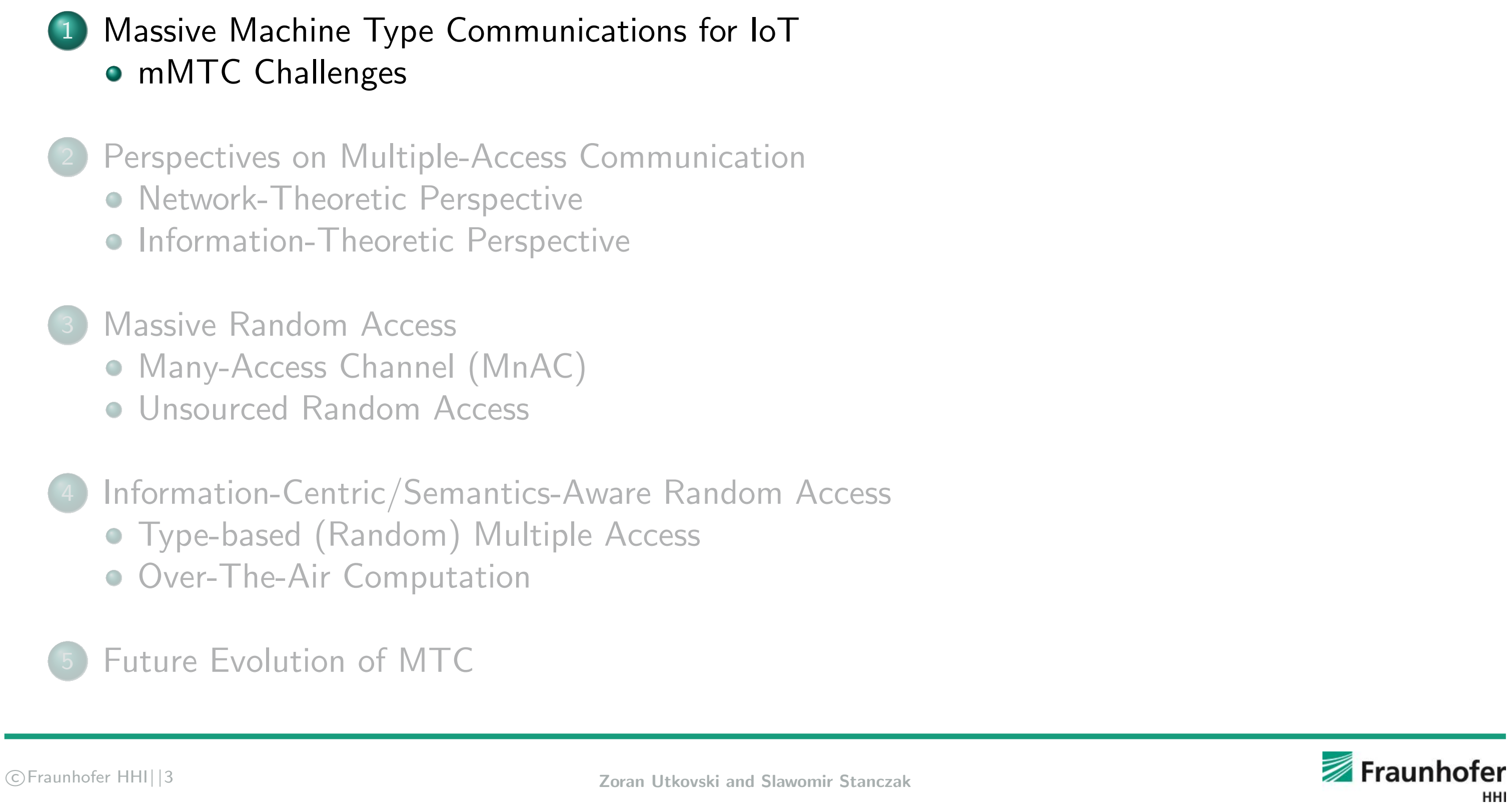
1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

1. Massive Machine Type Communications for IoT
2. Perspectives on Multiple-Access Communication
3. Massive Random Access
4. Information-Centric/Semantics-Aware Random Access
5. Future Evolution of MTC

Massive MTC as a key IoT enabler



Anything that can be connected will be connected



1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

©Fraunhofer HHI||3

Zoran Utkovski and Slawomir Stanczak

Requirements for mMTC

- 10-15 years device battery life
- Extended coverage
- 300000 connected devices per cell
  - New Radio (NR) goes to 1 000 000 devices/km2
- Low complexity
- Efficient transmission of sporadic small payloads
- Per-packet reliability relatively low, but
  - some stringent reliability constraint over an extended period
  - joint reliability requirements put to a group of IoT devices

mMTC Challenges

- mMTC systems are typically characterized by:
  - small payloads
  - uncoordinated access, possibly with grant-less or grant-free data transmission
  - sparse user activity, with number of active users possibly exceeding the overall message blocklength
  - correlated event-driven transmissions
  - fusion-based decoding, whereby functions of multiple IoT sensors' measurements, rather than individual measurements, are of interest to the receiver.
- "Conventional" Multiple Access Communication Models should be revisited!

1 Massive Machine Type Communications for IoT

2 Perspectives on Multiple-Access Communication

3 Massive Random Access

4 Information-Centric/Semantics-Aware Random Access

5 Future Evolution of MTC

Multiple-Access Communication

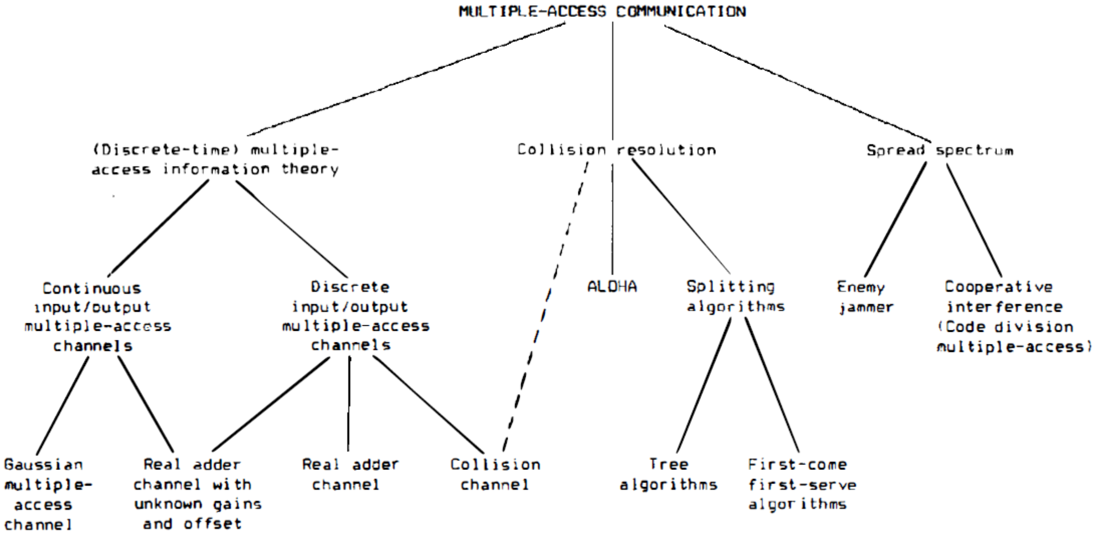
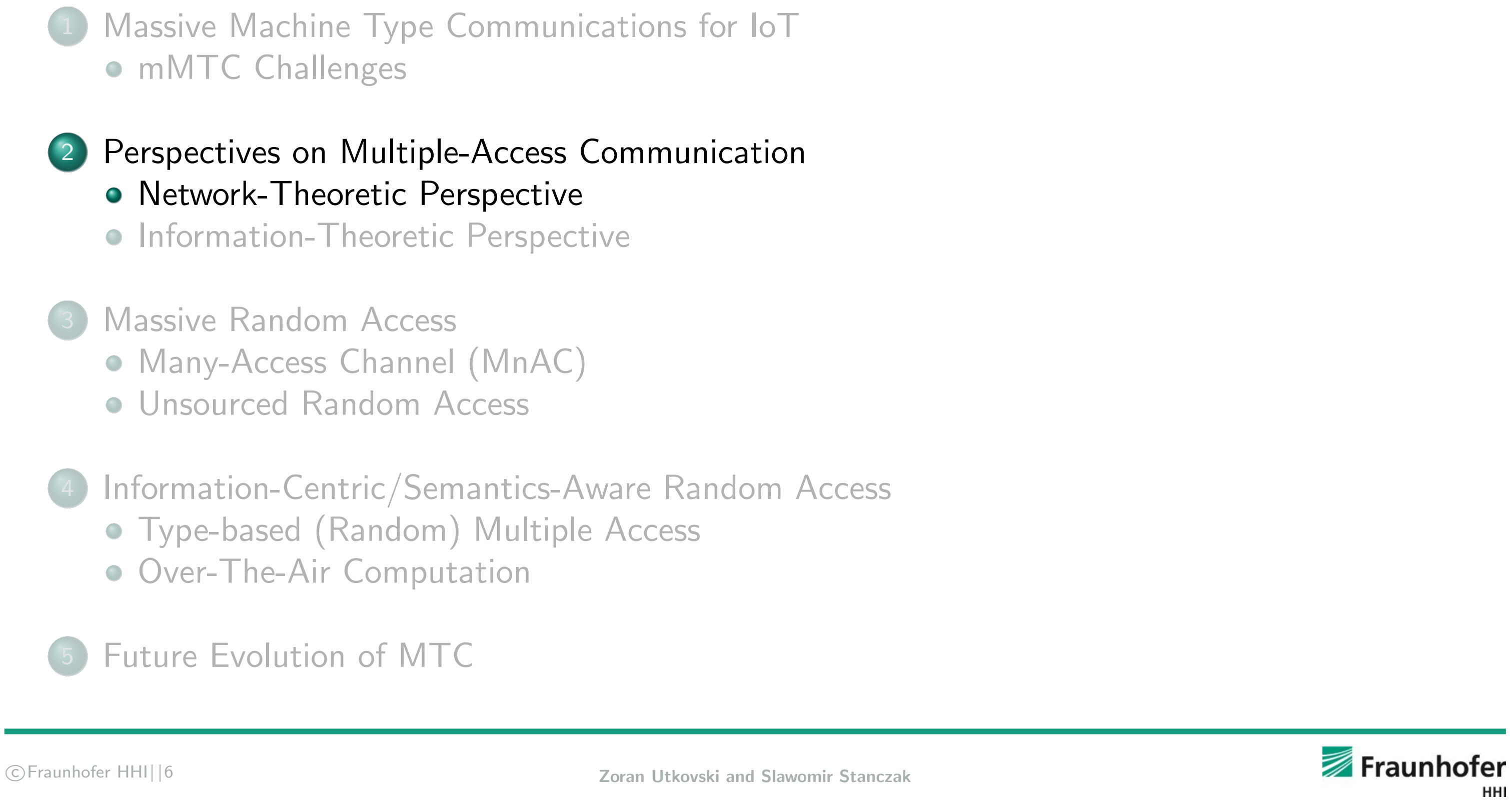

MULTIPLE-ACCESS COMMUNICATION
(Discrete-time) multiple-access information theory
Collision resolution
Spread spectrum
Continuous input/output multiple-access channels
Discrete input/output multiple-access channels
ALOHA
Splitting algorithms
Enemy jammer
Cooperative interference (Code division multiple-access)
Gaussian multiple-access channel
Real adder channel with unknown gains and offset
Real adder channel
Collision channel
Tree algorithms
First-come first-serve algorithms

Figure: Classification of Multiple-Access Communication Schemes. Source: [Mathys1990].



1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

ALOHA

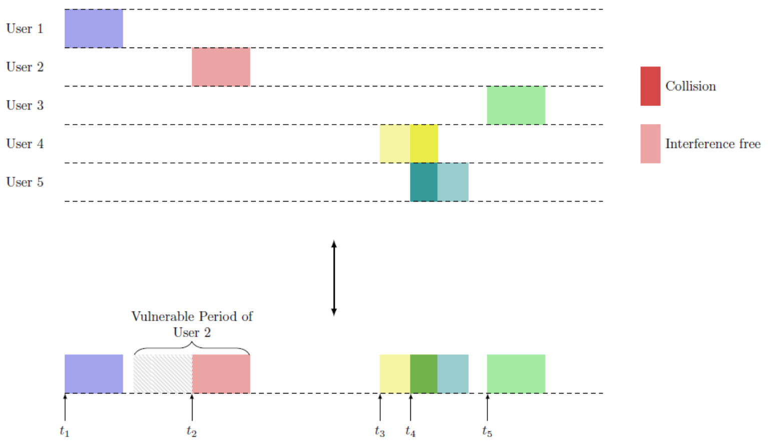


Figure: Depiction of the ALOHA protocol. Source: [Clazzer2017].

- In ALOHA packets are transmitted immediately upon generation in an uncoordinated fashion.
- Vulnerable period: time interval in which any other transmission causes a collision.

ALOHA/Slotted ALOHA

- Poisson process with intensity G for the transmission of packets from the entire population
- G is the channel load,i.e. the expected number of transmissions per packet duration
- Throughput ALOHA

$$S_A(G) = G \cdot e^{-2G}$$

- **Slotted ALOHA**: Time slots are introduced, resulted in halving of the vulnerable period
- Throughput Slotted ALOHA

$$S_{SA}(G) = G \cdot e^{-G}$$

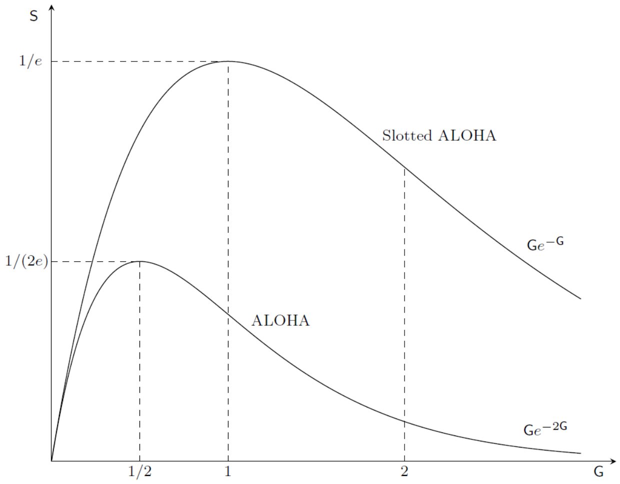


Figure: Throughput of ALOHA/Slotted ALOHA. Source: [Clazzer2017].

Contention Resolution Diversity Slotted ALOHA (CRDSA)

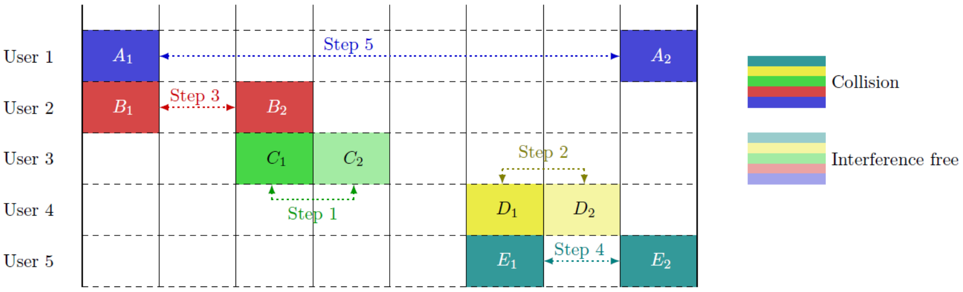
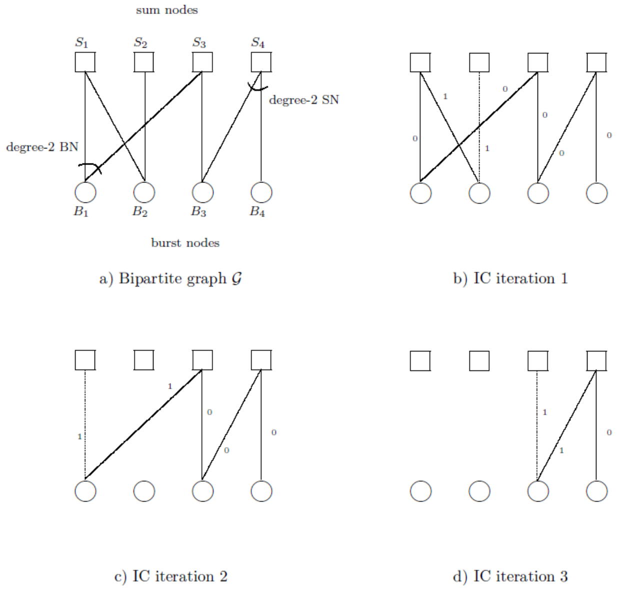


Figure: CRDSA with Interference Cancellation. Source: [Clazzer2017].

- *m* users share a group of *n* time slots (a frame)
- Each user transmits *d* replicas of the packet (the *d* slots are selected uniformly at random)
- Each replica contains information (pointer) for localizing all the *d* replicas
- Interference Cancellation (IC) is performed at the receiver

Irregular Repetition Slotted ALOHA (IRSA)

- The frame status can be represented by a bipartite graph $\mathcal{G}(B, S, E)$
  - set B of m variable nodes corresponding to packets (bursts) from the users
  - set S of n factor nodes corresponding to the slots in the frame
  - set E of edges corresponding to packet (burst) replicas
- CRDSA leads to regular graphs (constant node degree)
- Irregular Repetition Slotted ALOHA (IRSA) (variable node degree)
- IC: nessage-passing along the graph edges



a) Bipartite graph $\mathcal{G}$

b) IC iteration 1

c) IC iteration 2

d) IC iteration 3

Figure: Graph representation of the IC iterative process. Source: [Liva2011].

Performance of IRSA

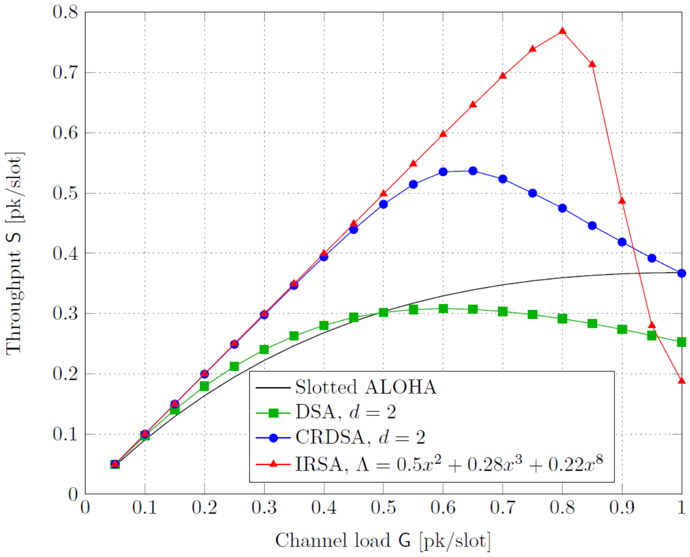
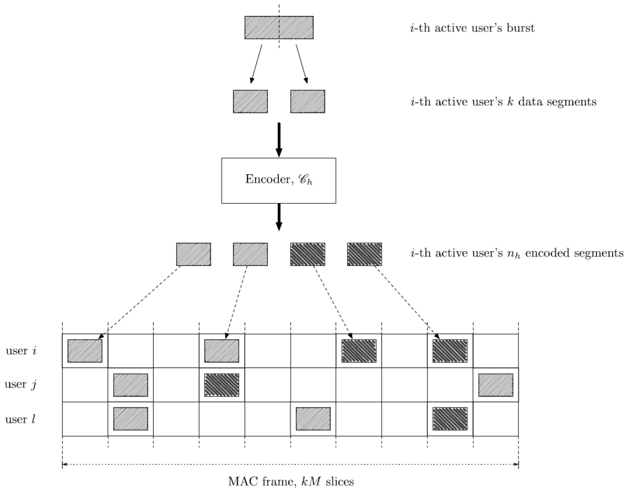


Figure: Performance comparison of SA, DSA, CRDSA and IRSA. Source: [Liva2011].

Coded Slotted ALOHA



i-th active user's burst
i-th active user's k data segments
Encoder, $\mathscr{C}_h$
i-th active user's n_h encoded segments
user i
user j
user l
MAC frame, kM slices

Figure: Graph representation of the IC iterative process. Source: [Liva2011].

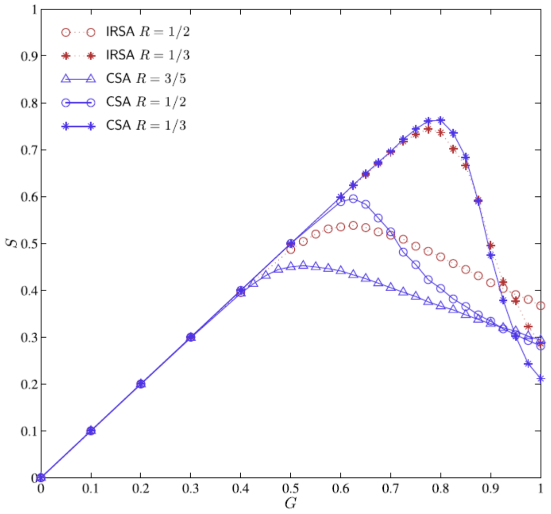


Figure: Graph representation of the IC iterative process. Source: [Liva2011].

1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

K-User MAC

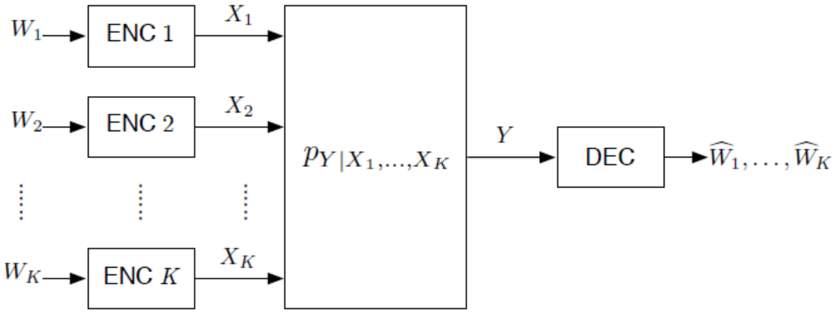


Figure: Block-diagram of a Multiple Access Channel (MAC)

- $W_1, \ldots, W_K$ independent messages (each of which is only accessible by one encoder).
- Rate tuple: $(R_1, \ldots, R_K)$.

2-User MAC

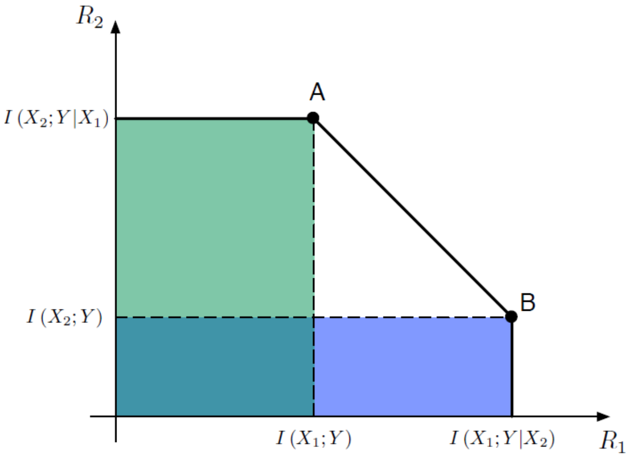


Figure: 2-user MAC: Achievable rate region with successive interference cancellation.

- SIC with decoding order $W_1 \to W_2$ achieves A (the green region).
- SIC with decoding order $W_2 \to W_1$ achieves B (the blue region).
- With time sharing, all other rate pairs inside the inner bound region can be achieved.

2-User Gaussian MAC

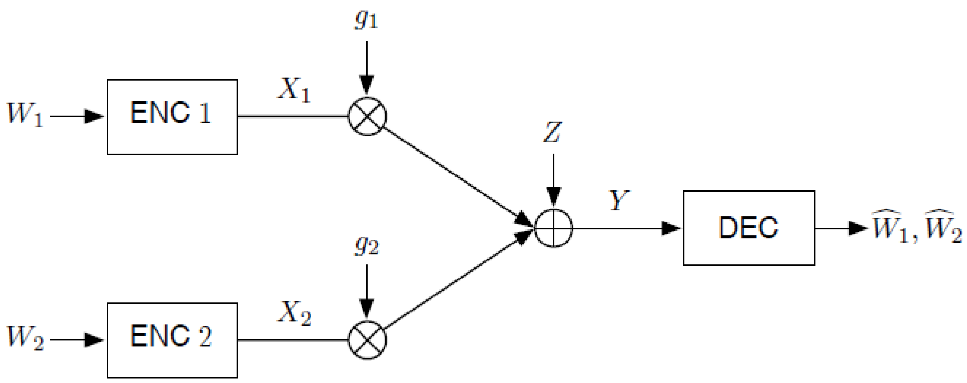
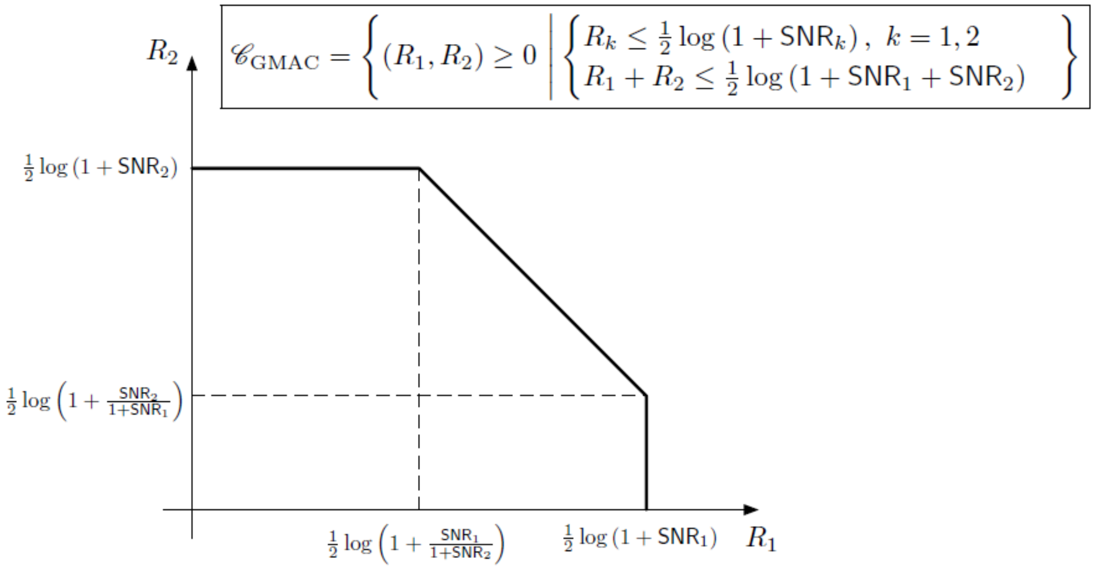


Figure: Block-diagram of the 2-User Gaussian MAC

- Channel model: $Y = g_1X_1 + g_2X_2 + Z$; $Z \sim \mathcal{N}(0, \sigma^2)$.

2-User Gaussian MAC

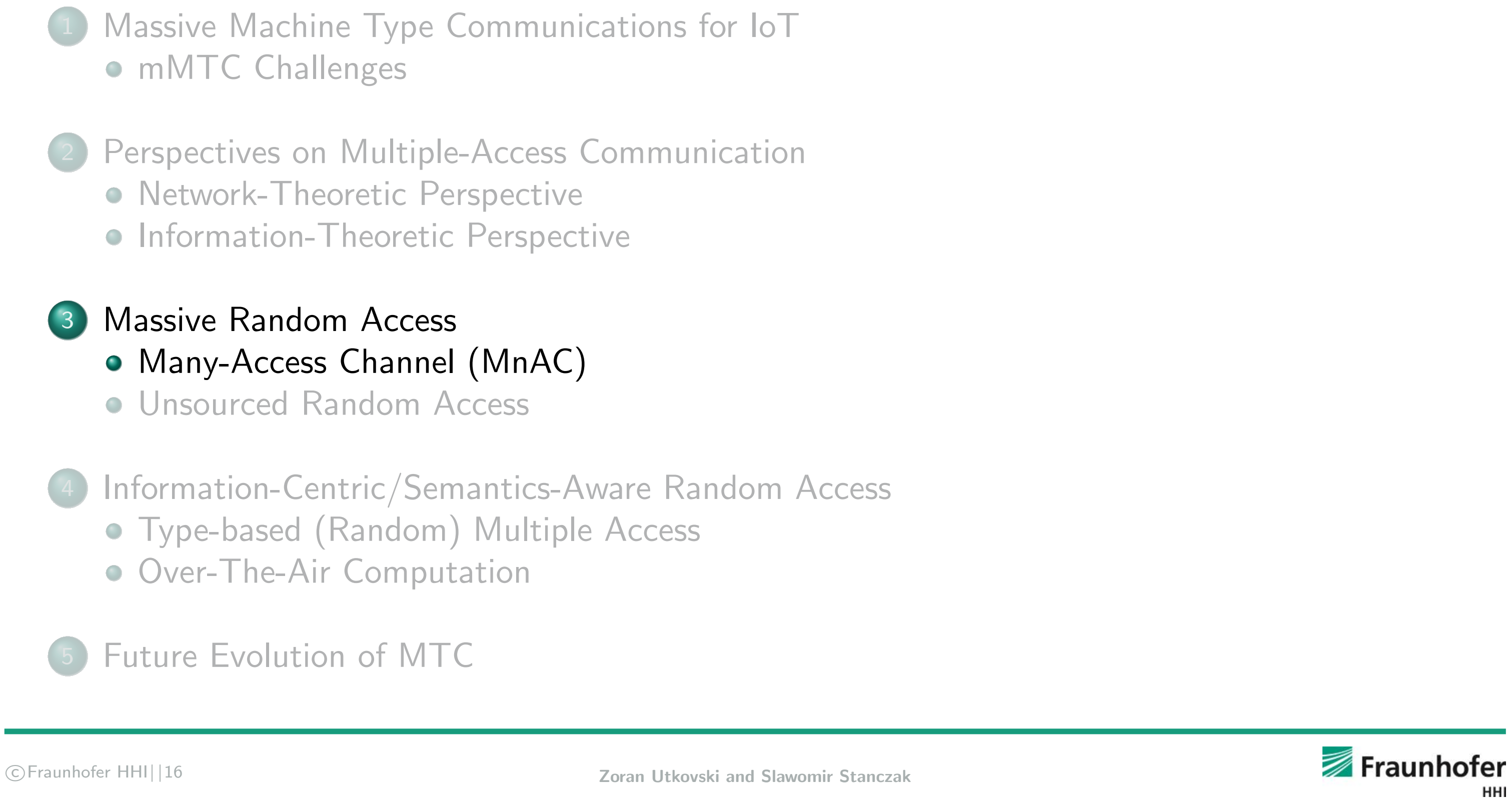


$$\mathscr{C}_{\mathrm{GMAC}} = \left\{ (R_1, R_2) \geq 0 \;\middle|\; \begin{cases} R_k \leq \frac{1}{2}\log\left(1 + \mathsf{SNR}_k\right), \; k = 1, 2 \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + \mathsf{SNR}_1 + \mathsf{SNR}_2\right) \end{cases} \right\}$$

R_2
$\frac{1}{2}\log(1+\mathsf{SNR}_2)$
$\frac{1}{2}\log\left(1+\frac{\mathsf{SNR}_2}{1+\mathsf{SNR}_1}\right)$
$\frac{1}{2}\log\left(1+\frac{\mathsf{SNR}_1}{1+\mathsf{SNR}_2}\right)$
$\frac{1}{2}\log(1+\mathsf{SNR}_1)$
R_1

Figure: Capacity region of the 2-User Gaussian MAC

1. Massive Machine Type Communications for IoT
2. Perspectives on Multiple-Access Communication
3. Massive Random Access
4. Information-Centric/Semantics-Aware Random Access
5. Future Evolution of MTC



1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

Many-Access Channel (MnAC)

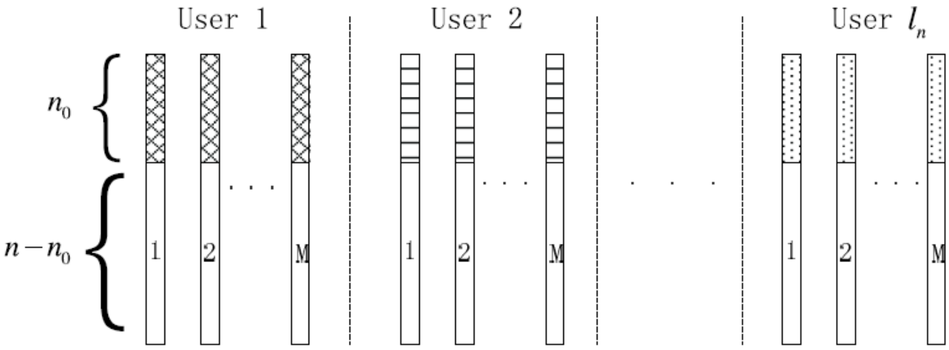


Figure: Codebook structure for a MnAC code. Source: [Chen2017].

- Each user maintains M codewords with each consisting of a message-bearing codeword prepended by a signature.

Many-Access Channel (MnAC)

- detecting active users of central importance
- related to the problem of sparse recovery (compressed sensing)
- analyzed when both blocklength n and number of users ℓ_n go to infinity
- key element is user detection based on signatures
- error defined based on joint correct detection of all users

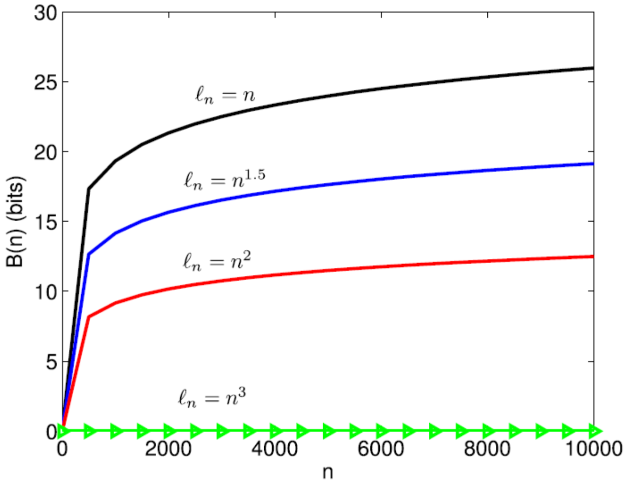
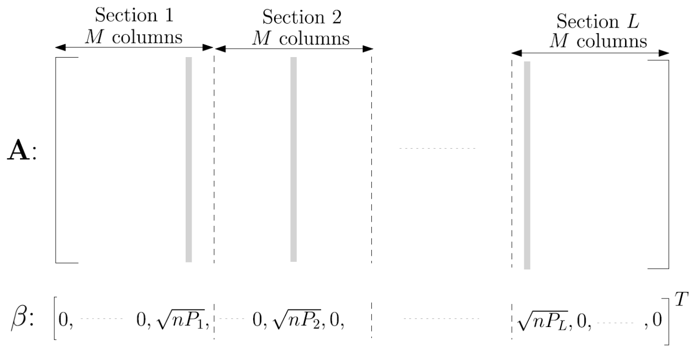


Figure: Asymptotically achievable message length. Source: [Chen2017].

Coding for MnAC

Sparse Regression Codes (SPARCs)

- Sparse regression codes (SPARCs) achieve the capacity of the AWGN channel [Joseph&Barron].
- SPARCs can be decoded with Approximate Message Passing (AMP) - based decoder.
- Probability of decoding error with AMP goes to zero as the block length goes to infinity, for all rates $R < C$ [Rush et al.]


Section 1
M columns
Section 2
M columns
Section L
M columns
$\mathbf{A}$:
β: $[0, \cdots 0, \sqrt{nP_1}, \cdots 0, \sqrt{nP_2}, 0, \cdots \sqrt{nP_L}, 0, \cdots, 0]^T$

Sparse Regression Code (SPARC) is specified by a design matrix $\mathbf{A}$ containing L sections of size M.

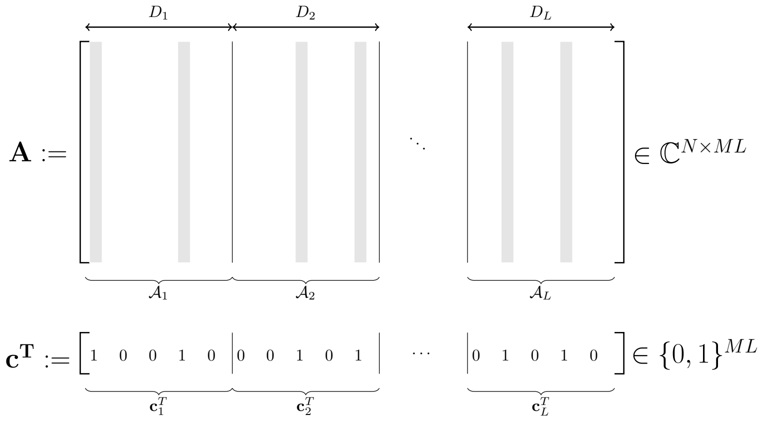
Connection to AMP via the measurement model

$$\mathbf{y} = \mathbf{A}\beta + \mathbf{w}.$$

Coding for MnAC

Sparse Superposition Codes (SSCs)

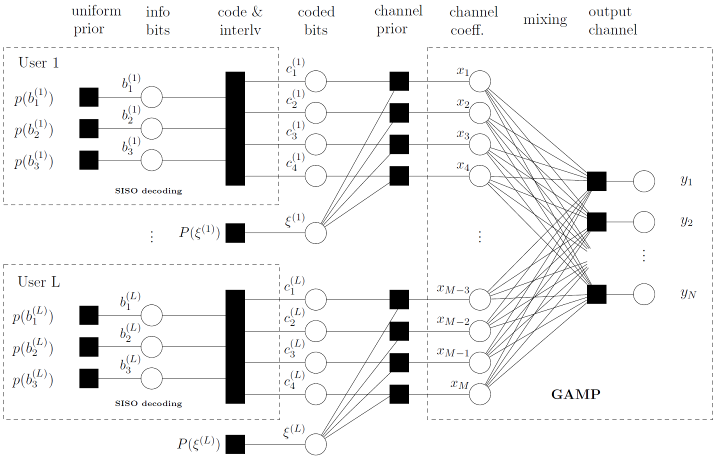
- We assume that each device D_l is active with probability ρ
- Device D_l has an associated dictionary $\mathcal{A}_l$ with M sequences of length N
- Information is conveyed by choosing a linear combination of the M sequences
- The linear combination is defined by a linear/nonlinear code $\mathcal{C}_l$



$$\mathbf{y} = \underbrace{\sum_{l=1}^{L} \lambda_l \gamma_l \mathrm{h}_l \mathbf{A}_l \mathbf{c}_l}_{\mathbf{Ax}} + \mathbf{w}$$

Coding for MnAC

Decoding of SSCs via Approximate Bayesian Inference



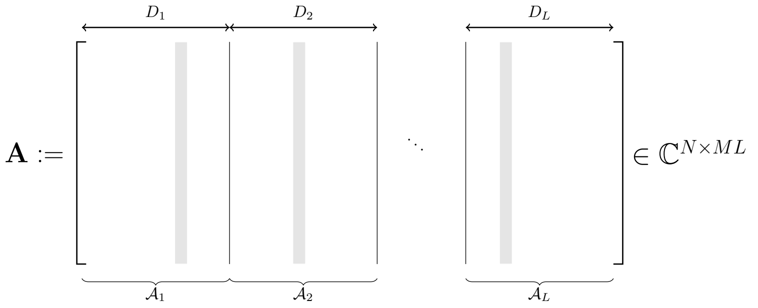
- The unknown vector $\mathbf{x}$ exhibits a specific structure dictated by:
  - the choice of the sets $\mathcal{A}_l$, $l \in [L]$ associated with the system users;
  - the encoding structure captured by $\mathcal{C}_l$;
  - the probability of user activation p_l;
- The joint probability density on which the inference algorithm operates, factorizes as

$$p(\mathbf{x},\mathbf{c},\xi|\mathbf{y}) \propto p(\mathbf{y}|\mathbf{x},\mathbf{c},\xi)p(\mathbf{x},\mathbf{c},\xi)$$
$$= \underbrace{p(\mathbf{y}|\mathbf{x})}_{g(\mathbf{x})}\prod_{l}\underbrace{p(\mathbf{c}_l)}_{h_l}P(\xi_l)\prod_{n}\underbrace{p(x_{l,n},c_{l,n},\xi_l)}_{f_{l,n}}$$

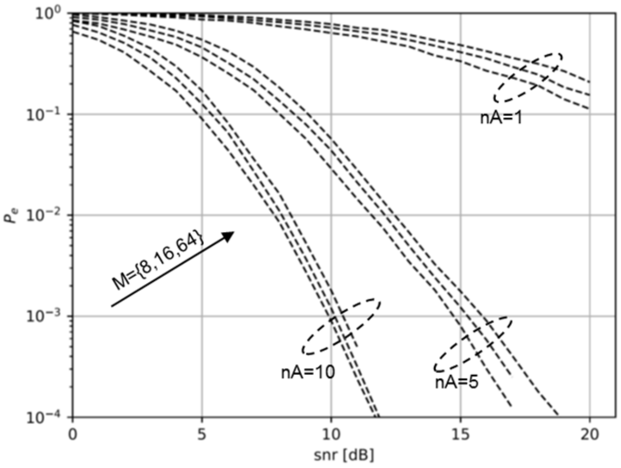
Joint activity detection and decoding

Performance Evaluation

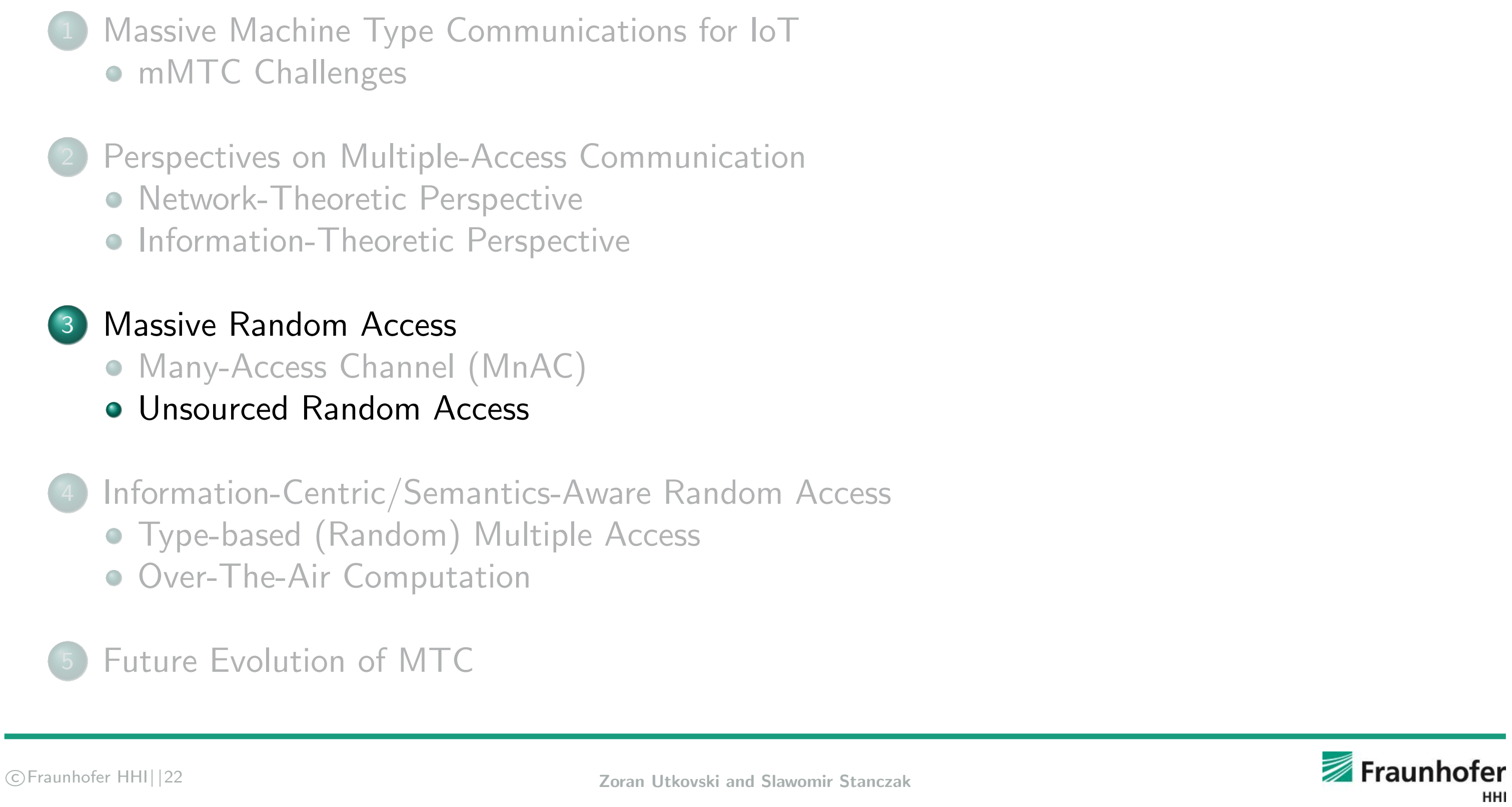
Nonlinear code (1-out-of-M)



$$\mathbf{c}^{\mathbf{T}} := \left[\underbrace{0\ 0\ 0\ 1\ 0}_{\mathbf{c}_1^T} \,\middle|\, \underbrace{0\ 0\ 1\ 0\ 0}_{\mathbf{c}_2^T} \,\middle|\, \cdots \,\middle|\, \underbrace{0\ 1\ 0\ 0\ 0}_{\mathbf{c}_L^T}\right] \in \{0,1\}^{ML}$$



$L = 1000$ Users. Probability of activation 0.1. Block error probability incl. false alarms and missed detections.

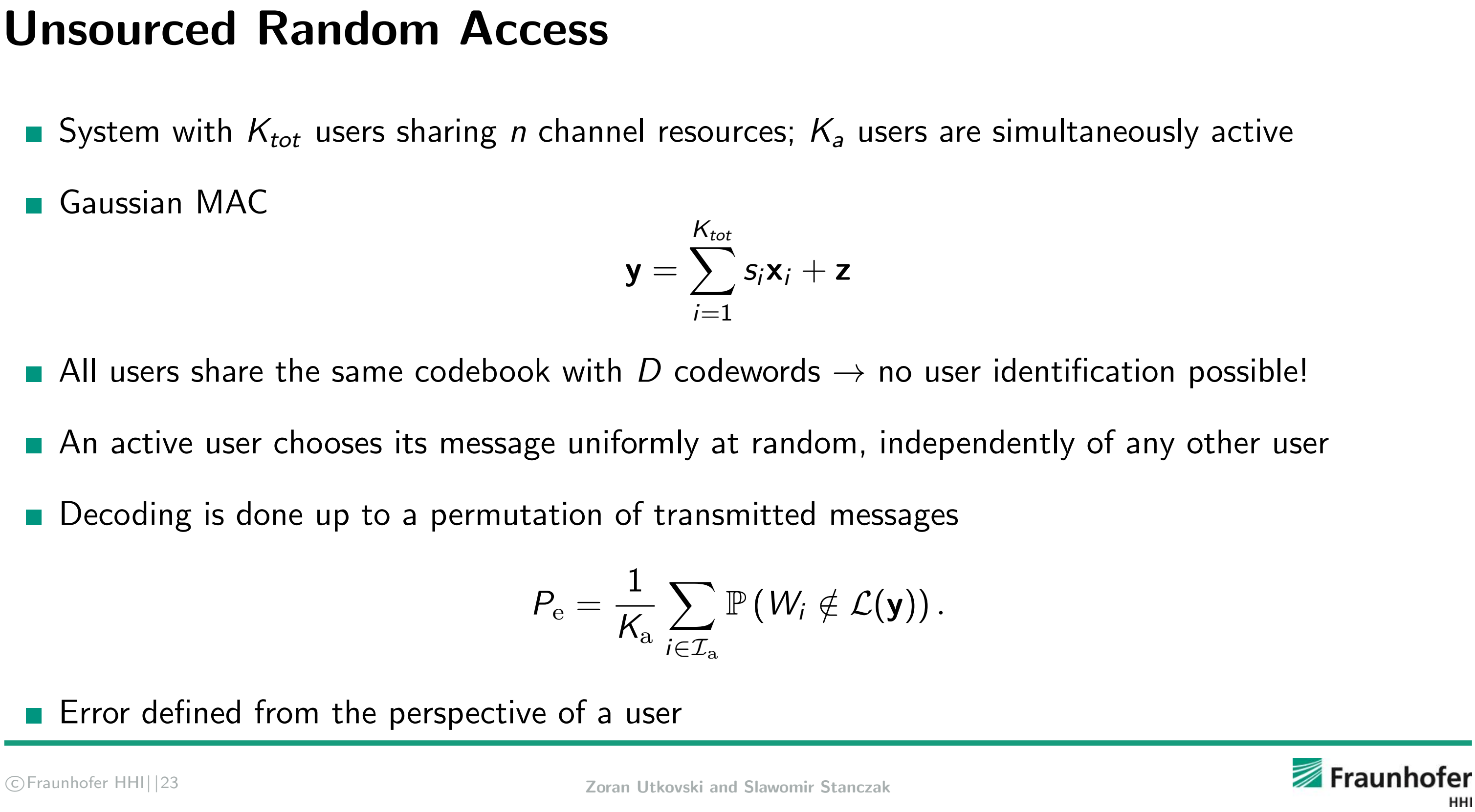


1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. **Massive Random Access**
   - Many-Access Channel (MnAC)
   - **Unsourced Random Access**
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

©Fraunhofer HHI||22

Zoran Utkovski and Slawomir Stanczak

Fraunhofer HHI



Unsourced Random Access

- System with K_{tot} users sharing n channel resources; K_a users are simultaneously active
- Gaussian MAC

$$\mathbf{y} = \sum_{i=1}^{K_{tot}} s_i \mathbf{x}_i + \mathbf{z}$$

- All users share the same codebook with D codewords → no user identification possible!
- An active user chooses its message uniformly at random, independently of any other user
- Decoding is done up to a permutation of transmitted messages

$$P_{\mathrm{e}} = \frac{1}{K_{\mathrm{a}}} \sum_{i \in \mathcal{I}_{\mathrm{a}}} \mathbb{P}\left(W_i \notin \mathcal{L}(\mathbf{y})\right).$$

- Error defined from the perspective of a user

©Fraunhofer HHI||23

Zoran Utkovski and Slawomir Stanczak

Fraunhofer HHI

Unsourced Random Access

State-of-the-Art Coding Schemes

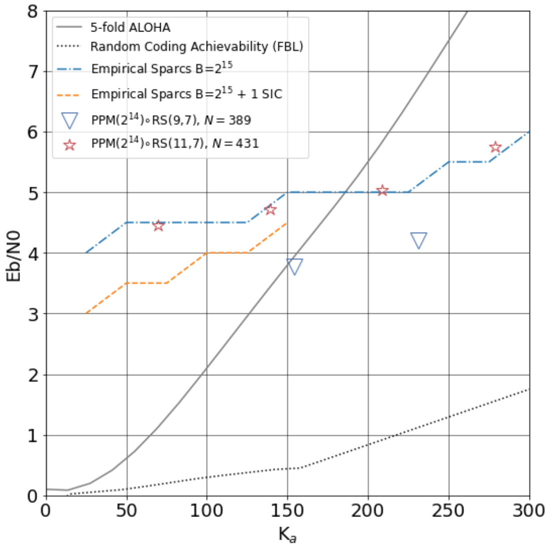
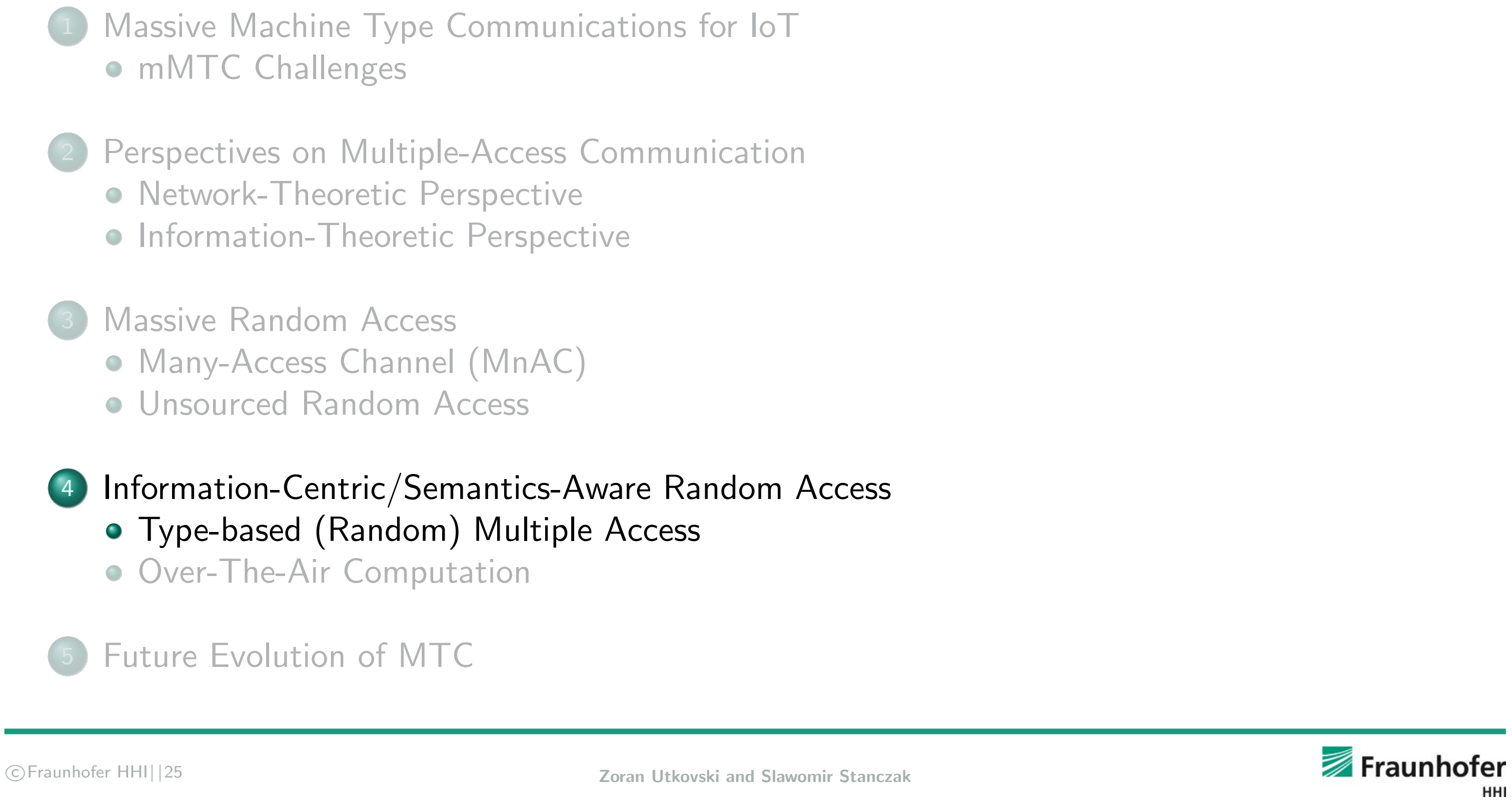


Figure: Performance comparison of coding schemes for unsourced random access.

1. Massive Machine Type Communications for IoT
2. Perspectives on Multiple-Access Communication
3. Massive Random Access
4. **Information-Centric/Semantics-Aware Random Access**
5. Future Evolution of MTC

Information-Centric Random Access

- The standard assumption in the literature on random access is that the user activation and the information content in the users' messages are **independent**.
- This, however, may not be the case in **event-driven communication**, where the user transmit **common messages** (e.g. alarms) upon the observation of a certain event.
- We refer to this operational mode as *information-centric* as it focuses on the recovery of a common information (messages) initiated by a group of simultaneously active transmitters.



1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. **Information-Centric/Semantics-Aware Random Access**
   - **Type-based (Random) Multiple Access**
   - Over-The-Air Computation
5. Future Evolution of MTC

©Fraunhofer HHI||25

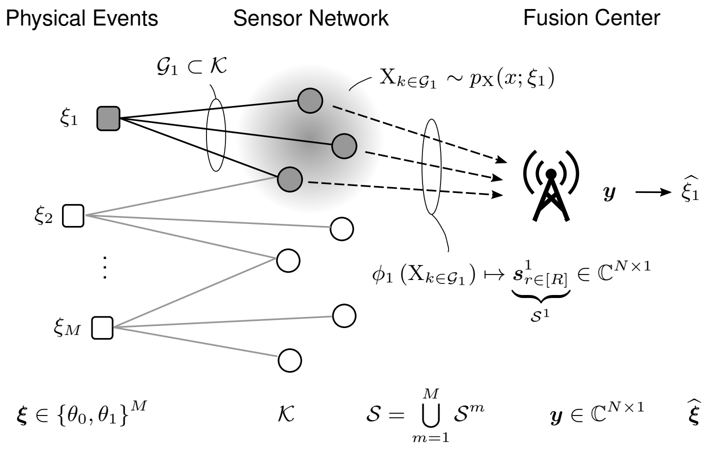
Zoran Utkovski and Slawomir Stanczak

Fraunhofer HHI

Type-based (random) multiple access

Event-based IoT

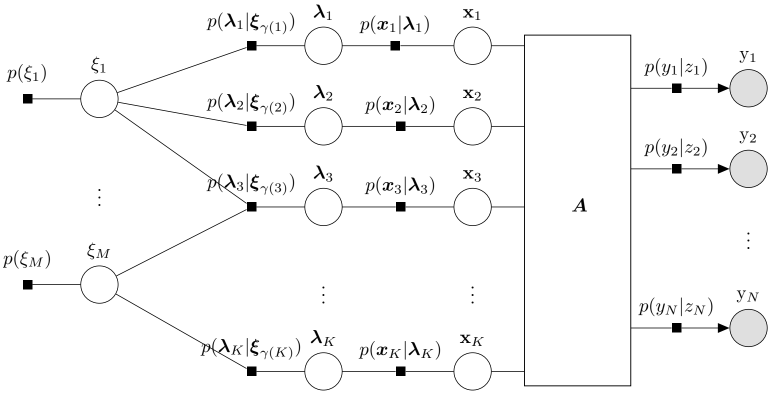
- A wireless sensor network $\mathcal{K}$ observes physical events $\boldsymbol{\xi}$ at different states $\boldsymbol{\theta}$.
- Upon detection of a specific state of the m-th event, each sensor k measures a specific value X_k
- X_k is quantized into R discrete values and transmitted over the MAC to a fusion center


Physical Events
Sensor Network
Fusion Center
$\mathcal{G}_1 \subset \mathcal{K}$
$\mathrm{X}_{k\in\mathcal{G}_1} \sim p_{\mathrm{X}}(x;\xi_1)$
ξ_1
ξ_2
ξ_M
$\boldsymbol{y}$
$\widehat{\xi}_1$
$\phi_1\left(\mathrm{X}_{k\in\mathcal{G}_1}\right) \mapsto \underbrace{\boldsymbol{s}^1_{r\in[R]}}_{\mathcal{S}^1} \in \mathbb{C}^{N\times 1}$
$\boldsymbol{\xi} \in \{\theta_0,\theta_1\}^M$
$\mathcal{K}$
$\mathcal{S} = \bigcup_{m=1}^{M} \mathcal{S}^m$
$\boldsymbol{y} \in \mathbb{C}^{N\times 1}$
$\widehat{\boldsymbol{\xi}}$

Type-based (random) multiple access

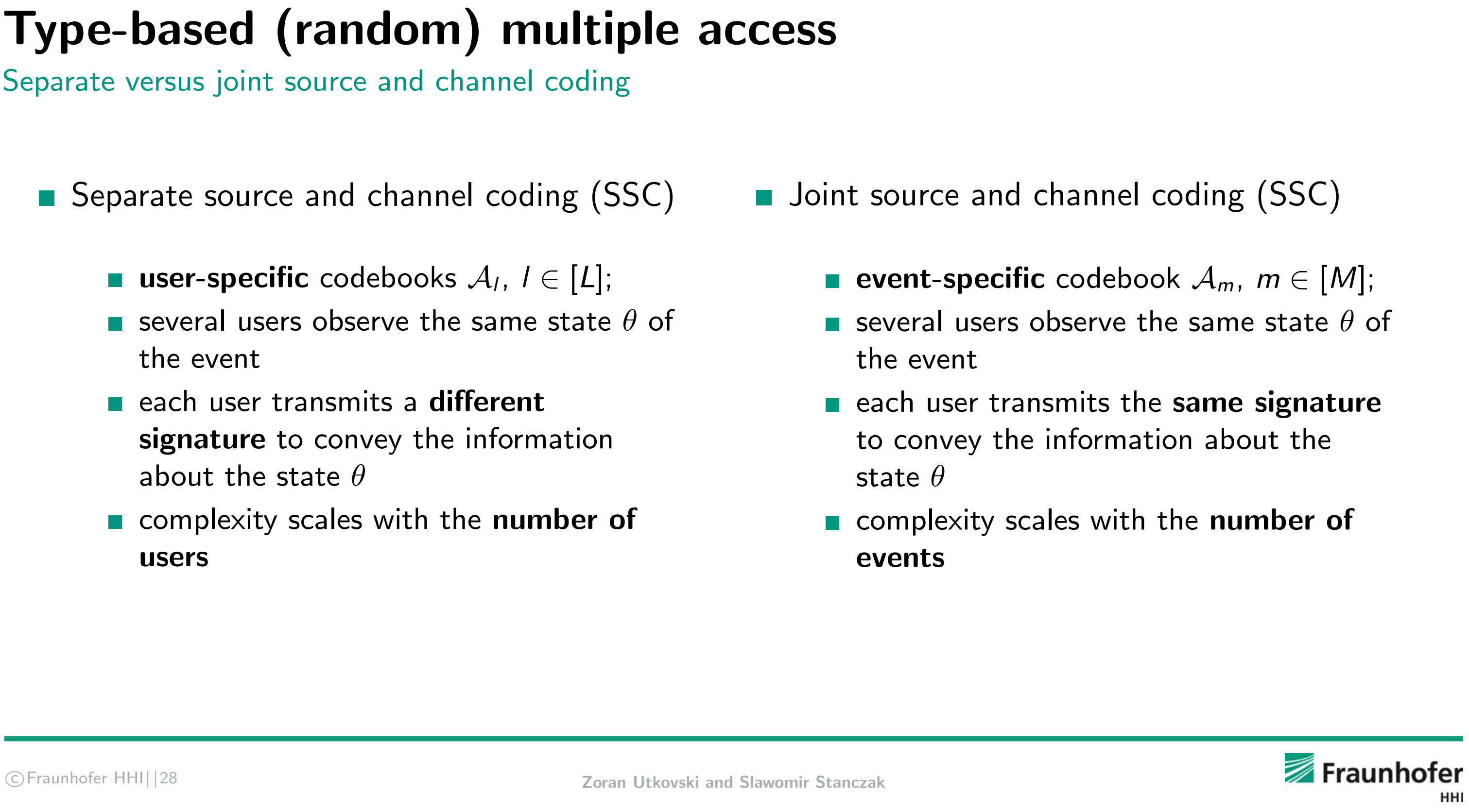
A Bayesian perspective

- $\lambda_1, \ldots, \lambda_K$ capture the activity of the devices
- $p(\lambda_k|\xi_m)$ representing the *sensitivity* of the device k to the event E_m
- $p(\boldsymbol{\lambda}|\boldsymbol{\xi})$ prescribes the devices membership to the groups $\mathcal{G}_1, \ldots, \mathcal{G}_M$


$p(\xi_1)$
ξ_1
$p(\xi_M)$
ξ_M
$p(\boldsymbol{\lambda}_1|\boldsymbol{\xi}_{\gamma(1)})$
$p(\boldsymbol{\lambda}_2|\boldsymbol{\xi}_{\gamma(2)})$
$p(\boldsymbol{\lambda}_3|\boldsymbol{\xi}_{\gamma(3)})$
$p(\boldsymbol{\lambda}_K|\boldsymbol{\xi}_{\gamma(K)})$
$\boldsymbol{\lambda}_1$
$\boldsymbol{\lambda}_2$
$\boldsymbol{\lambda}_3$
$\boldsymbol{\lambda}_K$
$p(\boldsymbol{x}_1|\boldsymbol{\lambda}_1)$
$p(\boldsymbol{x}_2|\boldsymbol{\lambda}_2)$
$p(\boldsymbol{x}_3|\boldsymbol{\lambda}_3)$
$p(\boldsymbol{x}_K|\boldsymbol{\lambda}_K)$
$\mathbf{x}_1$
$\mathbf{x}_2$
$\mathbf{x}_3$
$\mathbf{x}_K$
$\boldsymbol{A}$
$p(y_1|z_1)$
$p(y_2|z_2)$
$p(y_N|z_N)$
y_1
y_2
y_N

$$p(\boldsymbol{\xi}, \boldsymbol{\lambda}, \mathbf{x}, \mathbf{y}) = \prod_{m=1}^{M} p(\xi_m) \prod_{k=1}^{K} p(\boldsymbol{\lambda}_k|\boldsymbol{\xi}_{\gamma(k)}) \prod_{j=1}^{K} p(\boldsymbol{x}_j|\boldsymbol{\lambda}_j) \prod_{i=1}^{N} p(y_i|z_i),$$

where $z_i = \mathbf{a}_i^{\mathrm{T}}\mathbf{x}$, with $\mathbf{a}_i$ being the i-th row of $\mathbf{A}$.



Type-based (random) multiple access

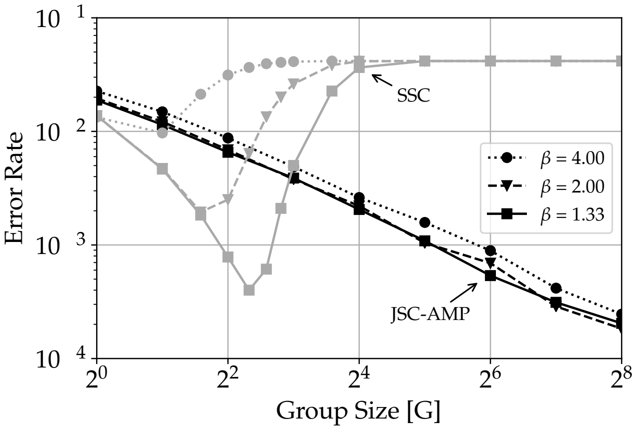
Separate versus joint source and channel coding

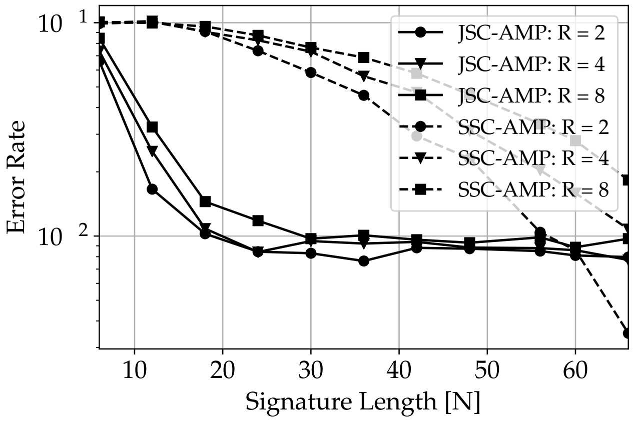
- Separate source and channel coding (SSC)
  - **user-specific** codebooks $\mathcal{A}_l$, $l \in [L]$;
  - several users observe the same state θ of the event
  - each user transmits a **different signature** to convey the information about the state θ
  - complexity scales with the **number of users**

- Joint source and channel coding (SSC)
  - **event-specific** codebook $\mathcal{A}_m$, $m \in [M]$;
  - several users observe the same state θ of the event
  - each user transmits the **same signature** to convey the information about the state θ
  - complexity scales with the **number of events**

Type-based (random) multiple access

Performance Evaluation (Preliminary)

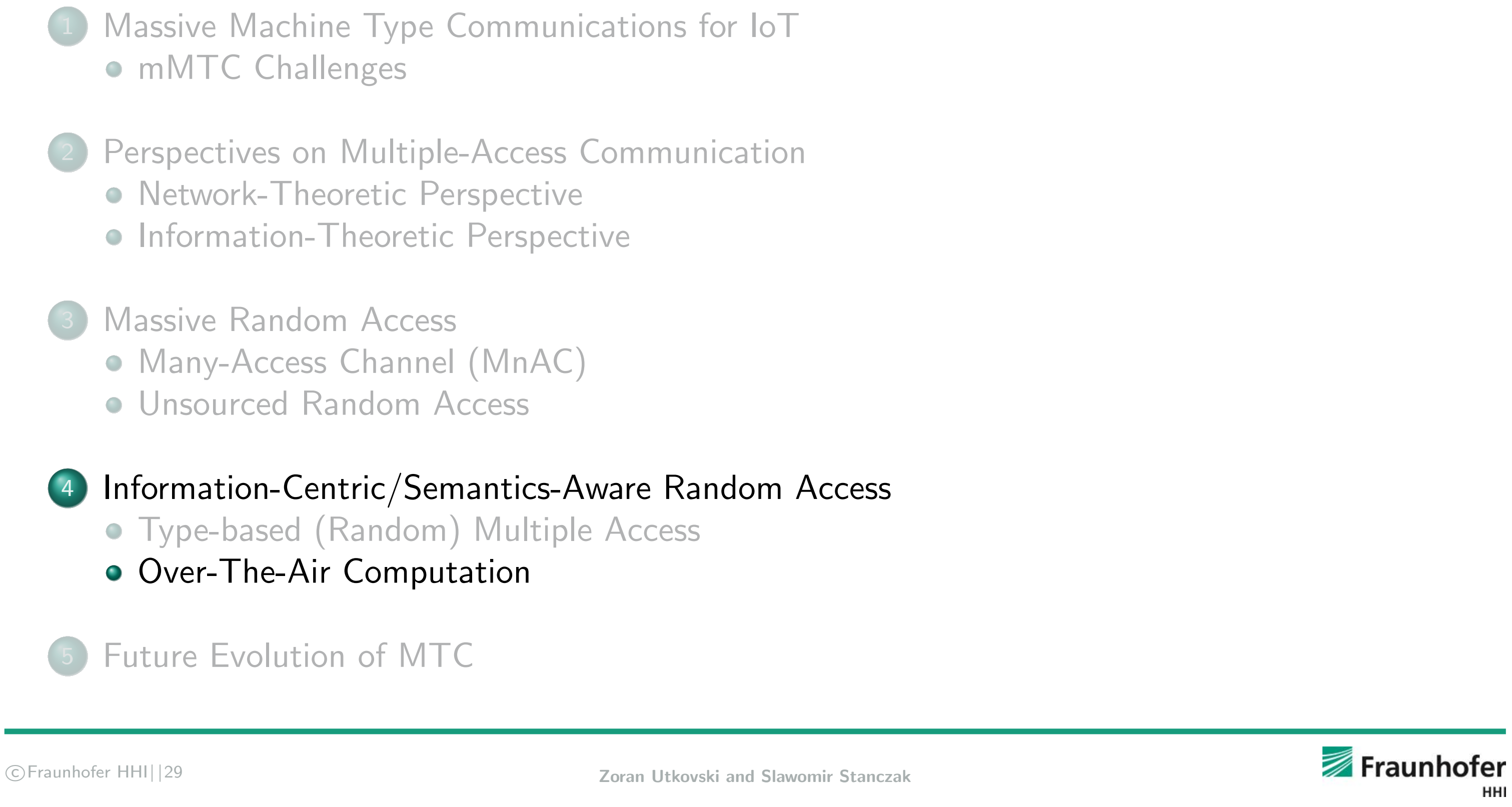




ⓒFraunhofer HHI||29

Zoran Utkovski and Slawomir Stanczak

Fraunhofer HHI

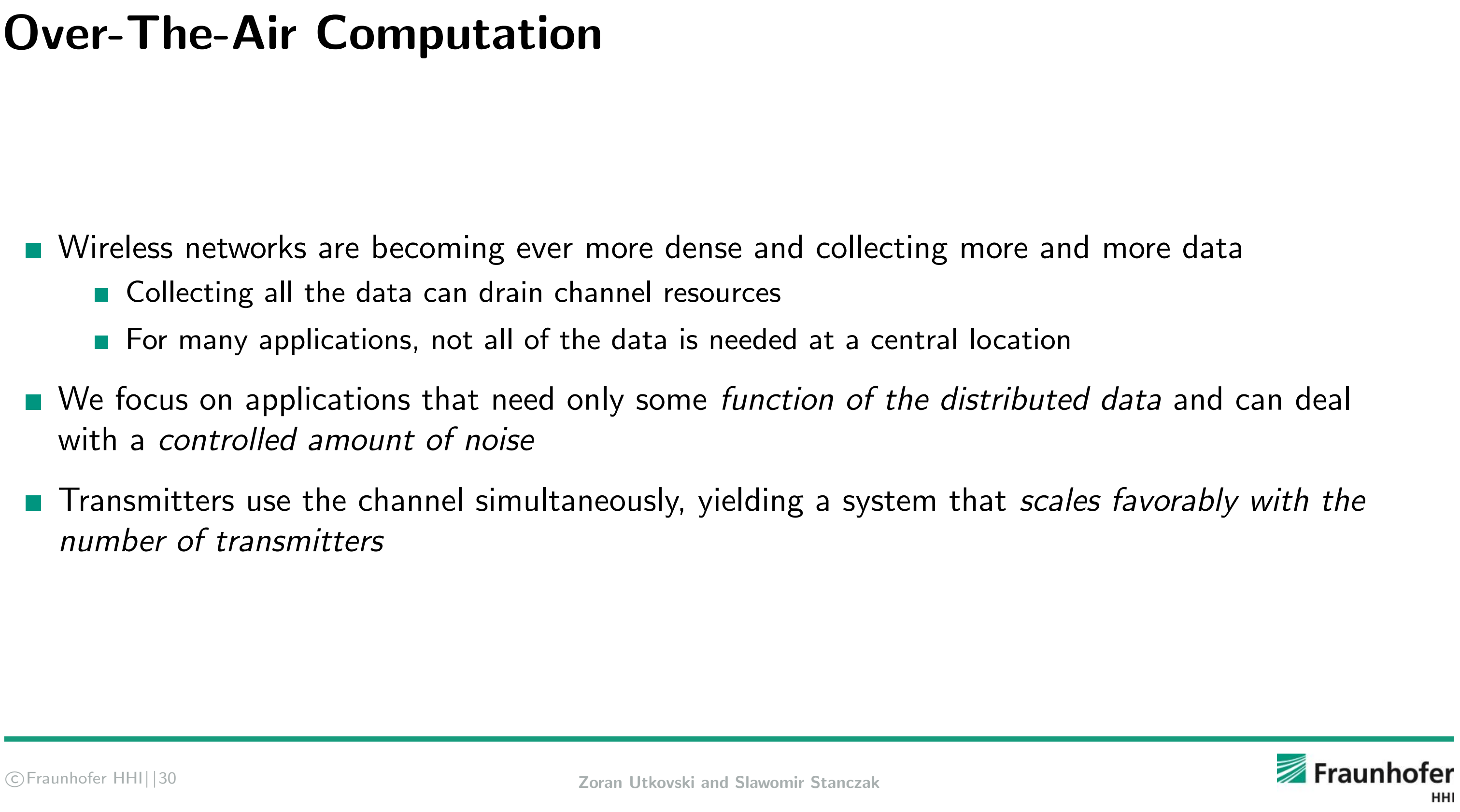


1. Massive Machine Type Communications for IoT
   - mMTC Challenges
2. Perspectives on Multiple-Access Communication
   - Network-Theoretic Perspective
   - Information-Theoretic Perspective
3. Massive Random Access
   - Many-Access Channel (MnAC)
   - Unsourced Random Access
4. Information-Centric/Semantics-Aware Random Access
   - Type-based (Random) Multiple Access
   - Over-The-Air Computation
5. Future Evolution of MTC

©Fraunhofer HHI||29

Zoran Utkovski and Slawomir Stanczak

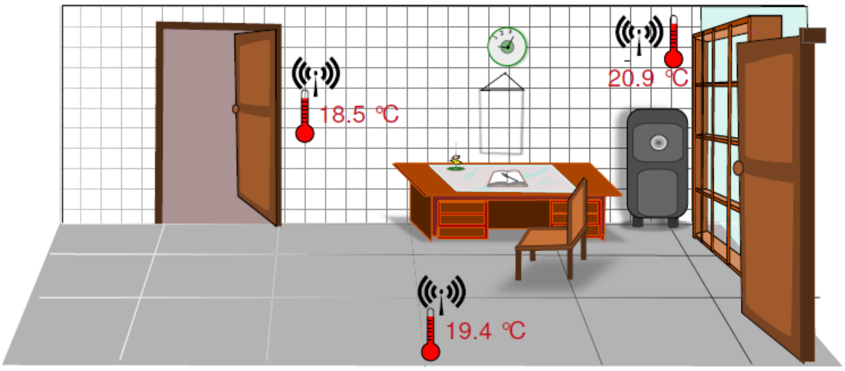
Fraunhofer HHI

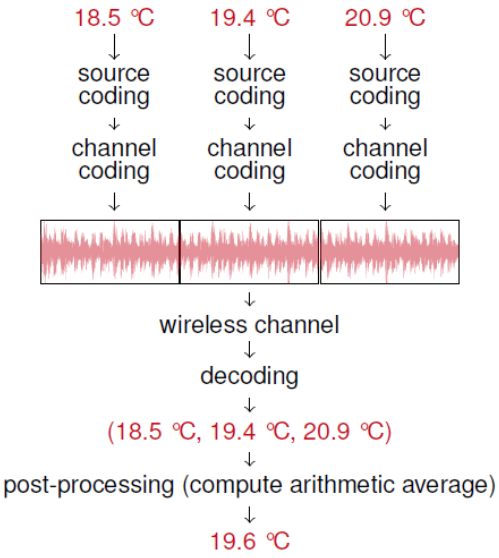


Over-The-Air Computation

- Wireless networks are becoming ever more dense and collecting more and more data
  - Collecting all the data can drain channel resources
  - For many applications, not all of the data is needed at a central location
- We focus on applications that need only some *function of the distributed data* and can deal with a *controlled amount of noise*
- Transmitters use the channel simultaneously, yielding a system that *scales favorably with the number of transmitters*

Over-The-Air Computation





18.5 °C	19.4 °C	20.9 °C
↓	↓	↓
source coding	source coding	source coding
↓	↓	↓
channel coding	channel coding	channel coding
↓	↓	↓

↓

wireless channel

↓

decoding

↓

(18.5 °C, 19.4 °C, 20.9 °C)

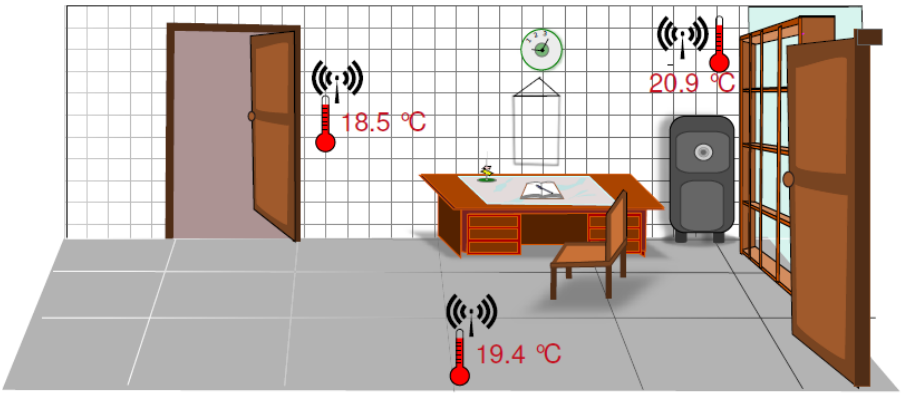
↓

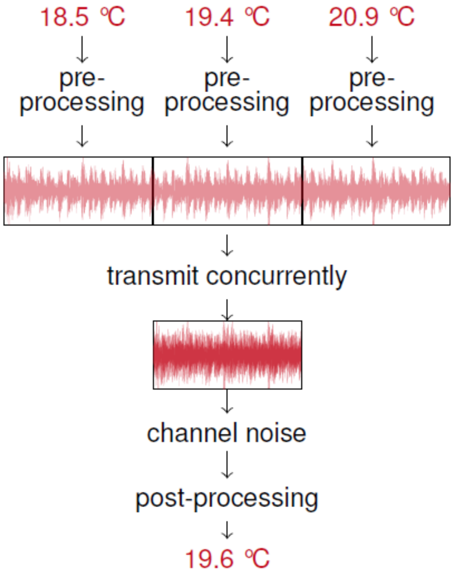
post-processing (compute arithmetic average)

↓

19.6 °C

Over-The-Air Computation





18.5 ℃ → pre-processing

19.4 ℃ → pre-processing

20.9 ℃ → pre-processing

↓

transmit concurrently

↓

channel noise

↓

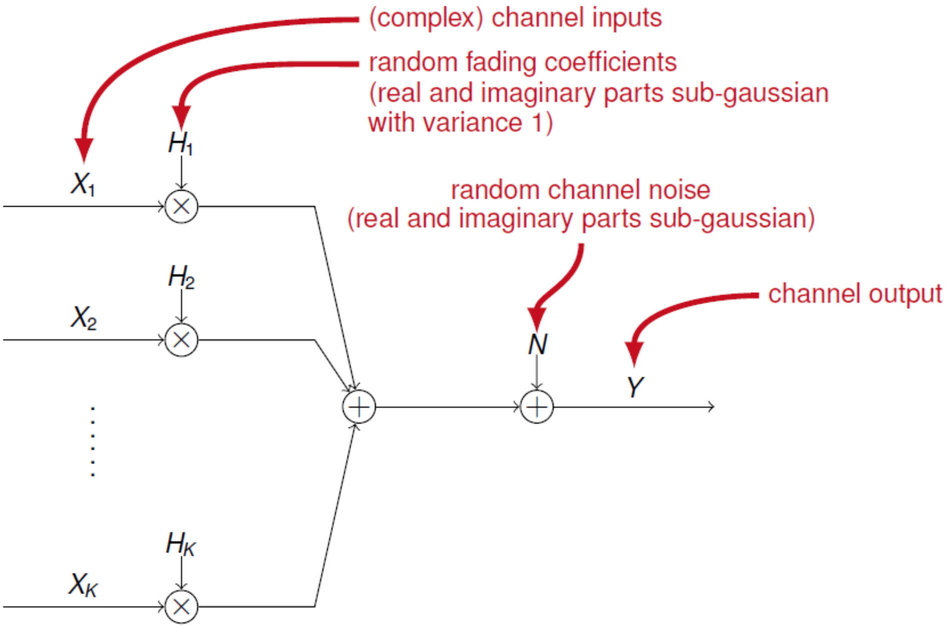
post-processing

↓

19.6 ℃

Over-The-Air Computation

Channel Model



(complex) channel inputs

random fading coefficients
(real and imaginary parts sub-gaussian
with variance 1)

random channel noise
(real and imaginary parts sub-gaussian)

channel output

Over-The-Air Computation

Nomographic Functions

- Every function $f : [0,1]^K \to \mathbb{R}$ has a *nomographic representation*

$$f(s_1,\dots,s_K) = F\big(f_1(s_1) + \cdots + f_K(s_K)\big).$$

- Problem: A small error in the argument (e.g., due to channel noise) can have huge effects on the computed value
- Every *continuous* function $f : [0,1]^K \to \mathbb{R}$ can be written as a sum of nomographic representations of the form

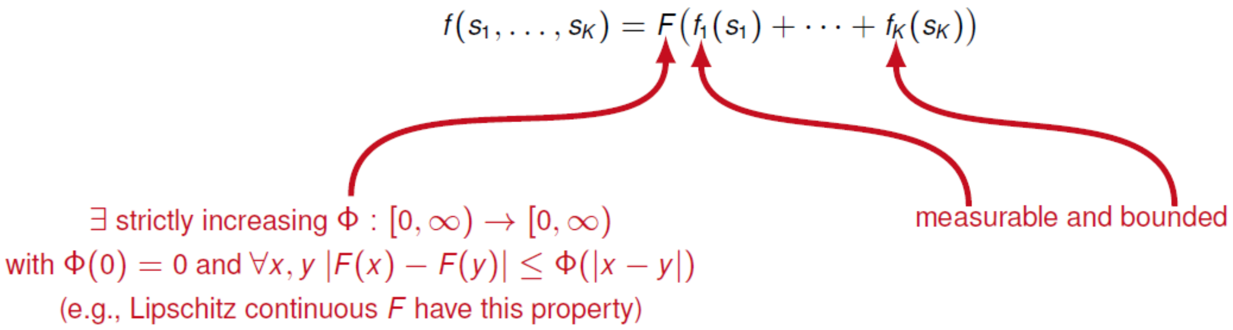
$$f(s_1,\dots,s_K) = \sum_{k=1}^{2K+1} g_k(s_1,\dots,s_K),$$

where the g_k have nomographic representations in which *all functions involved are continuous*.

- Problem: Even continuity offers no guarantees for the effects of slight errors in the arguments

Over-The-Air Computation

Class of Functions to be approximated



$$f(s_1, \dots, s_K) = F(f_1(s_1) + \cdots + f_K(s_K))$$

$\exists$ strictly increasing $\Phi : [0, \infty) \to [0, \infty)$
with $\Phi(0) = 0$ and $\forall x, y$ $|F(x) - F(y)| \leq \Phi(|x - y|)$
(e.g., Lipschitz continuous F have this property)

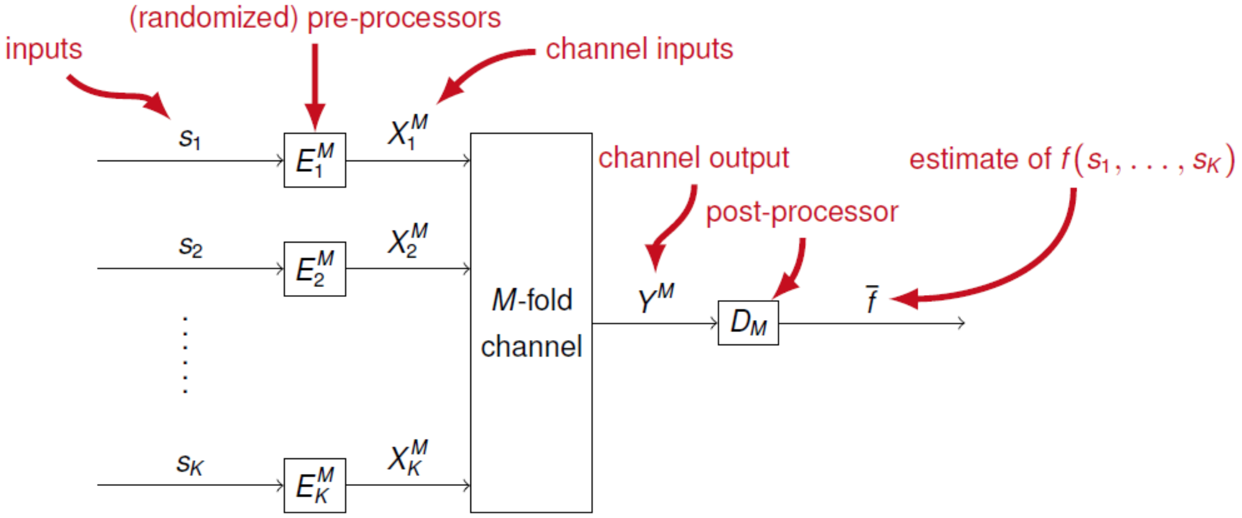
measurable and bounded

Examples:

- *K-linear* functions, such as *sums* and *arithmetic averages* are in the class
- *p-norms* on compact domains for $p \geq 1$ are in the class
- The *maximum* function is *not* in the class

Over-The-Air Computation

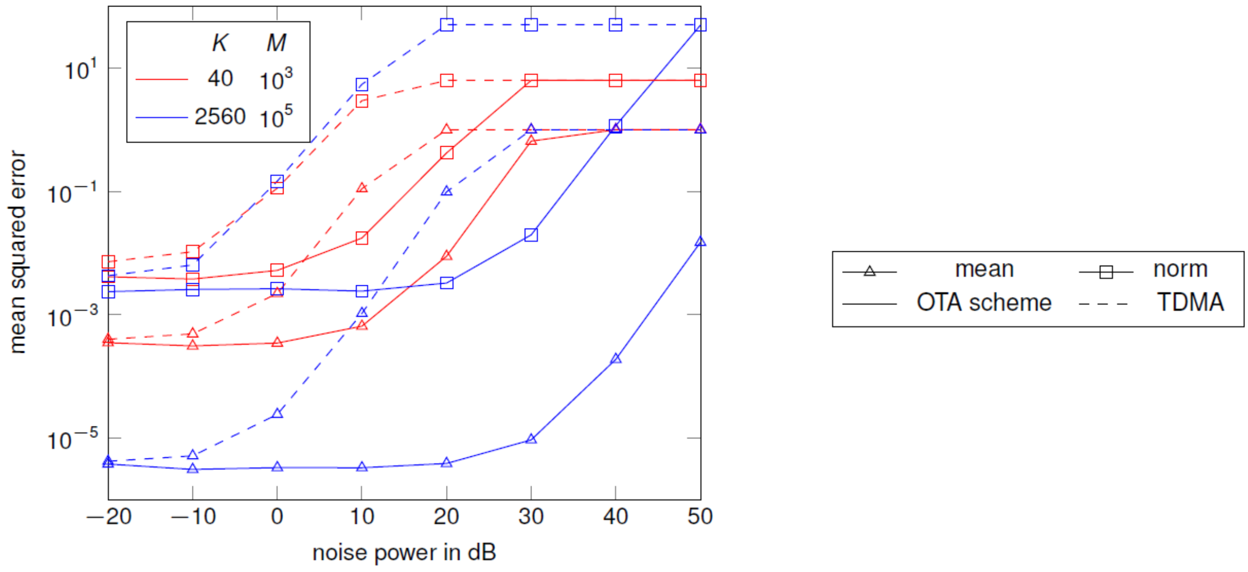
Main Result



$$f(s_1, \ldots, s_K) = F(f_1(s_1) + \cdots + f_K(s_K))$$

Over-The-Air Computation

Numerical Results



1. Massive Machine Type Communications for IoT
2. Perspectives on Multiple-Access Communication
3. Massive Random Access
4. Information-Centric/Semantics-Aware Random Access
5. **Future Evolution of MTC**

Future Evolution of MTC

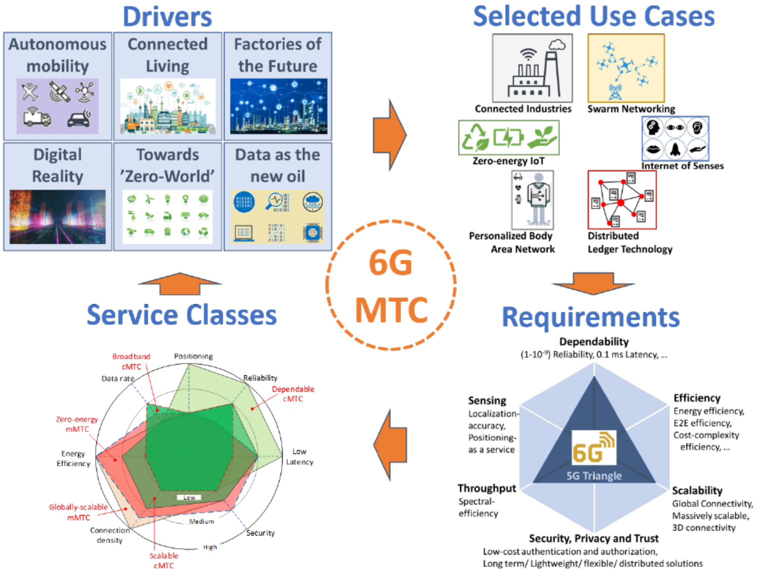


Figure: Source: [White Paper on Critical and Massive Machine Type Communication Towards 6G]

CPS&IoT'2021 Summer School on
Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

Schedule

Day 1, Monday 7 June:

09:00-10:00 Event Chairs and Special Guests

Title: Opening Ceremony of the CPS&IoT'2021 Summer School, and MECO'2021 and CPS&IoT'2021 Conferences
Opening Keynote by Konstantin Novoselov, Nobel Laureate in Physics 2010, NUS, SG

10.00-11.00 Ioannis Pitas, Aristotle University of Thessaloniki, GR

Title: **Keynote**: Privacy Protection, Ethics, Robustness and Regulatory Issues in Autonomous Systems

11.00-11.30 Break

11.30-12.00 Lech Jóźwiak, TU/e, NL

Title: Introduction to the CPS&IoT'2021 Summer School

12.00-13.30 Lech Jóźwiak, TU/e, NL

Title: Design of Green CPS and IoT

13.30-15.00 Lunch Break

15.00-16.30 Mario Kovač, FER, HR

Title: European Processor Initiative: Cornerstone of European HPC and eHPC strategy

16.30-17.00 Break

17.00-18.00 Nicola Capodieci, University of Modena and Reggio Emilia, IT

Title: Timing predictability in GPGPU computing for ADAS: challenges and future directions in real-time embedded platforms

21.00 Gala Dinner

Day 2, Tuesday 8 June:

09.00-10.00 Benoît De Dinechin, KAELEY Inc., FR

Title: **Keynote**: Engineering a Manycore Processor for Edge Computing

10.00-11.00 Danilo Mandic, Imperial College, London, UK

Title: **Keynote**: Hearables: From in-ear recording of vital signs and neural function to doctorless hospitals

11.00-11.30 Break

11.30-13.00 Kim Guldstrand Larsen and Marius Mikučionis, AAU, DK

Title: Learning, Analysis, Synthesis and Optimization of Cyber-Physical Systems

13.00-14.00 Lunch Break

14.00-15.30 Radu Grosu, TU-WIEN, AT

Title: Machine Learning and Control of CPS/IoT

15.30-17.00 Muhammad Shafique, NYU-AD, UAE, Muhammad Abdullah Hanif, TU-WIEN, Alberto Marchisio, TU-WIEN, AT

Title: Energy-Efficient Deep Learning at the Edge: A Cross-Layer Approach

17.00-17.30 Break

17.30-19.00 Daniel Madronal Quintin, UNISS, Giacomo Valente, UNIVAQ, Francesco Ratto, UNICA, IT

Title: Dataflow-Based Toolchain for Adaptive Hardware Accelerators Deployment and Monitoring

Day 3, Wednesday 9 June:

09.20-10.00 Hui Cao, Head of Policy and Strategy of Huawei's EU office

Title: **Keynote**: 5G Connectivity: the Key to Success for European Industry

10.00-11.30 Eugenio Villar, TEISA/UNICAN, ES

Title: Model-Driven Design of CPSoSs: Application to drone-based services

11.30-11.45 Break

11.45-13.15 Stefanos Skalistis, Raytheon Technologies, Ireland

Title: Building adaptively fault-tolerant avionics systems

13.15-14.15 Lunch Break

14.15-15.45 Abdelhakim Baouya and Salim Chehida, University Grenoble-Alpes, FR

Title: Design and verification of collaborative robots system

15.45-17.15 Aris Lalos, Christos Koulamas and Dimitrios Serpanos ISI, GR

Title: Secure and Efficient Industrial IoT: Architectures and Technologies

17.15-17.30 Break

17.30-19.00 Radovan Stojanovic, University of Montenegro and MECOnet, ME

Title: Challenging issues in cost effective wearable and IoT medicat devices with emphasis on Covid19 detection

Day 4, Thursday 10 June:

09.00-11.00 Alberto Cardoso, António Dourado, Jorge Henriques, Paulo Gil**,** University of Coimbra, PT

Title: Intelligent data analysis towards predictive maintenance in cyber-physical systems

11.00-11.30 Break

11.30-13.00 Christoph Schmittner, AIT, AT

Title: Security engineering for smart farming – from automated vehicles to sensor networks.

13.00-15.00 Lunch Break

15.00-16.30 Slawomir Stanczak and Zoran Utkovski, HHI/FRAUNHOFER, DE

Title: Modern Random Access Protocols for Massive Connectivity in the Internet of Things

16.30-17.00 Closing of the CPS&IoT'2021 Summer School

Day 5, Friday 11 June: Excursion possible (excursion fee is not included in the summer school fee; on own cost of participants) **+ Free participation in sessions of the CPS&IoT'2021 Conference and MECO'2021 Conference**

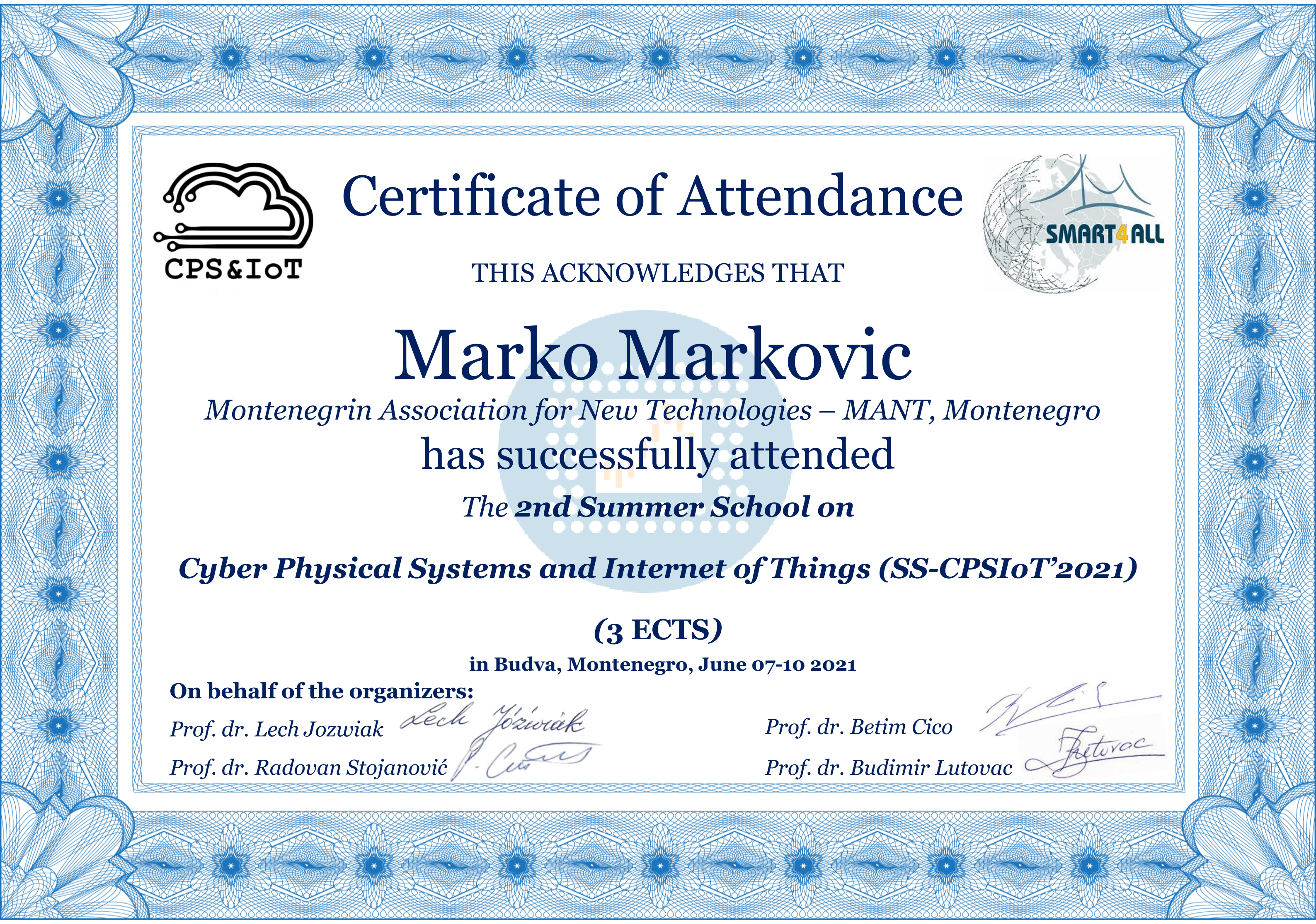
Summer School participants are expected to come with their own laptops. Internet access will be guaranteed.

2nd Summer School on Cyber Physical Systems and Internet of Things - SS-CPSIoT'2021

2nd Generation (Students and Teachers)

Budva, Montenegro, 07-10.06.2021

Student or Teacher	Country	Affiliation
Abdelhakim Baouya	France	Université Grenoble Alpes
Abhinav Vishwakarma	Germany	BTU Cottbus - Senftenberg
Ahmed Abdo	United States	university of california,Riverside
Alberto Cardoso	Portugal	University of Coimbra, CISUC
Alberto Delgado Romero	Espańa	SMART4ALL, Polytechnic University of Valencia, Espańa
Alberto Marchisio	Austria	Vienna University of Technology
Albion Morina	Kosovo	SMART4ALL, University “Ukshin Hoti” Prizren, Kosovo
Alexandros Spournias	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
António Dourado	Portugal	University of Coimbra, CISUC
Ardit Deda	Albania	Comdata
Ardit Dervishi	Albania	Metropolitan University
Aris Lalos	Greece	Industrial Systems Institute, Athena R.C.
Bahar Houtan	Sweden	Mälardalen University
Betim Cico	Albania	Metropolitan University of Tirana
Budimir Lutovac	Montenegro	University of Montenegro
Burak Karaduman	Belgium	University of Antwerp
Christoph Schmittner	Austria	AIT
Christos Koulamas	Greece	Industrial Systems Institute / "Athena" R.C.
Dadmehr Rahbari	Estonia	Tallinn University of Technology
Dhurate Hyseni	Kosovo	University "Ukshin Hoti" Prizren
Dimitrios Serpanos	Greece	Computer Technology Institute and Press "Diophantus", Industrial Systems Institute, Athena R.C.
Dimitris Kontargiris	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
Đorde Novakovic,	Serbia	SMART4ALL, FTN University of Novi Sad, Serbia
Elia Leoni	Italy	University of Bologna - Fondazione Bruno Kessler
Emima Jiva	Espańa	SMART4ALL, Polytechnic University of Valencia, Espańa
Eugenio Villar	Spain	University of Cantabria
Foisal Ahmed	Estonia	Tallinn University of Technology
Genti Rustemi	Albania	Metropolitan University, Tirana, Albania
Georgia Kaisari	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
Giacomo Valente	Italy	University of L'Aquila
Hector Gerardo Muñoz Hernandez	Germany	Brandenburg University of Technology Cottbus-Senftenberg
Hector Posadas	Spain	University of Cantabria
Ivan Aleksi	Croatia	University of Osijek
Javier Hoffmann	Germany	B-TU Cottbus-Senftenberg
Javier Merino	Spain	University of Cantabria
Jawhara Bader	Saudi Arabia	University of glasgow
Jorge Henriques	Portugal	University of Coimbra, CISUC
Jose Carlos Almeida	Portugal	Coimbra University
Josip Zidar	Croatia	University of Osijek
Jovan Djurkovic	Montenegro	MECOnet, Montenegro
Kevin Hutto	United States	Georgia Institute of Technology
Keyvan Shahin	Germany	Brandenburg university of technology
Kim G Larsen	Denmark	Aalborg University, Denmark
Kwame Ampadu	Germany	Brandenburg University of Technology
Lech Jozwiak	Netherlands	Eindhoven Technical University
Lefteris Pappas	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
Malina Adach	Sweden	Mälardalen University
Marina Subotin,	Serbia	SMART4ALL, FTN University of Novi Sad, Serbia
Marius Mikučionis	Denmark	Aalborg University
Mitko Veleski	Germany	BTU Cottbus-Senftenberg
Mohammadreza Heidari Iman	Estonia	SMART4ALL, Tallinn University of Technology, Estonia
Nicola Capodieci	Italy	University of Modena And Reggio Emilia
Nouha Laamech	France	University of Pau and the Adour Region
Panagiotis Bountas	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
Paulo Gil	Portugal	University of Coimbra, CISUC
Priscile Suawa	Germany	Brandenburg University of Technology Cottbus–Senftenberg
Radovan Stojanovic	Montenegro	University of Montenegro
Radu Grosu	Austria	TUW
Raul Gomez	Spain	University of Cantabria
Salim Chehida	France	Université Grenoble Alpes
Sara Pettinari	Italy	UNICAM - University of Camerino
Stefan Mirkovic,	Serbia	SMART4ALL, FTN University of Novi Sad, Serbia
Stratos Tiganourias	Greece	SMART4ALL Project, ESDA LAB, University of Peloponnese
Sujay Narayana	Netherlands	Delft University of Technology
Tanja Radovanovic	Montenegro	MECOnet
Vijay Kumar	India	Indian Institute of Technology Delhi, India
Vincenzo Stoico	Italy	University of L'Aquila
Virtyt Lesha	Albania	Metropolitan University of Tirana
Zenepe Satka	Sweden	Mälardalen University



CPS&IoT

Certificate of Attendance

SMART4ALL

THIS ACKNOWLEDGES THAT

Marko Markovic

Montenegrin Association for New Technologies – MANT, Montenegro

has successfully attended

The ***2nd Summer School on***

Cyber Physical Systems and Internet of Things (SS-CPSIoT'2021)

(3 ECTS)

in Budva, Montenegro, June 07-10 2021

On behalf of the organizers:

Prof. dr. Lech Jozwiak Lech Józwiak

Prof. dr. Radovan Stojanović

Prof. dr. Betim Cico

Prof. dr. Budimir Lutovac Lutovac

Author Index

CPS&IoT'2021
Summer School on Cyber-Physical Systems and Internet-of-Things
Budva, Montenegro, June 7-10, 2021

Citation:

Lech Jóźwiak, Radovan Stojanović, Proceedings of Summer School on Cyber-Physical Systems and Internet-of-Things, Vol. II, MECOnet, 2021

Publishers:

MECOnet Institute (Mediterranean Excellence in Computing and Ontology),www.meconet.me

Montenegrin Association for New Technologies - MANT, www.mant

Year/Place: Montenegro, Podgorica, 2021