



## D13.2

### MILS: Business, Legal and Social Acceptance

<b>Project number:</b>	31835
<b>Project acronym:</b>	EURO-MILS
<b>Project title:</b>	EURO-MILS: Secure European Virtualisation for Trustworthy Applications in Critical Domains
<b>Start date of the project:</b>	1st October, 2012
<b>Duration:</b>	42 months
<b>Programme:</b>	FP7/2007-2013

<b>Deliverable type:</b>	Report
<b>Deliverable reference number:</b>	ICT-318353 / D13.2/ 1.0
<b>Activity and Work package contributing to the deliverable:</b>	Activity A1 / WP 1.3
<b>Due date:</b>	SEPT 2015 – M36
<b>Actual submission date:</b>	30 <sup>th</sup> September 2015

<b>Responsible organisation:</b>	JR
<b>Editor:</b>	Christophe Toulemonde
<b>Dissemination level:</b>	PU
<b>Revision:</b>	1.0

<b>Abstract:</b>	Final report on EURO-MILS Work Package 13 Business, Legal and Social Acceptances
<b>Keywords:</b>	Virtualisation, MILS, security, safety, trustworthiness

## **Editor**

Christophe Toulemonde, JR

## **Contributors**

Jacques Brygier (SYSF),

Holger Blasum, Sergey Tverdyshev (SYSGO),

Bertrand Leconte (AOS),

Kevin Müller (EADS IW),

Axel Söding-Freiherr von Blomberg (OPSYN),

Igor Furgel (TSYS),

Martina Truskaller (TEC)

## **Disclaimer**

“This project has received funding from the European Union’s Seventh Framework Programme for research, technological development and demonstration under grant agreement n° 318353”.

This document has gone through the consortium’s internal review process and is still subject to the review of the European Commission. Updates to the content may be made at a later stage.

## Executive Summary

This document is the result of EURO-MILS Work Package 1.3. The objective of the WP is to analyse the business impact of trustworthy ICT for networked high-criticality systems. A multistep work has been done to make a quantitative and qualitative analysis of the different markets and understand the potential of exploitation. It has analysed how security requirements vary from a business (companies) and a social (consumer) point of view. It has analysed the legal implications (national certification authority) of high-assurance cross-European certification.

During the project, we have performed the following tasks:

1. We started the analysing by studying the business requirements and values for multiple independent levels of security in the core markets, defence, avionic, and automotive those require virtualised high-demand critical systems. For that matter, we interviewed face to face the business partners of the project. Along with defining their business requirements, they help to define a questionnaire that has been used in the following steps.
2. We extended the analysis to adjacent markets such as medical, finance, utilities, industries network and communication. All these market deploy embedded systems with high level of security. For example, medical devices become more sophisticated and need to integrate wireless communication, security protocols, USB connectivity, persistent storage, and portable touch screens. Smart meters are being deployed by utility companies in client house and need embed security mechanisms such as worm prevention, or end-to-end data encryption. As Information security research is one of the most intrusive types of organisation research<sup>1</sup>, we have focused on a few, selected firms with whom the project team members have developed an excellent rapport and trust. To interact with the selected professionals in the adjacent markets, we ran phone interviews and web surveys. We leveraged the questionnaire elaborated in step 1.
3. We then finish the evaluation in analysing the business impacts and requirement in the consumer market, for example mobile devices. Today, mobile phones run complex multimedia operating systems and require an environment that guarantees the security of critical information and applications without compromising the user experience. We setup a web survey to interact with professionals in enterprises and governments. A partnership with a specialised press media has been established to extend the market responses to the consumer space. To consolidate the results of the study, we ran a Big Data analysis to listen to potential consumers.
4. We analysed legal implications of trustworthy ICT for networked high-criticality systems. In this project, we worked on standardisation to provide an abstract description (“Protection Profile”) of the concrete MILS implementation in the Common Criteria for Information Technology Security (CC) framework. In the context of this project, we therefore analysed the economic value of standardisation and tried to confirm results coming out previous studies such as “Economic benefits of standardization” (Commissioned by DIN in 2000) or “The Empirical Economics of Standards” (Commissioned by the UK Department of Trade and Industry in 2006).

The following document represents the results of these tasks.

- Part I defines the project terminology. As often in information and telecommunications technologies, generic concepts as trustworthiness, security, and safety have different

---

<sup>1</sup> Kotulic2003, “Why there aren’t more information security studies”

meanings for markets, providers and consumers. The meaning of the terms varies considerably from one context to another. So, it is an important starting point to define the common vocabulary when discussing with experts in different technical domains or even with simple end-user consumers.

- Part II presents the results of the business impact analysis of MILS cross-sectorally beyond the avionics and automotive sectors. MILS is a platform that allows the horizontal integration, which is more open than vertically stacked products. In every industry sector, a trend to such horizontal platforms has been observed. We investigated the business value of a trustworthy ICT from a horizontal platform perspective and identified market requirements of MILS systems
- Part III presents the results of the social impact analysis with a strong focus on consumers. Using a survey, we questioned consumers on their security awareness and practices. We wanted to understand the main security expectations when buying and using a connected device such as a smartphone. We also listened to what consumers were saying on the connected device and security theme using a Big Data analysis. .
- Part IV presents the results of the legal impact analysis of a certified platform with a specific focus on the new paradigm of the Internet of Things and its legal implications and issues.
- Part V concludes this work.

# Contents

<b>Part I: Common Definitions .....</b>	<b>1</b>
<b>Chapter 1 Introduction .....</b>	<b>2</b>
<b>Chapter 2 Trustworthiness, EURO-MILS Project Value.....</b>	<b>4</b>
2.1 Safety.....	4
2.2 Security .....	5
2.3 Trustworthiness (also known as Dependability) .....	7
2.3.1 Ensuring Trustworthiness.....	9
2.3.2 Risks Management .....	10
2.4 Others Security Concepts .....	12
2.5 Safety vs. Security .....	12
2.5.1 IT Safety and IT Security.....	13
2.5.2 Avoiding Ambiguities: SEMA Framework .....	14
<b>Chapter 3 Trustworthiness by Design, Technology Concepts .....</b>	<b>16</b>
3.1 What is a System? .....	16
3.2 System of Systems .....	16
3.3 Embedded System.....	18
3.3.1 Definition.....	18
3.3.2 Characteristics .....	19
3.3.3 Real Time and RTOS.....	20
3.3.4 Internet of Things .....	21
3.3.5 Critical Infrastructure .....	22
3.4 Virtualization: Improving Resource Utilization .....	22
3.4.1 Virtualization Types.....	23
3.4.2 Virtualization Techniques .....	24
3.4.3 Embedded Virtualization .....	25
3.4.4 Virtualization Value .....	26
3.5 MILS: High-Assurance Security Architecture .....	26
3.5.1 MILS Definition.....	27
3.5.2 MILS Characteristics .....	27
3.5.3 From MLS to MILS .....	28
3.5.4 Security Using Separation Microkernel.....	29
<b>Chapter 4 Trustworthiness by High Assurance: Certification Environment .</b>	<b>30</b>

4.1	Do we need Standards? .....	30
4.1.1	Standards Value .....	30
4.1.2	International Standard Organizations .....	31
4.1.3	Main Security and Safety Standards .....	32
4.2	Security Standards.....	34
4.2.1	ISO/IEC 15408 (Evaluation Criteria for IT Security).....	34
4.2.1.1	<i>Evaluation Assurance Levels</i> .....	35
4.2.1.2	<i>Target of Evaluation, Protection Profiles, and Security Target</i> .....	36
4.2.2	ISO/IEC ISMS Information Security Management System family of standards.....	37
4.2.3	FIPS-140-2 .....	38
4.3	European Privacy Seal .....	38
4.4	Safety Standards .....	39
4.4.1	Avionic Safety Standard: DO-178B Certification Standard .....	39
4.4.2	IEC 61508: Functional Safety for Electronic Devices.....	40
4.4.3	EN 50128 Certified Software for Railways Applications.....	40
4.4.4	ISO 26262 Certification for Automotive Appliances .....	40
4.4.5	IEC 62304: Certification for Medical Devices.....	40
<b>Part II: Business Value .....</b>		<b>41</b>
<b>Chapter 5 Trustworthiness by Business Acceptance: Market Value .....</b>		<b>42</b>
5.1	EURO-MILS Business Justification.....	42
<b>Chapter 6 EURO-MILS Business Values.....</b>		<b>44</b>
6.1	Reliable Embedded Platforms .....	44
6.1.1	Different Domains Share Common Characteristics and Requirements.....	44
6.1.2	Embedded Platforms Are Used Everywhere .....	46
6.1.3	Embedded System Market Description .....	48
6.2	Targets, Constraints, and Requirements of Reliable Embedded Platforms ...	49
6.2.1	Criticality .....	50
6.2.2	Quality of service .....	51
6.2.3	Time-to-market.....	51
6.2.4	Costs .....	51
6.3	Ensuring Security .....	52
6.3.1	Key stakeholders .....	52
6.3.2	Dealing with certification .....	54
6.3.3	Security Market Trends .....	55
6.4	Virtualization for Building Independent Partitions.....	55
6.5	Certification To Increase User Confidence .....	56



- 6.5.1 A Key Security Standard .....56
- 6.5.2 Stakeholders Business Value.....57
- Chapter 7 Understanding Markets Requirements..... 58**
- 7.1 Industry Panel..... 58
  - 7.1.1 Creation .....58
  - 7.1.2 Industry Panel Statistics .....59
  - 7.1.3 Interviews.....59
  - 7.1.4 Additional contacts.....60
- 7.2 Data collection and analysis ..... 60
- Chapter 8 EURO-MILS General Perception ..... 62**
- 8.1 On Security and Safety ..... 62
  - 8.1.1 Despite Understanding Ambiguities, Security And Safety Become Key Requirements .....62
  - 8.1.2 Systems Are Crossing The Line Toward Criticality .....62
  - 8.1.3 Some Markets Make Security A Priority .....63
  - 8.1.4 Consumers Do Not Care About Safety And Security .....63
  - 8.1.5 How To Create Secure Products Without Slowing Down Business? .....64
  - 8.1.6 Data Privacy Will Impose Security In Consumer Products .....64
  - 8.1.7 Internet Of Things Will Have A Big Impact On Communication Security Requirements .....64
  - 8.1.8 Fear Is A Good Motivation For Safety And Security .....65
- 8.2 On Platform Virtualization and Partitioning ..... 65
  - 8.2.1 It Is Becoming A Norm To Operate Independent Software Stacks With Different Criticalities On A Same Platform.....65
  - 8.2.2 Leveraging Hardware Security Capabilities May Be Complex .....66
  - 8.2.3 Complexity Can Be A Barrier .....66
  - 8.2.4 High Volume Markets Need To Keep Costs Under Control .....67
- 8.3 On User Acceptance and Certification ..... 67
  - 8.3.1 Consumers Don't Get Security .....67
  - 8.3.2 User Acceptance Do Not Imply Certification.....68
  - 8.3.3 Costs And Length Of Certification Vs. Security Requirements .....68
  - 8.3.4 Complexity Of Certification.....69
- Chapter 9 EURO-MILS Industry Views..... 71**
- 9.1 Home Automation ..... 71
  - 9.1.1 Market description.....71
  - 9.1.2 Market Size and Projections.....72
  - 9.1.3 Home Automation Market Players.....73

9.1.4	Market and EURO-MILS Adherence .....	74
9.1.4.1	<i>Virtualization Value</i> .....	74
9.1.4.2	<i>Security Value</i> .....	74
9.1.4.3	<i>Certification Value</i> .....	75
9.2	Smart Meter .....	76
9.2.1	Market description.....	77
9.2.2	Market Size and projections .....	77
9.2.3	Market Players .....	78
9.2.4	Market and EURO-MILS Adherence .....	79
9.2.4.1	<i>Virtualization Value</i> .....	79
9.2.4.2	<i>Security Value</i> .....	80
9.2.4.3	<i>Certification Value</i> .....	80
9.3	Healthcare Information Technology .....	81
9.3.1	Market description.....	81
9.3.2	Market Size and projections .....	83
9.3.3	Market Players .....	84
9.3.4	Market and EURO-MILS Adherence .....	86
9.3.4.1	<i>Virtualization value</i> .....	86
9.3.4.2	<i>Security value</i> .....	86
9.3.4.1	<i>Certification Value</i> .....	87
9.4	Mobile .....	87
9.4.1	Market description.....	87
9.4.2	Market Size and projections .....	88
9.4.3	Market Players .....	89
9.4.4	Market and EURO-MILS Adherence .....	91
9.4.4.1	<i>Security Value</i> .....	92
9.4.4.2	<i>Certification Value</i> .....	92
9.4.4.3	<i>Virtualization Value</i> .....	93
9.5	Industrial Control Systems .....	94
9.5.1	Market description.....	94
9.5.2	Market Size and projections .....	96
9.5.3	Market Players .....	97
9.5.4	Market and EURO-MILS Adherence .....	97
9.5.4.1	<i>Security Value</i> .....	98
9.5.4.2	<i>Certification Value</i> .....	99
9.5.4.3	<i>Virtualization Value</i> .....	99
<b>Part III: Social Acceptance .....</b>		<b>100</b>
<b>Chapter 10</b>	<b>Social Survey: Questioning the Consumers .....</b>	<b>101</b>



10.1	Social Survey Methodology .....	101
10.2	Social Survey Questionnaire .....	103
10.2.1	English Version of the Social Survey Questionnaire .....	103
10.2.2	Sample of the On-line Version of the Social Survey Questionnaire .....	108
10.3	Social Survey Demography .....	109
10.4	Social Survey Analysis .....	112
10.4.1	Security Awareness .....	112
10.4.2	Security Practices .....	113
10.4.3	Personal Data Protection .....	114
10.4.4	Confidence in Security Mechanisms.....	115
10.4.5	Criteria of Choice .....	116
10.4.6	Main Security Expectations .....	117
10.4.7	Trust in Data Privacy Enforcement.....	120
10.4.8	Decision Factor .....	121
10.4.9	Trust in Technologies.....	122
10.4.10	Security Mechanisms Awareness.....	123
<b>Chapter 11</b>	<b>Big Data Analysis: Listening to the Consumers.....</b>	<b>124</b>
11.1	Big Data Analysis Methodology.....	124
11.1.1	What is Big data .....	125
11.1.2	Digital Insighters .....	125
11.1.3	Collected big data .....	126
11.1.4	Listening to Customer Analysis .....	126
11.2	First Iteration: Connected Device Online Conversations .....	127
11.3	Second Iteration: The Smartphone Customer Journey .....	128
11.3.1	Mention, Upstream, and Media: Explaining the Results.....	131
11.3.2	Research: Exploring the Results .....	132
11.4	Focus on Operating Systems .....	133
11.5	Security Sensibilities in the Automotive Industry .....	135
<b>Part IV:</b>	<b>Legal Implications .....</b>	<b>138</b>
<b>Chapter 12</b>	<b>EURO-MILS and Internet of Things.....</b>	<b>139</b>
12.1	Internet of Things .....	139
12.2	IoT Risks .....	139
12.3	Legal Issues .....	140
12.4	Potential Answers.....	140
12.5	EURO-MILS Platform Ready for a Safe and Secure IoT .....	141
<b>Part V:</b>	<b>Conclusion .....</b>	<b>143</b>

## List of Figures

Figure 1: Trustworthy and Security Attributes of the EURO-MILS platform .....	9
Figure 2: Trustworthiness and Security Tree .....	10
Figure 3 : Most frequent words found in definitions of Safety .....	12
Figure 4: Most frequent words found in definitions of Security .....	13
Figure 5: Relationship between IT Safety and Security.....	13
Figure 6: SEMA Referential Framework .....	15
Figure 7 : Embedded System, System, and System of Systems .....	17
Figure 8: Virtualization.....	23
Figure 9 : Hypervisor Types.....	24
Figure 10: Simplified Timeline of Type-1 Hypervisors.....	25
Figure 11: Multiple Independent Levels of Security Architecture.....	28
Figure 12 : Working Areas of International Standard Organizations.....	31
Figure 13 : CC Certified Products by Category (source Common Criteria) .....	34
Figure 14: Certified Products by European Countries.....	36
Figure 15: Protection Profile, Security Target and Target of Evaluation Relationship - Simplified (source: Common Criteria) .....	37
Figure 16: EURO-MILS Value Propositions .....	43
Figure 17: Domains of Embedded System Applications .....	48
Figure 18: Embedded Technology Market.....	48
Figure 19: Security Value Chain .....	52
Figure 20 : Embedded Systems Usage (source VDC 2007) .....	55
Figure 21: Industry Panel Invitation .....	58
Figure 22 : Industry Panel Statistics .....	59
Figure 23: Industry Panel Markets.....	59
Figure 24 : Impact on Costs and Schedules of CC Evaluations .....	69
Figure 25 : Smart Meter Linking Consumers To Producers .....	76
Figure 26: Functional Requirements For Energy Smart Metering System.....	79
Figure 27: Security Compliance Framework .....	80
Figure 28: eHealth services.....	82
Figure 29 : French Electronic Medical Record .....	83
Figure 30: Top Five Smartphone Vendors, Q3 2014 – Source IDC .....	89
Figure 31: FY 2014 incidents reported by sector (245 total) - Source: ICS-CERT.....	98
Figure 32: Social Survey Call To Action .....	102

Figure 33: Social Survey Introduction Page.....	102
Figure 34: On-line Questionnaire (Page 1-a).....	108
Figure 35: On-line Questionnaire (Page 1-b).....	109
Figure 36: Security Awareness.....	112
Figure 37: Security Practices.....	113
Figure 38: Personal Data Protection.....	114
Figure 39: Confidence in Security Mechanisms.....	115
Figure 40: Criteria of Choice for a New Connected Device.....	116
Figure 41: Trust in Data Privacy Environment.....	120
Figure 42: Decision Factors.....	121
Figure 43: Trust in Technologies.....	122
Figure 44: Security Mechanism Awareness.....	123
Figure 45: From Awareness to Protection.....	127
Figure 46: Conversation Chronology.....	128
Figure 47: Smartphone Customer Journey.....	129
Figure 48: Smartphone Customer Journey in France.....	130
Figure 49: Smartphone Customer Journey in Germany.....	130
Figure 50: Smartphone Customer Journey in the UK.....	131
Figure 51: Influent Web Sites in Germany and France.....	132
Figure 52: Purchase Criteria by Country.....	132
Figure 53: Total Mentions of Security in Conversations.....	133
Figure 54: Security Perception of Operating Systems.....	134
Figure 55: Security Perception of Operating Systems – Verbatim.....	134
Figure 56: Conversations about Cars and Security.....	135
Figure 57: Conversations about Smartphone and Security.....	135
Figure 58: Weekly Evolution of Security Mentions in Online Car Conversations.....	136
Figure 59: Weekly Evolution of Security Mentions in Online Smartphone Conversations ...	136
Figure 60: EURO-MILS Values by Market Segment.....	143



# List of Tables

Table 1 : ICT Powered Types of System of Systems .....17

Table 2: Virtualization Models.....25

Table 3: Main Security and Safety Standards .....33

Table 4: Embedded Systems Characteristics by Domains.....46

Table 5 : Required Characteristics for Reliable Embedded Systems .....50

Table 6: Worldwide Smartphone Forecast by Shipments, 2014 and 2018 – Source IDC.....88

Table 7: Worldwide Smartphone Forecast by Value, 2014 and 2018 – Source IDC .....89

Table 8: Worldwide Smartphone Sales by OS - Source Gartner Mars 2015 .....90

Table 9: Distinctions between IT and Control Systems .....95

Table 10: Criteria of Choice for a New Device .....117

Table 11: Security Expectations on Selected Connected Devices .....117

## Part I: Common Definitions

As often in information and telecommunications technologies, generic concepts as trustworthiness, security, and safety have different meanings for markets, providers and consumers. The meaning of the terms varies considerably from one context to another.

It is therefore important to define these concepts as it is the starting point of our work and provide the basis of the analysis performed during the project. We also have decided to concentrate on defining the concepts from a business perspective and value.

## Chapter 1 Introduction

*An extract from the EURO-MILS announcement letter says:*

Based on **embedded systems**, cyber-physical networks are part of our society, and gain wider spread and importance. Next generations of aircraft and cars will be tightly interconnected with each other, with the internet, and other infrastructures. The same holds for many industries and areas of our life. Ubiquitous, highly **critical systems** go online and create a domain of mixed-criticalities, where **security** and **safety** requirements of different levels mix. However, state of the art technologies do not provide today secure and safe **trustworthiness** to achieve this interconnection and mixing.

Further, it continues:

The main outcomes of the EURO-MILS project are to develop market relevant technologies and concepts for **virtualisation** of **heterogeneous embedded systems** and the formal verification for those systems as part of rigorous cross-European security certification:

- Trustworthy foundations by the **MILS** approach, architecture, and applications.
- A European MILS virtualisation platform and its usage
- High assurance backed by the “Common Criteria for Information Technology Security” standard
- A true cross-European **certification**

As said in introduction of this part, the meaning of the concepts of trustworthiness, security, and safety varies considerably from one context to another. For example, security is defined as *the prevention and detection of malicious acts* by the nuclear industry<sup>2</sup> where ISO adds accidental actions to its security definition for computers<sup>3</sup>. Also the use of the terms varies also from a language to another. In France, the airline crew members are in charge of the *sécurité à bord* which translates to *inflight safety*. Therefore it may lead to ambiguities which become problematic in critical environments such as avionic or automotive.

Other terms such as Common Criteria, certification or MILS may be obvious from domain specialists but are unclear for the general reader interested in the outputs of the EURO-MILS project.

It is therefore important to define these concepts and terms as they are the starting point of our work. Defining the project terminology and glossary allows members of the EURO-MILS project to discover and to reduce potential ambiguities, and to ensure a consistent, complete and common understanding of the terms.

Another objective is to prepare a business analysis of the project value. Sharing a common definition of these concepts and terms allows us to discuss with subject matter experts in other industries such as health care, energy, or telecommunications and avoid misunderstanding derived from different meanings and ambiguities.

---

<sup>2</sup> “IAEA Safety glossary: terminology used in nuclear safety and radiation protection: 2007 edition.” — Vienna: International Atomic Energy. Agency, 2007

<sup>3</sup> “Information technology — Vocabulary — Part 8: Security” - ISO/IEC 2382-8

In the following chapters, we define concepts and terms that are the core of the EURO-MILS project. As the project value is organized around trustworthiness, we organise the definitions in the respective chapters:

- Trustworthiness, EURO-MILS project value
- Trustworthiness by design: Technology concepts
- Trustworthiness by high assurance: Certification environment
- Trustworthiness by Business, Legal, and Social acceptance: Market value.

## Chapter 2 Trustworthiness, EURO-MILS Project

### Value

This chapter aims to give precise definitions characterizing the various concepts that come in play with the EURO-MILS project. It is important to clarify the concepts as we apply them for critical, highly interconnected complex systems used in diverse industries where security and safety requirements are different.

#### trustworthiness

##### Web definitions

the trait of deserving trust and confidence.

[wordnetweb.princeton.edu/perl/webwn](http://wordnetweb.princeton.edu/perl/webwn)

### 2.1 Safety

The new Oxford dictionary of English<sup>4</sup> describes safety as:

The condition of being protected from or unlikely to cause danger, risk, or injury.

Safety can also denote something designed to prevent injury or damage (e.g. safety barrier). It also adds a definition of safe:

1) Protected from or not exposed to danger or risk; not likely to be harmed or lost

(Not likely to cause or lead to harm or injury; not involving danger or risk)

2) Uninjured; with no harm done

System Safety

Safety is the inability of the environment to affect the system in an undesirable way.

Safety is the state of being "safe", the condition of being protected against physical, social, spiritual, financial, political, emotional, occupational, psychological, educational or other types or consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable.

Safety should be regarded as a relative term. Using a strict definition, any system that presents an element of risk is unsafe. No aircraft could fly, no automobile move and no train put on rail if all hazards had to be eliminated first. The problem is even exacerbated by the

---

<sup>4</sup> New Oxford dictionary of English - Pearsall and Hanks, 2001



fact that attempts to eliminate a risk often result in risk displacement rather than risk elimination.

### Safety and Safety-critical systems

Safety-critical systems are systems whose failure could endanger human life, lead to substantial economic loss, or cause extensive environmental damage.

If the failure of a system could lead to unacceptable consequences, then the system is safety-critical. In essence, a system is safety-critical when we depend on it for our well being.

Areas such as medical care, commercial aircraft, and nuclear power have traditionally considered safety-critical systems. Failure in these areas can quickly lead to human life being put in danger and loss of equipment. Other examples are transportation control, banking and financial systems, electricity generation and distribution, telecommunications, and the management of water systems. All of these applications are extensively computerized, and computer failure can and does lead to extensive loss of service with consequent disruption of normal activities.

## 2.2 Security

Close concept to safety, there is an immense literature on the definition and categorization of security. The Oxford English Dictionary defines security as:

The state of being free from danger or threat.

Security applies to many realms, from physical range (airport, food...), political fields (homeland, public security), monetary disciplines (financial security), and information technology domains.

### System security

Security is the inability of the system to affect its environment in an undesirable way.

Security is difficult to ensure as in most security systems, the "weakest link in the chain" is the most important. The situation is asymmetric since the 'defender' must cover all points of attack while the attacker need only identify a single weak point upon which to concentrate.

### Information Security

In the IT world, experts on security concentrate on how to secure information. Wikipedia defines Information Security as:

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

In publications, the terms information security, computer security and information assurance are frequently used interchangeably as these fields are interrelated and share the common goals of protecting information.

Defining computer security, the International Standard Organization explains that actions can be accidental or malicious<sup>5</sup>:

---

<sup>5</sup> "Information technology — Vocabulary — Part 8: Security" - ISO/IEC 2382-8

The protection of data and resources from accidental or malicious acts, usually by taking appropriate actions. These acts may be modification, destruction, access, disclosure, or acquisition, if not authorized.

And the Computer Service Division of the NIST has worked in defining the security concepts more precisely<sup>6</sup>:

The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

Information or computer security is the protection of information and information systems. It is a composite concept requiring the concurrent existence of:

- *Confidentiality*: A requirement that private or confidential information not be disclosed to unauthorized individuals.
- *Integrity*: Information has integrity when it is timely, accurate, complete, and consistent.
- *Availability*: A requirement intended to assure that systems work promptly service is not denied to authorized users.

Note: The CIA triad of **confidentiality**, **integrity**, and **availability** is at the heart of information security. The members are interchangeably referred to in the literature as security attributes, properties, security goals, fundamental aspects, information criteria, critical information characteristics and basic building blocks.)

There are also some additional attributes that can be defined:

- *Accountability*: availability and integrity of the person who performed the operation
- *Authenticity*: integrity of a message content and origin, and possibly of some other information, such as time of emission
- *Non-repudiability*: availability and integrity of the identity of the sender or receiver of a message

End-users require security

From an end-user perspective, securing an embedded device (such as a smartphone) requires security functions to ensure the confidentiality, integrity, and availability requirements:

- User Identification function to restrict the use of the system to a selected set of authorized users
- Secure Network Access function to authorize accessing the network
- Security functions such as authentication and access control mechanisms
- Availability functions preventing malicious entities to degrade or block the service
- Content Security functions, to protect critical or sensitive information throughout its lifetime, including erasing at the end of its lifetime.
- Secure Storage function, to secure information in the embedded system's storage devices, external or internal

---

<sup>6</sup> NIST Publication 800-12: [An Introduction to Computer Security: The NIST Handbook](#)

- Tamper resistance function, to maintain these security functions even when the device falls into the hands of malicious parties.

### Importance of Security for embedded systems

Security issues are not new for embedded system but could prove a more difficult problem than security does for enterprise computing although both environments are tightly linked. Today more embedded systems are connected to the Internet and exchange information with enterprise IT systems and industrial control systems, the potential damages from security vulnerabilities scale up dramatically. Home appliances are internet-enabled, hospital use wireless IP network for patient equipment's, cars have indirect connections to safety-critical control systems, and planes are now outfitted with either 3G cellular service or satellite delivery systems, for downloading movies or sending emails.

## 2.3 Trustworthiness (also known as Dependability)

The EURO-MILS project is working on a “Secure European Virtualization for Trustworthy Applications in Critical Domains”. It leverages a security architecture that supports the coexistence of untrusted and trusted components. For example, in a car, a system that runs non-trusted applications (e.g. a music player on a Linux operating system), medium critical applications (e.g. advanced driver assistance systems such as the GPS), and highly-critical application (e.g. AUTOSAR real-time application that deal with car performance and safety).

But what are the characteristics of trustworthy applications? What is trustworthiness in this context?

The Merriam-Webster online dictionary defines the adjective trustworthy as:

“worthy of confidence, dependable”.

More precisely, in the context of the work programme 2011 for the ICT theme of the FP7 Specific Programme 'Cooperation' which funds the EURO-MILS project, the European Commission defines trustworthy as:

secure, reliable and resilient to attacks and operational failures; guaranteeing quality of service; protecting user data; ensuring privacy and providing usable and trusted tools to support the user in his security management

In the EURO-MILS project, we use the following definition based on the dependability definition of Laprie<sup>7</sup>:

Trustworthiness is the ability for a system to deliver service that can justifiably be trusted.

### Trustworthiness or Dependability?

Synonym of reliable and contrary of uncertain, a trustworthy system is capable of being dependable upon.

In a related paper<sup>8</sup>, Jean-Claude Laprie explains that the dependability concept is very similar to trustworthiness. A side-by-side comparison leads to the conclusion that both

---

<sup>7</sup> A. Avizienis, J.C. Laprie, B. Randell, C.Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", *IEEE Transactions on Dependable and Secure Computing*, Vol.1, No.1, Jan-March 2004

<sup>8</sup> A. Avizienis, J.C. Laprie , B. Randell, “Dependability and Its Threats: A Taxonomy”, *IFIP Congress Topical Sessions 2004: 91-120*

concepts are equivalent in their goals and address similar threats. Trustworthiness was used in a US-based study where dependability is more an European term.

In our document we consider that the terms trustworthiness and dependability are equivalent. We nevertheless use the term trustworthiness as it refers to the title of our project “*Secure European virtualization for trustworthy applications in critical domains*”.

#### Trust or Trustworthy?

It is important to note that trust and trustworthiness are different. A disgruntled R&D employee working on a strategic project who sells an enterprise trade secret to a competitor can be qualified as ‘trusted but not trustworthy’. The US National Security Agency (NSA) defines a trusted computer system or component as one “whose failure can break the security policy”, and a trustworthy system or component as one “that will not fail”. A trusted system therefore is one where trust is used to describe a role, irrespective of whether a system is able to perform adequately in that role, whereas trustworthy is used to describe the adequacy of a system to perform as expected.

Trust may exist where there is no evidence to justify the reliance placed in the system, whereas trustworthiness suggests that there are assurance criteria to justify the confidence in the system. In our project, the Common Criteria certification will be the assurance, the guarantee, that the system will perform correctly, as expected.

#### Trustworthy System

Trustworthy systems do what users expect (and not something else) despite environmental disruption, human user and operator errors, attacks by hostile parties, and system design and implementation errors.

A trustworthy system encompasses the following attributes<sup>7</sup>:

- Availability: readiness for correct service.
- Reliability: continuity of correct service.
- Safety: absence of catastrophic consequences on the user(s) and the environment.
- Integrity: absence of improper system alterations.
- Maintainability: ability to undergo modifications and repairs.

#### Trustworthy Information System

The EURO-MILS project works on a trustworthy technology applied to computers and the focus is about information management. Therefore we can refine our definition in the field of ICT:

Applied to computing technology, trustworthy systems are information and communication systems that are reliable, usable, interoperable, and secure. They are systems that can justifiably be trusted.

#### EURO-MILS: A trustworthy environment

In chapter 2.2, page 5, we elaborate on security. The EURO-MILS project will provide a trustworthy and secure ICT environment. As in the EU definition cited before, we need to add the key attribute of security in our definition because security is often considered<sup>9</sup> as an inseparable characteristic of a trustworthy computer system<sup>6</sup>.

---

<sup>9</sup> For example, the Trustworthy Information Systems program of the National Institute of Standards and Technology (NIST) works on “the development and deployment of information and communication systems that are reliable, usable, interoperable, and secure”.

To present the EURO-MILS environment, trustworthiness must be combined with security. We introduce the new attribute of confidentiality and adapt the previous integrity and availability definitions in the context of information security:

- Confidentiality: information is prevented from disclosure to unauthorized individuals or systems
- Integrity: information has not been modified inappropriately
- Availability: information is accessible to authorized individuals or systems at all times

The EURO-MILS project will develop an environment that supports applications with the trustworthiness and security attributes as shown in Figure 1.



Figure 1: Trustworthy and Security Attributes of the EURO-MILS platform

### 2.3.1 Ensuring Trustworthiness

It is difficult to ensure trustworthiness. Systems are composed of multiple components. Design and implementation errors must be avoided, eliminated, or somehow tolerated. It is not sufficient to address only some of these diverse dimensions, nor is it sufficient simply to assemble components that are themselves trustworthy. Often using commercial off-the-shelf components, system developers have neither control nor detailed information about many of their system's components. Tools used to support the development of the components (such as a compiler) become critical in ensuring the dependability of the system. Integrating the components and understanding how the trustworthiness dimensions interact is a central challenge in building a trustworthy system. Moreover, as components' functionalities can be extended or replaced after deployment (using "plug-and-play" or other extensible operating system features), system designers cannot know what actions those components might take.

#### Faults, errors, and failures

Threats to trustworthiness and security are faults caused by errors leading to a system failure. A trustworthy system delivers correct services. Working on such systems, developers need to understand and specify which faults (internal or external to the system) will cause errors that may lead to failures preventing the system to deliver a correct service. To attain trustworthiness and security, many means have been developed. They can be grouped in four major categories:

- Prevention, to prevent the occurrence or introduction of faults.
- Tolerance, to avoid services failures in the presence of faults.
- Removal, to reduce the number and severity of faults.
- Forecasting, to estimate the present number, the future incidence and the likely consequence of faults.

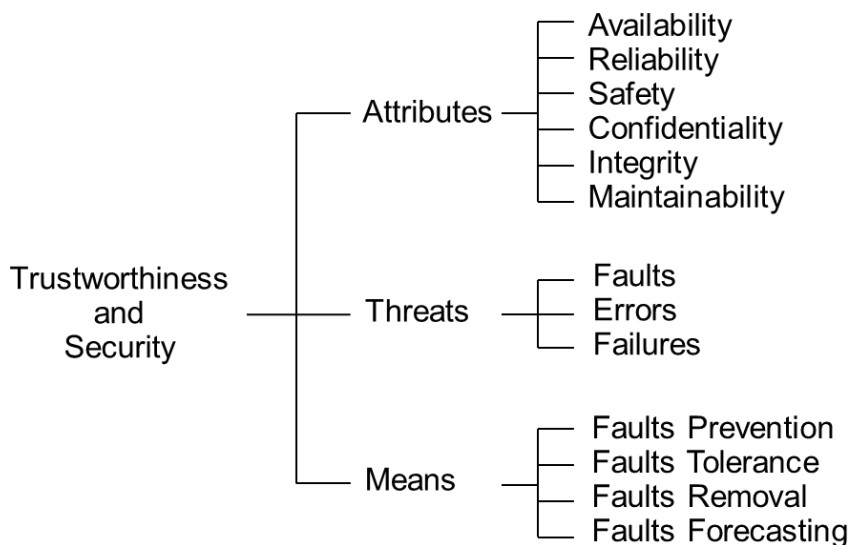


Figure 2: Trustworthiness and Security Tree

A vulnerability is a property of a system or its environment, which, in conjunction with an internal or external threat, can lead to a failure.

### 2.3.2 Risks Management

As the most secure and safe system is a system that does nothing, security is often associated with the notion of risk. A risk can be defined as follow:

A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through pre-emptive action

Companies face three basic types of risks:

- External risks for data breaches occur when someone outside the organization “breaks into” the organizations information network to try to secure items of value
- Internal risks for data security focus on when an organization’s employees or authorized users access the information network to secure personal information for their own benefit.
- Human error risks create security breaches. An information security network may be improperly designed or implemented leaving some employees at risk for error and causing harm to the organization. Even if network security controls are in place, employees or authorized affiliates or third parties can make mistakes.

The objective of risk management is to identify, analyze and mitigate risks to an acceptable or tolerable level.

What is a trustworthy car?

A trustworthy system needs to perform correctly as expected. We expect for a car that it will provide the service of transporting us at home. To perform correctly, the car has the following attributes:

Availability,

The car is able to be used or obtained.



Reliability

The car is able to provide the service. It performs and maintains its functions in routine or unexpected circumstances

Safety

The car provides safety for the driver



Integrity

The car is a whole and undivided

Maintainability

The car is capable of being maintained



## 2.4 Others Security Concepts

For the completeness of the discussion, we can also cite additional concepts recur throughout different fields of security:

- Assurance - assurance is the level of guarantee that a secure system will behave as expected
- Countermeasure - a countermeasure is a way to stop a threat from triggering a risk event
- Defence in depth - never rely on one single security measure alone
- Exploit - a vulnerability that has been triggered by a threat - a risk of 1.0 (100%)
- Threat - a threat is a method of triggering a risk event that is dangerous
- Vulnerability - a weakness in a target that can potentially be exploited by a security threat

## 2.5 Safety vs. Security

Safety and security are words that seem clear and precise at first glance, but their meaning varies considerably from one context to another.

At a linguistic level, the common phrase 'safe and secure' indicates a limited distinction and, in German, no real distinction can be made as the term *Sicherheit* means both safety and security. Sometimes (e.g. in the appendix of Laprie, p. 264), the term “Vertraulichkeit” is used. For French, Laprie (ibid.) suggests “sécurité-confidentialité”.

To analyse the ambiguities between security and safety, researchers<sup>10</sup> have done a lexicographical analysis of definitions of safety and security. They have analysed a corpus of 89 documents from different industrial sectors. Figure 3 and Figure 4 show the most frequent words used in the definition of respectively safety and security. The safety vocabulary refers to accidental causes and to physical systems. The notion of the environment as opposed to the system under consideration is common in the safety definition.



Figure 3 : Most frequent words found in definitions of Safety

Security definitions often refer to malicious and voluntary action with some specific terms related to information security (e.g., confidentiality, integrity, and availability).

<sup>10</sup> L. Piètre-Cambacédès, C. Chaudet, “The SEMA referential framework – Avoiding ambiguities between security and safety”, *Journal of Critical Infrastructure Protection*, Volume 3, Issue 2, 2010.





Figure 4: Most frequent words found in definitions of Security

### 2.5.1 IT Safety and IT Security

In the context of information technology, a simple research for safety on the Internet shows that this term is defined in terms of security (and vice versa) or even used instead of security. There is ambiguity in the terms.

While safety is protection against hazards (accidents that are unintentional), security is a state of feeling protected against threats that are deliberate and intentional. Safety focuses on unintentional events, while security also focuses on threats coming from outside the system, often caused by malicious parties.

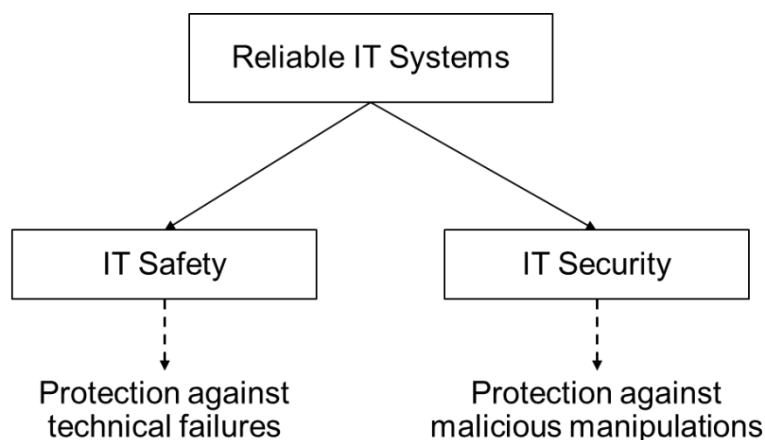


Figure 5: Relationship between IT Safety and Security

But in practice, it is difficult to decide when to use which term. For example, the following problems might be treated as problems of safety or security (or both):

- unauthorized modification to the contents of a ROM in a car Automatic Braking System (ABS) leading to a fatal accident;
- a software design fault in a programmed trading system which causes a bank to buy many times its assets, hence bankrupting the company;
- a syringe pump whose setting was altered by an unauthorized (and untrained) individual to give a fatal dose of drugs;
- A malicious modification of measurements data in a safety-instrumented system leads to unsafe conditions in an industrial infrastructure.

### An automated door: a safety or security feature

There are more diverse and subtler interdependencies to consider. We can illustrate the point using the often-used example of an automated door. A system is in charge of opening and closing an automated door, single entry to an access-restricted zone. From a safety point, the system needs to be designed with a fail-safe behaviour in case of electrical supply failure: the door would fail open in order to ease emergency operations. From a security standpoint, the system would have to be designed with a fail-secure behaviour: the door would remain shut in order to prevent an intrusion, the electrical failure being potentially caused by a malicious action.

When analysing the risks for a system, one should focus on the whole picture — including both safety and security, not just one or the other. By doing so one obtains a complete overview of potential threats/hazards towards a system. Software safety and information security are not separate issues. Information security breaches can compromise the ability of software to function safely, or they can enable misuse of safe software in an unsafe way. Safety breaches can make information security impossible.

## **2.5.2 Avoiding Ambiguities: SEMA Framework**

To establish a common understanding of the terms security and safety and to set a common meaning in different contexts, we propose to use the referential framework called SEMA. This framework allows making the differences underlying the use of the terms "security" and "safety" explicit by a simple graphical notation. It maps the different sectors definitions of security and safety, makes their respective meaning explicit, and reveals inconsistencies and overlaps.

The SEMA framework is based on two important distinctions:

- System versus Environment

Security is concerned with the risks originated from the environment and potentially impacting the system, whereas safety deals with the risks arising from the system and potentially impacting the environment

- Malicious versus Accidental

Security typically addresses malicious risks while safety addresses purely accidental risks

Having identified the distinctions, generic notions of security and safety can be decomposed into sub-notions that are less ambiguous.

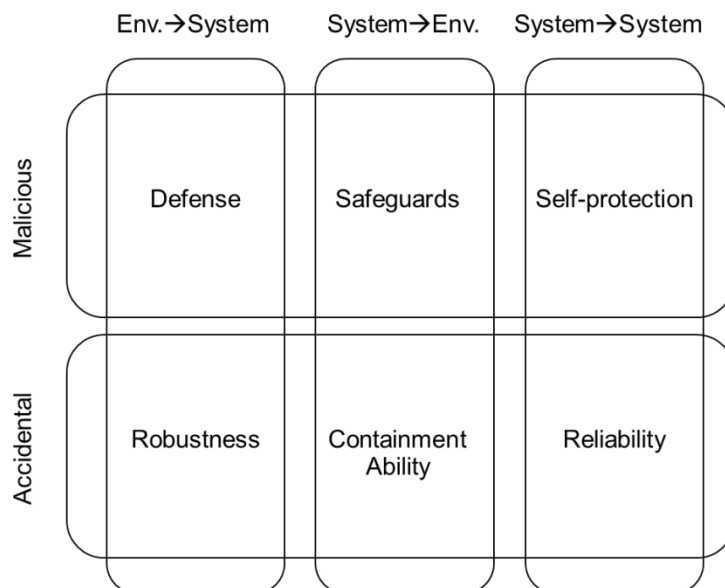


Figure 6: SEMA Referential Framework

Shown in Figure 6, the SEMA framework divides the security and safety space into six distinct sub-notions less ambiguous: defense, safeguards, self-protection, robustness, containment ability and reliability.

## Chapter 3 Trustworthiness by Design, Technology Concepts

The main outcome of the EURO-MILS project is to develop technologies and concepts for virtualization of heterogeneous embedded systems using the MILS architecture. In the following sections, we define each of the terms.

We start defining a computing system used in the IT and enterprise domain. We explain the different techniques for virtualization, a concept well known in the Enterprise IT organizations. We then focus on embedded system with a focus on its real time capabilities. Finally, we explain why MILS, a virtualization architecture for embedded system, is required to ensure the right level of security and safety.

### 3.1 What is a System?

Just for the sake of completeness, it may be useful to define what a system is.

A system is an entity that interacts with other entities, i.e., other systems, including hardware, software, humans, and the physical world with its natural phenomena. These other systems are the environment of the given system. The system boundary is the common frontier between the system and its environment<sup>7</sup>.

For example, a watch is a time display system. It contains hardware, needles, battery, dial, chassis and strap. All needles move clockwise only, the long needle rotates every minute, the short every hour. Every needle returns to the original position after 12 hours...

Another example is a computer. A computer is a computing system that processes information. It includes hardware (central processing unit, memory), peripheral input and output devices. Software (operating system, middleware, applications) makes the computer function.

A system is an entity that interacts with others entities. A computer is a system that processes information.

Computing systems are also characterized by fundamental properties such as functionality, performance, dependability, security, and of course, cost.

### 3.2 System of Systems

As the embedded world meets the internet world there is an increasing number of interacting systems with strong connectivity utilised in both society and in industry. The growing overall complexity of systems has triggered a paradigm shift and the need to enhance the classical view of Complex System Engineering towards System of systems (SoS) Engineering. System-of-Systems describes the large scale integration of many independent self-contained systems to satisfy global needs or multi-system requests.

A System of Systems is a metasystem - multiple embedded and interrelated autonomous complex subsystems - that must function as an integrated complex system to produce desirable results [25].

Examples of ICT system of systems that are found in everyday life are highlighted in Table 1<sup>11</sup>. We find also system of systems in biology, sociological, environmental, organisational and political structures.

System	System of Systems
Car, road	Product range, Integrated Traffic System
Aeroplane	Airport, Air Traffic Control System
Train	Station, Signalling, Rail Network
Wind Turbine	Smart Grid
Building	Town, Shopping Mall
Computer	Distributed IT System

Table 1 : ICT Powered Types of System of Systems

Embedded systems are essential part of a system that participates in a system of systems. Figure 7 illustrates the links between embedded system, a system, and its system of system in an automotive scenario.

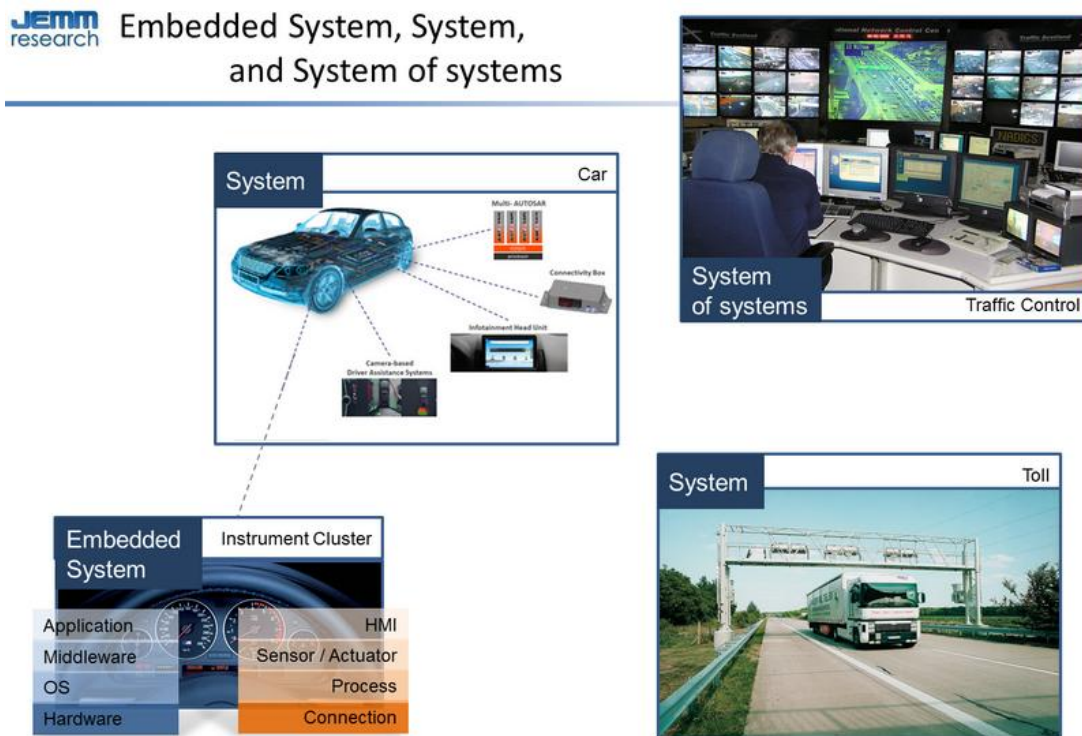


Figure 7 : Embedded System, System, and System of Systems

The overall system has to warrant certain properties: predictable, dependable, safe and secure. And from a security perspective, it is important to notice that a simple security

<sup>11</sup> Source: “[Directions in Systems of Systems Engineering](#)”, July 2012, Unit A3-DG CONNECT, European Commission

vulnerability in an embedded system may compromise the entire security of the system of systems it belongs to.

### 3.3 Embedded System

Most people don't realize that the most common form of computer in use today is by far the embedded computer. In fact, 98% of computing devices are embedded in all kinds of electronic equipment and machines. Computers are moving away from the desktop and are finding themselves in everyday devices like credit cards, mobile phones, cars and planes or places like homes, offices and factories.

Embedded systems are the interface between the physical world and the digital world. They include sensors and actuators to measure and control physical phenomena, such as temperature, traffic, and electricity usage. Embedded systems have local computing power to pre-process raw data and extract salient features in order to reduce communication requirements or to locally process data in order to control actuators.

But before we go further, we need to define what an embedded system is. How does it compare to computers and servers?

#### 3.3.1 Definition

Artemis Joint Undertaking<sup>12</sup> introduces embedded systems<sup>13</sup> with:

Embedded computing systems are made of hardware (nanoelectronic components) and software.

This definition says that an embedded system is a computing system but does not differentiate it from a computer such as a PC or a server. So, we can highlight the difference by saying that an embedded system<sup>14</sup> is

A system whose prime function is not that of information processing, but which nevertheless requires information processing in order to carry out its prime function.

The following definition<sup>15</sup> adds an interesting notion of enclosing product, the host of the embedded system:

Embedded systems can be defined as information processing systems embedded into enclosing products.

And this one<sup>16</sup> specifies the role of monitoring and controlling the physical process:

Embedded software is software integrated with physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa.

In the EURO-MILS project, we define an embedded system as the following:

---

<sup>12</sup> ARTEMIS JU is a public-private partnership for R&D in embedded systems between the European Commission, ARTEMIS Member States, and the ARTEMIS Industry Association, the non-profit Industrial Association

<sup>13</sup> Source: "[What is an Embedded System?](#)", Artemis Web site

<sup>14</sup> A Burns, AJ Wellings, "Real-time systems and programming languages: Ada 95, real-time Java, and real-time POSIX", Pearson Education, 2001

<sup>15</sup> P. Marwedel, "Embedded System Design", Springer-Verlag New York Incorporated, 2005

<sup>16</sup> Edward A. Lee and Sanjit A. Seshia, "Introduction to Embedded Systems, A Cyber-Physical Systems Approach", <http://LeeSeshia.org>, ISBN 978-0-557-70857-4, 2011.

An embedded system is a system that has computer hardware with software embedded in it as one of its important components, and perhaps additional mechanical or other parts, designed to perform a dedicated function or a limited set of dedicated functions.

It has hardware (processor, timer, interrupt controller, I/O devices, memories, ports, etc). It has main application software that consists of a series of tasks. Often, it has real time operating system that supervises the application software and sets the execution rules.

Industrial machines, automobiles, medical equipment, cameras, household appliances, airplanes, vending machines and toys (as well as the more obvious cellular phone and PDA) are among the myriad possible hosts of an embedded system.

Some embedded systems have fixed capabilities, some are programmable. Some include an operating system, but many are so specialized that the entire logic can be implemented as a single program.

However, some devices cannot be classified so easily. Tablets or smartphones use hardware technologies that are suited for embedded systems but perform many PC-like functions. Modern cars have embedded computers onboard that not only control the safety features of the car but allow also infotainment functions such as the navigation system or MP3 player.

### **3.3.2 Characteristics**

An embedded system:

- Is built to perform its duty, completely or partially independent of human intervention.
- Is specially designed to perform a few tasks in the most efficient way.
- Interacts with physical elements in our environment

More specifically, embedded systems are characterized by the following aspects:

- Functionality

Implemented for a particular purpose, an embedded system is a computing system that is part of a larger system that is not primarily a computing device. They are special purpose computing systems that can perform a single or few functionalities done by dedicated hardware and software with limited resources. This implies that the embedded application is known at design time and can be tuned according to the requirements and the hardware capabilities.

In contrast, general purpose computers, such as PCs, Macs, and UNIX workstations, and servers, can perform many functions depending on available hardware and installed software. A PC usually serves many purposes: checking email, surfing the internet, listening to music, word processing.

- User interface

Embedded systems rarely have a generic interface but more often minimal or no user interface. Even if embedded systems have a keypad and an LCD display, they are rarely capable of using many different types of input or output. An example of an embedded system with I/O capability is a security alarm with an LCD status display, and a keypad for entering a password.

- Interacting

Embedded systems are often used to control or act on their physical environments; they use sensors (temperature, position...) to characterize it, actuators (relay, servo motor) to act on it. Connected, they also communicate with applications running in data center.

- Time critical

Most embedded systems are time critical applications meaning that the embedded system is working in an environment where timing is very important: the results of an operation are only relevant if they take place in a specific time frame. What happens when the car airbag is fired too late? An autopilot in an aircraft is a time critical embedded system. If the autopilot detects that the plane for some reason is going into a stall then it should take steps to correct this within milliseconds or there would be catastrophic results.

- Limited Resources

The hardware for the embedded system is usually chosen to make the device as cheap as possible. Therefore, they are generally constrained by limited resources such as processor speed, power consumption, memory, real-time constraints, and network bandwidth. This means the programmer must create efficient programs that work with limited resources such as slow processors and low memory.

- Power consumption

Embedded systems put a great emphasis on energy and power consumption as there is a dichotomy in their design: the simultaneous need to be low power and high performance. Low power consumption increases the battery lifetime for battery-powered electronics and reduces the cooling and energy costs.

- Lifetime

An embedded system usually runs continuously. It never reboots. That leads to another characteristic: the embedded system belongs to a larger system whose life cycle can last many years. A medical implant must function properly for decades. An airplane operates for more than 50 years, and a nuclear plant even longer. This implies that embedded system must be trustworthy when installed as field repairs are difficult.

### **3.3.3 Real Time and RTOS**

Real time computing enabled by real-time operating system are essentials in the embedded world.

#### *Real time computing*

Embedded systems frequently control hardware, and must be able to respond to them in real time. It is important to define the notion of real-time system as this aspect distinguishes embedded systems from others where response time is important but not crucial. The Oxford Dictionary of Computing gives the following definition of a real-time system:

Any system in which time at which output is produced is significant. This is usually because the input corresponds to some movement in the physical world, and the output has to relate to that same movement. The lag from input time and output time must be sufficiently small for acceptable timeliness.

More precisely, real-time systems are ones whose correctness involves both the logical correctness of the outputs and their timeliness<sup>17</sup>. Unlike transaction-oriented enterprise

---

<sup>17</sup> "[Internet of Things — An action plan for Europe](#)", COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, June 2009



computers, embedded systems have to perform correctly within a specified time limit or deadline.

Real-time systems are classified by the consequence of missing a deadline: hard (Missing a deadline is a total system failure), firm (Infrequent deadline misses are tolerable, but may degrade the system's quality of service), and soft (The usefulness of a result degrades after its deadline)

There are many examples of real-time systems. For example, a car engine control system is a real-time system because a delayed signal may cause engine failure or damage. Other examples include medical systems such as heart pacemakers and industrial process controllers such as SCADA<sup>18</sup>. Almost all embedded systems are able to prioritize some tasks over others, and to put off or skip low priority tasks (such as user interface) in favor of high priority tasks (like hardware control).

### *Real-time Operating System*

To enable real time operations, a specialized operating system is required: a real-time operating system (RTOS). In order to be classifiable as an RTOS an operating system must have response time predictability and be deterministic, that is guaranteed within a certain margin of error. Of course, other qualities like speed, features set, small size etc, while important, are not what really characterize an RTOS.

RTOS differ from general-purpose operation systems (GPOS) on scheduling and interruption management. Most operating systems allow the programmer to specify a priority for different tasks. The goal is that if two or more tasks are ready to run at the same time, the OS will run the task with the higher priority. GPOS typically ensures some amount of run-time for each task, to make sure that all tasks receive at least some processing time. In a RTOS, if a high priority task is using 100% of the processor, no other lower priority tasks will run until the high priority task finishes.

While general-purpose operating systems may take a variable amount of time to respond to a given interrupt, real-time operating systems must guarantee that all interrupts will be serviced within a certain maximum amount of time.

Finally, although real-time operating systems may not have better performance than general purpose operating systems, they can provide much more precise and predictable timing characteristics than the later.

### **3.3.4 Internet of Things**

Embedded systems are key component for the Internet of Thing (IoT) and require a special focus regarding trust, acceptance and security.

In its communication to the European parliament and the council<sup>17</sup>, titled "*Internet of Things — An action plan for Europe*", the commission defines IoT as the umbrella for a new paradigm:

*One major next step in this development is to progressively evolve from a network of interconnected computers to a network of interconnected objects, from books to cars, from electrical appliances to food, and thus create an 'Internet of things'. These objects will sometimes have their own Internet Protocol addresses, be embedded in complex systems and use sensors to obtain information from their environment (e.g. food products that record the temperature along the supply chain) and/or use actuators to interact with it (e.g. air conditioning valves that react to the presence of people).*

---

<sup>18</sup> Supervisory Control And Data Acquisition, a type of industrial control system.

The communication complements its definition in noting three important points:

- IoT should not be seen as a mere extension of today's Internet but rather as a number of new independent systems that operate with their own infrastructures (and partly rely on existing Internet infrastructures).
- Second, as detailed in a recent ISTAG report, IoT will be implemented in symbiosis with new services.
- Third, IoT covers different modes of communication: things-to-person communication and thing-to-thing communications, including Machine-to-Machine (M2M) communication that potentially concerns 50-70 billion 'machines', of which only 1 % are connected today. These connections can be established in restricted areas ('intranet of things') or made publicly accessible ('Internet of things').

### **3.3.5 Critical Infrastructure**

Critical infrastructure is an asset or system that is essential for the maintenance of vital societal functions. Today critical infrastructure products are mostly developed with standard embedded systems platforms. This results in the reduction of costs and improved ease of use but at the same time increases the exposure to computer network-based attacks.

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. The Commission has identified the following critical infrastructure sectors:

- Energy
- Nuclear industry
- Information, Communication Technologies, ICT
- Water
- Food
- Health
- Financial
- Transport
- Chemical industry
- Space
- Research facilities

Recent deliberate disruptions of critical automation systems have proven that cyber-attacks have a significant impact on critical infrastructures and services. A secure platform such as EURO-MILS may ensure the adequate level of protection and limit as far as possible the detrimental effects of disruptions on the society and citizens.

## **3.4 Virtualization: Improving Resource Utilization**

Virtualization refers to running multiple execution environments on a single physical machine at the same time.

Virtualization is not a new concept. It was first introduced by IBM in the 1960s to allow the partitioning of large mainframe environments. Today, virtualization is adopted in the IT and enterprise domains for server and desktops. Software suppliers include VMware, Microsoft, and Citrix Xen in x86 environments.

Virtualization can be approached through hardware partitioning or hypervisor technology. Hardware partitioning subdivides a physical server into fractions, each of which can run an operating system. These fractions are typically created with coarse units of allocation, such as whole processors or physical boards. Hypervisors use a thin layer of code in software or

firmware to achieve fine-grained, dynamic resource sharing. Compared to hardware partitioning, hypervisors provide the greatest level of flexibility in how virtual resources are defined and managed.

The role of the hypervisor is to control the physical resources (CPU, memory, I/O...), and to allocate them to each virtual machine (a guest operating system) in turn and making sure that they cannot disrupt each other.

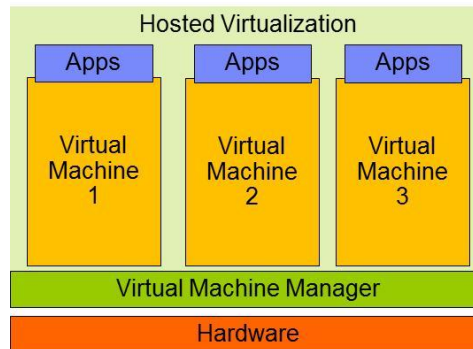


Figure 8: Virtualization

Virtualization is a key technology in the server space. Traditionally, server utilization is so small for a large number of workloads that virtualization permits multiple virtual servers instances to be created and hosted on a single physical server. Each virtual server has its own set of virtual hardware on which operating systems and applications are loaded.

Virtualized desktop is another type of virtualization, permitting a server to host multiple clients over a network using minimal client endpoints (thin clients).

Virtualization has recently become popular in the embedded-systems space.

### 3.4.1 Virtualization Types

There are two types of hypervisors<sup>19</sup>:

- Type 1 hypervisor, “bare metal”, runs directly on the hardware.
  - In the Information technology area, the many offerings include Oracle VM Server for SPARC, the Citrix XenServer, KVM, VMware ESX/ESXi, and Microsoft Hyper-V hypervisor.
  - In the embedded system area, LynxSecure Embedded Hypervisor and separation kernel from LynuxWorks, INTEGRITY-178B from GreenHills Software, Virtualization Profile for VxWorks from Wind River Systems, and PikeOS from SYSGO.
- A Type 2 hypervisor, “hosted”, runs on another operating system.
- E.g. VMware Workstation and VirtualBox in the IS area.

<sup>19</sup> R. Goldberg, “Architectural Principles for Virtual Computer Systems”, *Harvard University*, February 1973

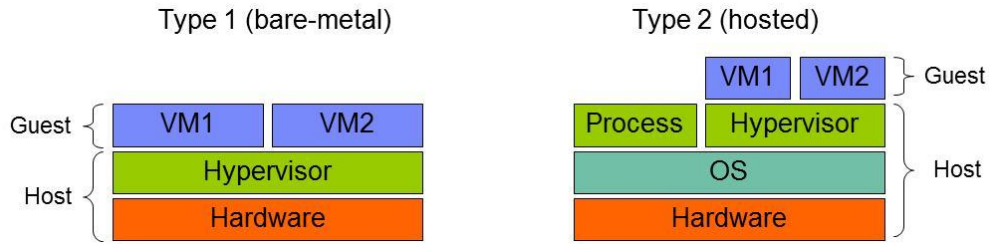


Figure 9 : Hypervisor Types

PikeOS, the real time operating system used in the EURO-MILS project, is a Type 1 hypervisor.

### 3.4.2 Virtualization Techniques

Table 2 presents the relative strengths by virtualization models.

Hardware Emulation	
<p>Using hardware emulation, a virtual machine is created on a host system to emulate the hardware of interest.</p> <p>As every instruction must be simulated on the underlying hardware, this technique is very slow. Hardware emulation is often used in co-development of firmware and hardware to allow simulation of a hardware in development.</p>	
Full virtualization	
<p>The hypervisor mediates between the guest operating systems and the native bare hardware. Certain protected instructions are trapped and handled within the hypervisor.</p> <p>Full virtualization is faster than hardware emulation, but performance is less than bare hardware because of the mediation. The guest OS can run unmodified, but requires to support the underlying hardware.</p>	
Paravirtualization	
<p>The hypervisor manages the shared access to the underlying hardware. It requires virtualization-aware code in the OS itself. There is no need for any recompilation or trapping because OS cooperate in the virtualization process</p> <p>It requires a modification of guest OS but performances are near that of an unvirtualized system. Multiple different OS can be supported concurrently.</p>	

Operating system-level virtualization

This method virtualizes servers on top of the OS itself. It isolates independent servers running same OS from one another

It requires changes to the OS kernel. Advantage is native performance. However, all instances have to be at the same OS and patch levels. If the master operating system is brought down, all of the virtual environments come down with it.

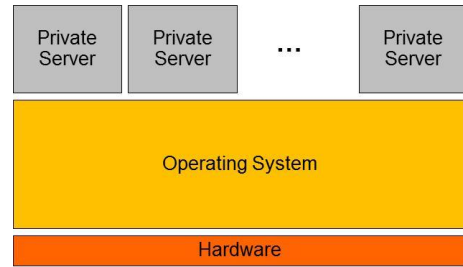


Table 2: Virtualization Models

There are several kinds of virtualization<sup>20</sup> that have relative strengths. In EURO-MILS, PikeOS implements paravirtualization

**3.4.3 Embedded Virtualization**

Virtualization followed the evolution of computing from servers, then desktops, and now embedded devices (Figure 10). The embedded domain has several useful applications for virtualization, including mobile handsets, security kernels, and concurrent embedded operating systems<sup>21</sup>. Embedded virtualization refers to a type-1 hypervisor deployed within an embedded system. It allows the support of a security kernel and concurrent embedded operating systems.

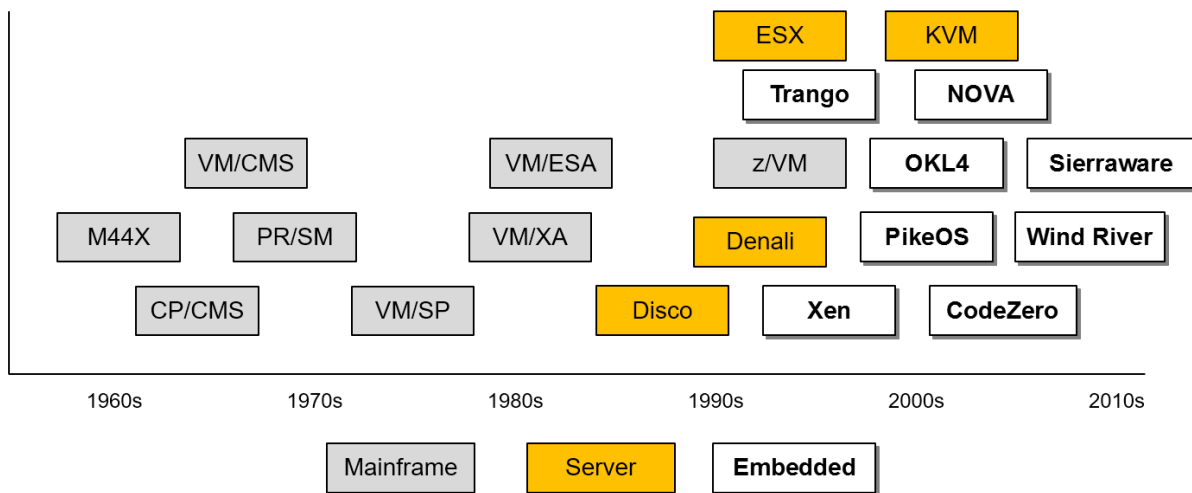


Figure 10: Simplified Timeline of Type-1 Hypervisors

Unlike traditional hypervisors, embedded hypervisors implement a different kind of abstraction with different constraints than other platforms:

<sup>20</sup> T. Jone, "Virtual Linux: An overview of virtualization methods, architectures, and implementations", *IBM DeveloperWorks*, December 2006.

<sup>21</sup> Time Jones, "Virtualization and Embedded Systems", *IBM developerWorks*, April 2011

- Efficiency. Due to the resources constraints of the embedded system, embedded hypervisors must be small. They also need to optimize the memory usage.
- Security. The smaller the hypervisor is, the smaller the code size, the easier it is to validate and prove the platform is secure and safe.
- Communication. The hypervisor manages the communication between guest applications. Efficient and secure, it permits privileged and non-privileged applications to coexist.
- Isolation. Using the hypervisor's communication mechanism provide containment for security and reliability by isolating applications from one another.
- Real-time. Scheduling with real-time characteristics allows the critical functions to coexist with applications that operate on a best-effort basis.

#### Microkernel and hypervisor

Main component of the operating system, the kernel can be seen as a bridge between applications and the actual data processing done at the hardware level. In the embedded space, to keep overhead to minimum, the microkernel defines a simple abstraction over the hardware, with a set of primitives or system calls to implement minimal OS services such as memory management and address spaces (for isolation), multitasking and threads (for concurrency), and inter-process communication (for communication between threads in different address spaces).

Microkernels have a lot in common with hypervisors: both provide a substrate on top of which the "real" operating system is implemented. The key difference is that microkernels such as LynxOS-SE are designed to be a minimal layer to support arbitrary systems, while hypervisors such as Xen are designed specifically to support (multiple) legacy operating systems. New generations of RTOS such as PikeOS, combining both functionalities of a virtualization platform with a microkernel, allow isolation between multiple VMs (operating system plus application) as well as individual applications.

### **3.4.4 Virtualization Value**

In the enterprise world, virtualization is an effective way to reduce IT expenses while boosting efficiency and agility. Virtualization lets organizations:

- Run multiple operating systems and applications on a single computer
- Consolidate hardware to get vastly higher productivity from fewer servers
- Simplify IT management, maintenance, and the deployment of new applications
- Increase the speed and functionality of systems while decreasing the power requirements.

Last but not least, virtualization can be used to separate processes with different security and safety requirements. Using virtualization, it is possible to isolate certified applications from noncertified applications to retain certification levels while extending functionality.

## **3.5 MILS: High-Assurance Security Architecture**

The software industry and the customers that implement applications rarely think about security first. Standard commercial operating systems are not built for security. But when supporting mission critical systems in industries such as aerospace, defense, healthcare or transportation, the architecture must enable protection against external threats such as malicious software, but also internal threats such as mistakes or failures. That is where MILS comes into the picture.

### 3.5.1 MILS Definition

Multiple Independent Levels of Security (MILS) is a high-assurance security architecture based on the concepts of separation and controlled information flow. The text of the definition in wikipedia<sup>22</sup> dates from 2007 and has withstood the times since then. It defines MILS as:

A high-assurance security architecture based on the concepts of separation and controlled information flow; implemented by separation mechanisms that support both untrusted and trustworthy components; ensuring that the total security solution is non-bypassable, evaluatable, always invoked and tamperproof.

It is hard to find a concise definition for MILS. In our D21.1 report on MILS architecture<sup>23</sup>, we list some other definitions we have found in the technical literature. All of these definitions share two concepts: resource management is used to manage components that are used in building blocks for controlled information flow.

Our shot at a catchy, architecture-centric, definition would be:

MILS is resource management and access control for controlled information flow.

which translates into a more consumer-centric definition:

MILS is a system architecture that allow secure parallel execution of multiple independent applications

### 3.5.2 MILS Characteristics

MILS is not a system design: it an architecture model that tells you what designs may be considered MILS.

The corner-stone of the architecture is a separation mechanism that encapsulates trusted and untrusted applications in compartments that reduce mutual dependencies to communications over channels explicitly defined by policies. The secure communication mechanisms must be:

- Non-bypassable: a component cannot use another communication path, including lower level mechanisms to bypass the security monitor.
- Evaluatable: any trusted component can be evaluated to the level of assurance required of that component. This means the components are modular, well designed, well specified, well implemented, small, low complexity, etc.
- Always-invoked: each and every access/message is checked by the appropriate security monitors (i.e., a security monitor will not just check on a first access and then pass all subsequent accesses/messages through).
- Tamperproof: the system controls "modify" rights to the security monitor code, configuration and data; preventing unauthorized changes.

These characteristics are often referenced using the acronym of NEAT.

---

<sup>22</sup> Source: "[Multiple independent levels of security](#)", Wikipedia.

<sup>23</sup> Source: "[MILS Architecture](#)", Holger Blasum and al., ICT-318353 / D21.1, EURO-MILS, 2013

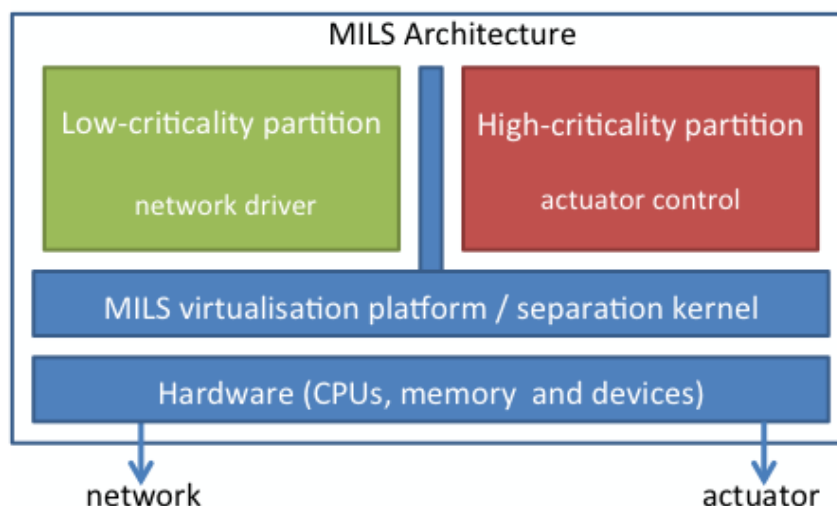


Figure 11: Multiple Independent Levels of Security Architecture

The *MILS architecture* (Figure 11), as the central concept right from the beginning, provides *separation* of applications and their security functionality. It limits the complexity and scope of security mechanisms and makes evaluation possible.

### 3.5.3 From MLS to MILS

The MILS approach resulted from the insight that it is impossible to provide high assurance for large monolithic systems. In general, security *cannot be shown on an abstract system* and then be *refined* to a concrete implementation. This implies that for monolithic systems security has to be treated by taking into account all the technical details that could lead to dependencies causing security flaws.

Moreover, at a purely conceptually level it turned out that a single *global* security policy, for example an instance of multi-level security, will not serve the needs of all the various heterogeneous applications running in a common environment. This has been traditionally a requirement in military applications where the system are processing data items that are classified at different level of security, and the information flow security policy that prevent the transfer of high-level classified information into low-level object must be preserved. The problem with full MLS system is that they must be rigorously analysed for security before they can be certified. And, because of its inherent complexity, it is very difficult to evaluate a MLS system.

High assurance systems require convincing evidence that system meets critical security and safety requirements. The proof is given using a formal methods analysis. However, with complex operation systems, it becomes difficult to separate security functionality from other system functions and therefore impossible to formally verify correctness. MILS develops a layered approach with lower layers providing security services to higher layers. Each layer is responsible for security services in its own domain and nothing else. The MILS approach decomposes security functionalities into small manageable components residing in compartments that reduce interdependencies to a small set of interfaces that can be overlooked and handled by the applications in a secure way.

The MILS approach was developed to resolve the difficulty of certification of MLS systems, by separating out the security mechanisms and concerns into manageable components, such as:

- SLS : Single-Level Secure component that only processes data at one security level



- MSLS Multiple Single-Level Secure component that processes data at different levels and maintains separations between classes of data.
- MLS Multi-Level Secure components that co-mingle data at different security levels

A MILS system isolates processes into partitions, which define a collection of data objects, code and system resources. These individual partitions can be evaluated separately. This divide and conquer approach exponentially reduce the proof effort for secure system<sup>24</sup>.

### **3.5.4 Security Using Separation Microkernel**

The foundational component of MILS is the virtualization platform: a separation micro-kernel which isolates processes and their resources into isolated execution spaces called partitions. Processes running in different partitions can neither communicate nor infer each other's presence unless explicitly permitted by the separation micro-kernel. It provides the security functions and serves as an hypervisor of one or several guest operating systems, i.e. real-time operating systems (RTOS), run-time environments (RTE) and/or APIs.

The separation kernel is the base layer of the system and is responsible for enforcing data separation and information flow control within a single microprocessor. It provides both time and space partitioning.

The MILS separation kernel enforces the following security policy:

- Data isolation: Information in a partition is accessible only by that partition, and private data remains private.
- Control of information flow: Information flow from one partition to another is from an authenticated source to authenticated recipients, and to nowhere else.
- Periods processing/sanitization: The microprocessor and any networking equipment cannot be used as a covert channel between partitions. All shared resources are cleaned before another partition can reuse them.
- Fault isolation: Damage is limited by preventing a failure in one partition from cascading to another partition.

Most hardware systems have a distinction of privileged and user mode machine instructions. With respect to security, the idea of a hypervisor is to intercept privileged machine instructions of the guest operating system and instead of running it directly on the hardware, first check the rights of the caller against the system configuration and other permission attributes before actual execution. Currently popular desktop operating systems usually have all device drivers managing I/O devices (graphics and network cards, keyboard controllers, pointing devices etc.) integrated into the kernel. And a failure in a network driver can take down the entire system ("panic" or "bluescreen").

Instead, the separation micro-kernel has a small set of core services which runs in privileged mode only and provides core services such as scheduling, context switches, process communication and synchronization, interrupt and processor exception handling, whereas device drivers are executed in user mode like any other application code, without access to privileged instructions.

Because the hypervisor is always invoked, non-bypassable, tamperproof, and evaluatable, it strongly contributes to security properties: when the privileged code base is small, then it is easier to verify against intrusion points for malicious attacks. Of course, a small micro-kernel also has less points that might fault (e.g. it is stored in less memory cells in hardware that might degrade), so there is also a safety dimension.

---

<sup>24</sup> J. Alves-Foss, W. S. Harrison, P. Oman and C. Taylor. "The MILS Architecture for High Assurance Embedded Systems", International Journal of Embedded Systems, 2006.

## Chapter 4 Trustworthiness by High Assurance: Certification Environment

To be labelled as trustworthy, a system must be safe and secure. It not only must behave as expected but also must reinforce the belief that it will continue to produce expected behaviour and will not be susceptible to subversion. It must also protect from harm users, components and information.

A number of governments and organizations have set up standards and in some times legal regulations to help ensure an adequate level of safety and security. Some industries, such as banking or healthcare, have also created guidelines that become standards among member of these industries.

High-assurance systems are used in environments where failure can cause security or safety breaches. Before a system can be deployed in an aircraft or in a car, there must exist convincing evidences that it is robust and reliable and performs correctly. Such an assurance is provided by certification performed by independent third parties according to widely accepted industry security and safety standards.

In the following sections, we give a brief introduction to the most commonly adopted security and safety standards and regulations.

### 4.1 Do we need Standards?

Standards, in one form or another, have always underpinned trade and business. Along with codes of practices and guides, they support compatibility and drive down costs through use of common parts, specifications and methods. They can also help open markets, create new industries and realize the potential of new technologies<sup>25</sup>. They provide benefits such as defining accurate and necessary measurements, lowering product costs; improving product performance and quality. Standards facilitate introduction of new technologies, weaken monopolies and enhance competitions by improving uniformity and functionality. Standards can reduce development costs. They are key for interoperability. And related to our domains, they aim to improve security and safety.

#### 4.1.1 Standards Value

International standards can be considered as economic building blocks. In 1999, the Organization for Economic Co-operation and Development published a report<sup>26</sup> which estimated the value of standards and technical regulations directly affecting global trade to be more than 80% of world trade with a value of more than 3 trillion €. International standards can accelerate the pace of technological development. For a supplier, the ability to harness the potential of standards is a source of competitive advantage.

---

<sup>25</sup> Source: [“United Kingdom National Standardization Strategic Framework”](#) 2003

<sup>26</sup> Source: [“OECD Report on Regulatory Reform and International Standardization”](#) – OECD - 1999

A study<sup>27</sup> done by the International Standard Organization demonstrates that companies achieve benefits from using standards. The overall benefits from the use of standards vary, for most cases, between around 0,5 % and 4 % of the annual sales revenues of the companies.

However, standardization is a time-lagged and long-term complex process. A study by TÜV on an IEC standardization process indicates that more than 5 years were required between the preliminary proposal and the final promulgation of the international standard.

#### 4.1.2 International Standard Organizations

Standardization needs also to involve multiple stakeholders with different objectives and agendas: customers, suppliers, competitors, and sometime regulation authorities. Due to the fragmentation of the embedded system industry and related communities, and the segmentation of domains and technologies, there is also sometime competition between committees and standardization bodies.



Figure 12 : Working Areas of International Standard Organizations

Standard bodies produce standards International and national standards are issued by organizations bodies:

International organizations create specifications and criteria to be applied consistently in the classification of materials, the manufacture of products and the provision of services. The main bodies are:

- International Organization for Standardization (ISO);
- International Electrotechnical Commission (IEC) ;
- International Telecommunication Union (ITU);

<sup>27</sup> Source: [“Economic benefits of standards - International case studies - Volume 1”](#) – ISO - 2011

The mission of European standardization bodies is to promote voluntary technical harmonization in Europe in conjunction with worldwide bodies and its partners in Europe European level. We can list:

- European Standardisation Council (ESC) works to develop European Standards in various sectors
- European Committee for Electrotechnical Standardization (ECES) works in the area of electrical engineering;
- European Telecommunications Standard Institut (ETSI) produces standards for ICT, including fixed, mobile, radio, converged, broadcast and internet technologies.;

All countries have their own standards organization; examples are:

- Association Française de Normalisation (AFNOR) in France ;
- Deutsche Industrie Normen (DIN) in Germany ;
- Institut Belge de Normalisation (IBN) in Belgium;
- Schweizerischen Normen Vereinigung (SNV) in Swiss;
- British Standard Institute (BSI) in United Kingdom ;
- Standards Council of Canada (SCC) in Canada;
- American National Standard Institute (ANSI) in United States

#### 4.1.3 Main Security and Safety Standards

The following table<sup>28</sup> lists the main safety and security standards.

Standard	Goals	Description
Common Criteria	Evaluation criteria for IT security	Provide assurance (levels) that the process of specification, implementation and evaluation of a computer security product or system has been conducted in a rigorous and standard manner. Meanwhile they became ISO/IEC 15408:2009 (3 parts).
DO 178B/ED-12B	SW Considerations in Airborne Systems and Equipment Certification	Depending on its criticality SW is assigned to 1 of 5 Design Assurance Levels. The level determines development methods and QA measures. Mandatory standard by FAA and EASA. The more "goal based" DO-178C is on the way that i. a. considers emerging software technologies.
IEC 62443	Industrial communication networks - Network and system security	Defines technical security requirements for communication scenarios for industrial automation and control systems. Consists of 4 sub-series: General, Asset Owner, System Integrator, Component Provider

<sup>28</sup> Source: "[Standards for Embedded Systems](#)" - Dr. Kai Strübbe - TÜV SÜD - 2011

Standard	Goals	Description
IEC 62351	Information Security for Power System Control Operations	Define security requirements for power system management and information exchange, including communications network and system security issues, TCP/IP and MMS profiles, and security for ICCP and Sub-station automation and protection as e. g. defined in IEC 61850.
ISO/IEC 25051	Requirements for quality of COTS software product and instruction for testing	Defines quality requirements for COTS software including product description and user documentation. The quality requirements, functionality, reliability, usability, efficiency, maintainability, portability, and quality in use. The test instruction requires documentation of test plan, test cases and test results.
ISO 27001	IT - Security Techniques – ISMS - Requirements	World's most widely adopted security standard. Specifies requirements on Information Security Management Systems (ISMS); intends to bring information security under management control. > 12 ISO 270xx standards
ISO/IEC 61508	Functional Safety of E/E/PE Safety-related Systems	Defines requirements on safety-related systems which incorporate electrical /electronic /programmable electronic (E/E/PE) devices (e.g. valves, electrical relays, switches or PLCs) depending on the Safety Integrity Level (SIL 1 to 4) assigned. Several industry specific standards have been derived from it, e.g. IEC 61511 for process -, IEC 61513 for nuclear industries, IEC 62061 for machinery safety, or IEC 26262 for automotive sector
VDI 2182	IT-security for industrial automation	Describes how to identify assets, define security objectives, identify threads, assess risks, implement counter measures and to perform audits of automation devices, systems and plants.
ISO/IEC 61850	Communication networks and systems in electrical substations	One of the core standards for Smart Grids and was issued in 2004. It is an international standard for communication networks and systems in electrical substations as well as transmission and distribution of electrical power.  The IEC 61850 communication protocol defines the ways of exchanging messages between nodes of the power grid.

Table 3: Main Security and Safety Standards

## 4.2 Security Standards

### 4.2.1 ISO/IEC 15408 (Evaluation Criteria for IT Security)

To ensure trust by high-assurance, the EURO-MILS platform “will go through a Common Criteria security standard evaluation”.

Created in response to increasing threats to IT products<sup>29</sup> security, the Common Criteria for Information Technology Security Evaluation, in short Common Criteria (CC) is an international standard (ISO/IEC 15408) for evaluating the security properties of IT security products. It is designed to bolster end-user confidence by providing clear and reliable assurance that a technology's integrity and security architecture have been thoroughly tested and validated by an accredited, third-party source. CC provides a common set of requirements for the security functionality of these products and for assurance measures applied to these products during a security evaluation.

1919 Certified Products by Category *	
Category	Products
Access Control Devices and Systems	80
Biometric Systems and Devices	3
Boundary Protection Devices and Systems	119
Data Protection	80
Databases	46
Detection Devices and Systems	45
ICs, Smart Cards and Smart Card-Related Devices and Systems	719
Key Management Systems	37
Multi-Function Devices	207
Network and Network-Related Devices and Systems	189
Operating Systems	102
Other Devices and Systems	211
Products for Digital Signatures	78
Trusted Computing	3
<b>Total:</b>	<b>1919</b>
* A Certified Product may have multiple Categories associated with it.	

Figure 13 : CC Certified Products by Category (source Common Criteria)

CC is a jointly developed evaluation standard for software that was created by a consortium representing the United States, United Kingdom, Germany, France, Canada, and the Netherlands. The purpose of CC is to standardize evaluation of security features in software, which allows, for example, the comparison of different security solutions.

This standard helps evaluate, validate, and certify the security assurance of a technology product against a number of factors, such as the security functional requirements specified in the standard. It defines a framework in which computer system users specify their security requirements, vendors implement it and testing laboratories evaluate the products security to determine if they actually meet the claims.

The Common Criteria process establishes confidence that the security functionality of IT products earning certification and the assurance measures applied to these IT products meet

<sup>29</sup> Hardware of software products, (i.e. embedded systems, general purpose computers, network devices, operating systems, applications)

the established Common Criteria evaluation requirements. Common Criteria is useful as a guide for the development, evaluation and/or procurement of IT products with security functionality.

CC has been in use for more than a decade and thus is understood by stakeholders in the vendor community who have worked with the certification over time. This experience and longevity provides a level of certainty and consistency in the CC.

#### 4.2.1.1 Evaluation Assurance Levels

The evaluation process establishes a level of confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements. The evaluation results may help consumers to determine whether these IT products fulfil their security needs.

Hardware and software are evaluated against CC requirements in accredited testing laboratories<sup>30</sup> to certify the exact EAL (Evaluation Assurance Level) the product or system can attain. The evaluation allows determining the fulfilment of particular security properties to an assurance level

The higher the assurance level, the stricter the requirements mandated by the CC. At the highest levels (EAL 5-7), the CC requires the use of formal methods, mathematical models, and proofs. There are 7 EALs:

- EAL1 - Functionally tested: the testing is performed without assistance from the product's development team.
- EAL2 - Structurally tested: more aspects of the product and its development and manufacturing processes are looked at, with the help of the product's developers
- EAL3 - Methodically tested and checked: the design of the product is looked at for appropriate security considerations. The depth of functional testing and examination of the processes is increased with respect to EAL 2.
- EAL4 - Methodically designed, tested and reviewed: the analysis goes deeper than for EAL 3. An informal security policy model of the product is also requested.
- EAL5 - Semi-formally designed and tested: at this level more stress is put on vulnerability analysis and testing, along with an assessment of the rigor of development practices.
- EAL6 - Semi-formally verified, designed and tested: even more vulnerability analysis and testing. The development process goes under a semi-formal examination.
- EAL7 - Formally verified, designed and tested: this is the highest assurance level that can be achieved. High resistance to penetration is required from the product. There is also a requirement for extended test results, both by the product developers and by the independent organization.

---

<sup>30</sup> Members of the EURO-MILS consortium, Thales Communications & Security SA, in France, T-Systems Bestätigungsstelle and Deutsches Forschungszentrum für künstliche Intelligenz GmbH, in Germany are accredited laboratories.

Certified Products by Scheme and Assurance Level																			
Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Germany	8	4	7	18	12	53	15	256	8	127	0	5	0	0	0	0	0	1	514
Spain	7	6	5	3	3	9	0	20	0	1	0	0	0	0	0	0	0	0	54
France	1	18	0	14	0	23	4	210	2	134	0	7	4	0	0	0	0	417	
Italy	1	5	0	0	2	0	1	0	0	0	0	0	0	0	0	0	0	9	
Netherlands	0	0	0	1	0	1	1	13	0	4	0	6	0	1	0	0	0	27	
Norway	0	0	1	10	0	5	12	7	2	3	0	0	0	0	0	0	0	40	
Sweden	0	0	0	0	1	0	0	2	0	0	0	0	0	0	0	0	0	3	
United Kingdom	0	0	1	10	1	3	0	7	0	0	0	0	0	0	0	0	0	22	
<b>Total (Europe)</b>	<b>17</b>	<b>33</b>	<b>14</b>	<b>56</b>	<b>19</b>	<b>94</b>	<b>33</b>	<b>515</b>	<b>12</b>	<b>269</b>	<b>0</b>	<b>18</b>	<b>4</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>1</b>	<b>1086</b>	
Rest of the world	20	3	103	181	158	131	48	162	0	10	0	2	1	0	0	0	0	14	833
<b>Total (worldwide)</b>	<b>37</b>	<b>36</b>	<b>117</b>	<b>237</b>	<b>177</b>	<b>225</b>	<b>81</b>	<b>677</b>	<b>12</b>	<b>279</b>	<b>0</b>	<b>20</b>	<b>5</b>	<b>1</b>	<b>0</b>	<b>0</b>	<b>15</b>	<b>1919</b>	

Figure 14: Certified Products by European Countries

#### 4.2.1.2 Target of Evaluation, Protection Profiles, and Security Target

The target of evaluation (TOE) is a set of software, firmware and/or hardware possibly accompanied by user and administrator guidance documentation. The TOE is the subject of an evaluation. In the EURO-MILS project, the TOE is the MILS-based system and its processor hardware.

A security target is an implementation-dependent statement of security needs for a specific identified TOE where a protection profile is an implementation-independent statement of security needs for a TOE type.

The security target specifies “what is to be evaluated” and serves as a basis for agreement between the developer and the evaluator on the exact security properties of the TOE and the exact scope of the evaluation. After the evaluation, the security target specifies “what was evaluated”.

A protection profile is typically a statement of common set of security needs for a specific type of IT. A User community will only consider buying a specific type of IT if it meets the protection profile. A regulatory entity will only allow a specific type of IT to be used if it meets the profile, or a group of developers agree that all IT that they produce of this type will meet this baseline.



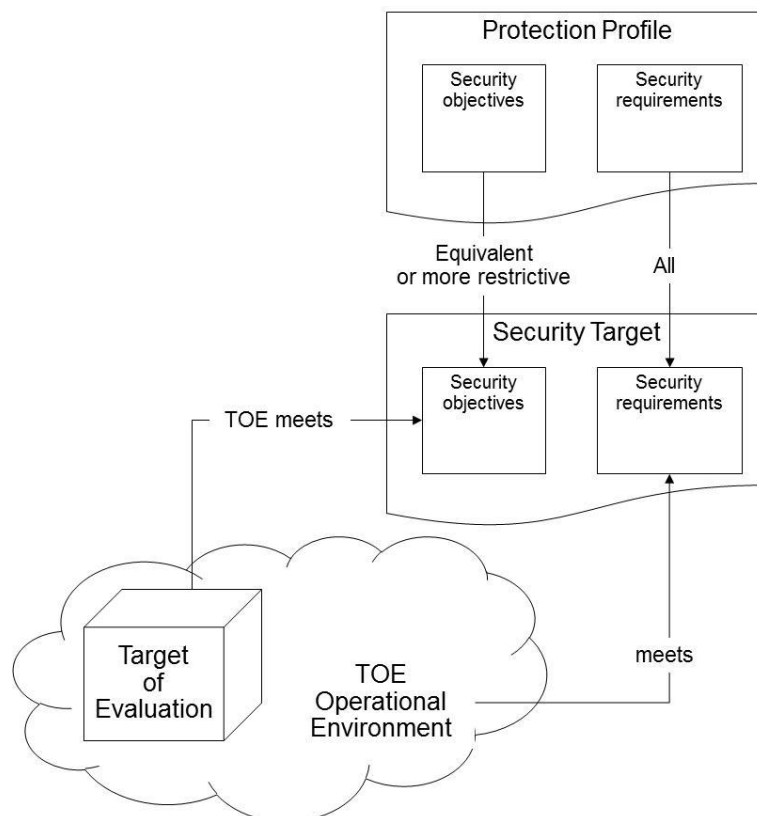


Figure 15: Protection Profile, Security Target and Target of Evaluation Relationship - Simplified (source: Common Criteria)

#### 4.2.2 ISO/IEC ISMS Information Security Management System family of standards

The ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission), the specialized bodies working on worldwide standardization, have established a joint technical committee, ISO/IEC JTC 1, to work on information security. The committee has prepared a set of standards for information security, otherwise known as the Information Security Management System (ISMS) family of standards

The ISMS family of standards provides a model to develop and implement a framework for managing the security of their information assets including financial information, intellectual property, and employee details, or information entrusted to them by customers or third parties.

The ISMS family of standards maintains relationships with many other ISO and ISO/IEC standards. ISO/IEC 27000<sup>31</sup> provides to organizations and individuals an overview of the family of standards. It introduces information security management systems and the terms and definitions used throughout the ISMS family of standards.

Two standards are specifying requirements:

- ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving formalized information security

<sup>31</sup> "ISO/IEC27000 Information technology — Security techniques — Information security management systems — Overview and vocabulary" - Second edition 2012-12-01

management systems (ISMS) within the context of the organization's overall business risks

- ISO/IEC 27006 specifies requirements and provides guidance for bodies providing audit and ISMS certification in accordance with ISO/IEC 27001.

Five standards describe general guidelines

- ISO/IEC 27002 provides a list of commonly accepted control objectives and best practice controls to be used as implementation guidance when selecting and implementing controls for achieving information security.
- ISO/IEC 27003 provides practical implementation guidance and provide further information for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an ISMS in accordance with ISO/IEC 27001.
- ISO/IEC 27004 provides guidance and advice on the development and use of measurements in order to assess the effectiveness of ISMS, control objectives, and controls used, as specified in ISO/IEC 27001.
- ISO/IEC 27005 provides guidelines for information security risk management
- ISO/IEC 27007 provides guidance on conducting ISMS audits, as well as guidance on the competence of information security management system auditors.

And some other standards describe sector-specific guidelines

- ISO/IEC 27010 provides guidelines for initiating, implementing, maintaining, and improving information security in inter-organizational and inter-sector communications.
- ISO/IEC 27011 provides guidelines supporting the implementation of Information Security Management in telecommunications organizations.
- ISO/IEC TR 27015 complements the guidance given in the ISO/IEC 27000 family of standards, for initiating, implementing, maintaining, and improving information security within organizations providing financial services.
- ISO 27799 provides guidelines supporting the implementation of Information Security Management in health organizations

### **4.2.3 FIPS-140-2**

Federal Information Processing Standards (FIPS) are publicly announced standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors. They are used also widely by other entities such as Financial Services organizations globally. FIPS standards are issued to establish requirements for various purposes such as ensuring computer security and interoperability, and are intended for cases in which suitable industry standards do not already exist. Many FIPS specifications are modified versions of standards used in the technical communities,

FIPS 140 series are security standards that specify requirements for cryptography modules. FIPS 140-2 covers the secure design and implementation of these cryptographic modules, including roles, services and authentication; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility; self-tests; design assurance; and mitigation of other attacks.

## **4.3 European Privacy Seal**

One of the main problems facing the information society is a lack of trust in IT products and services caused by the possibilities of electronic surveillance. Citizens and business often need "a good faith belief" when using privacy relevant IT products and services. Trustworthy

and reliable guidance is needed to assist users and consumers to select a privacy and data protection compliant product or service.

EuroPriSe<sup>32</sup>, the European Privacy Seal, is a European scheme providing privacy and data protection certification for IT products and IT-based services. The European Privacy Seal embodies a visible trust mark certifying that a product or service has been checked by independent experts and approved by an impartial privacy organization. EuroPriSe started in June 2007 as a pilot project funded by the European Commission's eTEN program<sup>120</sup>. The European Privacy Seal certifies that an IT product or IT-based service facilitates the use of that product or service in a way compliant with European regulations on privacy and data protection, taking into account the legislation in the EU Member States.

Manufacturers and vendors of IT products and IT-based services can apply for the European certificate. The trust mark is awarded after successful evaluation of the product or service by independent experts and a validation of the evaluation report by an impartial certification body.

EuroPriSe provides transparent procedures and reliable criteria. The European Privacy Seal embodies a visible trust mark certifying that a product or service has been checked by independent experts and approved by an impartial privacy organization. The European Privacy Seal distinguishes trustworthy products and services.

To manufacturers and vendors it delivers assurance of privacy compliance on the European level. EuroPriSe fosters consumer protection and trust and at the same time provides a marketing advantage to manufacturers and vendors of privacy respecting goods and services.

## 4.4 Safety Standards

### 4.4.1 Avionic Safety Standard: DO-178B Certification Standard

In the avionics, functional safety has naturally a long tradition. The avionics industry has the most stringent requirements for software safety, the most pioneering methods of implementation and the most advanced approach to control costs. Aerospace manufacturers use more and more commercial off-the-shelf hardware and software components for avionics control systems.

DO-178B is a mandatory certification standard for software used in airborne systems. DO-178B concentrates on objectives for software life cycle processes to assure the development of safe and reliable software for airborne environments. DO-178B determines five safety levels by examining the effects of a failure condition in the system: Level A (catastrophic), Level B (hazardous), Level C (major), Level D (minor), and Level E (no effects). According to these levels the software has to satisfy up to 66 objectives.

DO-178B has been accepted by the US Federal Aviation Administration (FAA) as certification standard and guideline to determine software safety. The European Organization for Civil Aviation Equipment (EUROCAE) adopted DO-178B as ED-12B.

DO-178C, a new version of the standard will replace DO-178B as the primary document by which the certification authorities such as FAA and EASA approve all commercial software-based aerospace systems. Certification Authority approval is still pending, with FAA approval expected sometime in 2013.

---

<sup>32</sup> EuroPriSe, the European Privacy Seal ([www.european-privacy-seal.eu](http://www.european-privacy-seal.eu))

#### **4.4.2 IEC 61508: Functional Safety for Electronic Devices**

Risk management and safety aspects become increasingly important for the selection of software platforms for embedded systems used in the industrial automation and process control industry.

IEC 61508 (also EN 61508) has been released in 1998 by the IEC and renewed in 2010. The document includes seven parts where part 3 defines the software requirements of "Functional safety of electrical/electronic/programmable electronic safety-related systems".

IEC 61508 distinguishes four Safety Integrity Level (SIL) according to the probability of failures and their potential damage. Certification after IEC 61508 is required if computer-based systems perform safety-critical functions which today is more and more common. For the software components, a V-model based development process mandatory.

#### **4.4.3 EN 50128 Certified Software for Railways Applications**

Railways and trains increasingly depend on software applications with safety-critical functions. These applications have to be certified according to EN 50128 with international acknowledgement due to transnational cooperation.

EN 50128 has been released in 2001 by CENELEC and is based on the IEC 61508 standard for electrical/electronic/programmable electronic equipment. EN 50128 defines safety requirements of software for railway applications (communication, signaling and processing systems), railway control and protection systems. Analogous to IEC 61508, EN 50128 distinguishes as well four Safety Integrity Level (SIL) according to the probability of failures and their potential damage. For the software components a V-model based development process is mandatory.

#### **4.4.4 ISO 26262 Certification for Automotive Appliances**

Today's cars are equipped with up to 100 electronic control units (ECU) which often have safety-critical functions. The upcoming ISO 26262 standard regulates the use of software in safety-critical environments in automotive applications. A modular software platform can integrate multiple ECUs on a single hardware platform and helps to reduce certification costs.

Based on IEC 61508, the ISO 26262 has been released in 2011 and is recommended but not mandatory for safety-critical automotive applications. ISO 26262 defines state-of-the-art design processes for software development comparable to DO-178B in the avionics.

#### **4.4.5 IEC 62304: Certification for Medical Devices**

Sophisticated medical devices have high cost saving potential. They are more and more used for the provision of patient care. The appliances directly in use at the patient have proven to be safe.

Functional safety of software for medical devices is certified according to IEC 62304, a standard for the software life cycle processes of medical device software, released in 2006. IEC 62304 requires safety classification of software and defines processes for development, maintenance and risk management, configuration management, problem-solving processes, and quality management.

IEC 62304 classifies three safety classes where Class A appoints the lowest (no risk) and Class C the highest class (risk of death or severe injuries).

## Part II: Business Value

In this part, we concentrate on the business value of the EURO-MILS platform. We investigate the business value of a trustworthy ICT from a horizontal platform perspective and identified market requirements of MILS systems. We asked an Industry panel composed of 39 professionals which represent key markets, about the value they find in the EURO-MILS platform. We summarized the in-depth discussions in the following chapters.

## Chapter 5 Trustworthiness by Business

### Acceptance: Market Value.

To emphasise the importance of the business acceptance in our project, we quote two speakers at ICT2013 - Digital Agenda for Europe, organized by the European Commission in Vilnius in October 2013.

« All ICT projects should be based on customers' demand »

Burton LEE, ICT in Horizon 2020

« Security is now part of all ICT projects »

Gustav KALBE, Digital security: cybersecurity, privacy and trust

In the project, we have analysed the impact of MILS cross-sectorally beyond the avionics and automotive sectors. MILS is a platform that allows the horizontal integration, which is more open than vertically stacked products. In every industry sector, a trend to such horizontal platforms has been observed (e.g. Davies 2006, "Organising for solutions: systems seller vs. systems integrator"). While there are high-level studies of economic aspects of ICT, (e.g. Anderson 2009, "Certification and evaluation: A security economics perspective") these usually treat security as a negative externality occurring with tightly integrated vertical systems. The objectives of the analysis are to investigate trustworthy ICT from a horizontal platform perspective and to identify market requirements of MILS systems.

#### 5.1 EURO-MILS Business Justification

Embedded systems have kept pace with the advances in general-purpose computing, so that many embedded systems nowadays have CPUs of almost similar power to desktop systems, engage virtualisation techniques, and can efficiently replace (e.g. in terms of computation, energy consumption, interconnections) multiple distributed simpler devices.



Figure 16: EURO-MILS Value Propositions

As the popularity of Embedded Linux and Windows CE shows, from a computing power perspective it is now often feasible to use a desktop operating system on an embedded device. Development for these operating systems is easier and cheaper. However, they are optimised for general average user experience in non-critical and non-secure environments. That is, even rare “kernel panics” or “blue screens” are not acceptable in systems where safety is an issue. Would you be confident to drive a car that presents a real risk to life in having a computer system that could be turned off remotely or make instruments give false reading? And from a security perspective, consumers and companies must be sure that exchanged data between them is secure, that is ensure confidentiality and privacy, availability and integrity. Would the energy company or the consumer accept to rely on smart meter devices that could be hacked to provide fake energy consumption data?

This is where EURO-MILS comes into the picture. The project creates a trustworthy embedded platform that ensures security and safety. The platform is based on the MILS architecture implementing both highly critical and less critical partitions on the same hardware. The platform is certified that allows a greater user confidence in its security capabilities.

As a summary, the EURO-MILS project is working on creating

- a reliable embedded platform
- ensuring security and safety
- by implementing a MILS architecture to support different partitions
- and certified for its security capabilities

Avionics and Automotive, currently, are two main natural markets for the EURO-MILS platform. In the following chapters, we analyse EURO-MILS values in others markets that can be regulated, targeted towards industries or consumer oriented.

## Chapter 6 EURO-MILS Business Values

### 6.1 Reliable Embedded Platforms

Reliable embedded platforms —IDC call them *intelligent systems*— are transforming the embedded industry and driving the value among the Internet of Things. They include high-performance microprocessors, connectivity, and a high level operating system. They often drive a sophisticated user experience and provide the user with relevant data. Traditionally, reliable embedded systems have played a major role in industrial sectors such as:

- Defence, avionics and space,
- Transportation (road and rail),
- Nuclear industry,
- Energy production, distribution and use management,
- Industrial production (automatic, discrete and continuous systems).

They also become increasingly important in many other areas such as:

- Telecommunications infrastructures,
- Medical instrumentation,
- Building and home automation,
- Consumer electronics (mobile, multimedia, games and digital entertainment),
- Logistics (trading and distribution),
- Urban infrastructure (water, traffic, capture the air quality),
- Security (CCTV, means of identification),
- Banking and commercial transactions (payment terminals, smart cards).

#### **6.1.1 Different Domains Share Common Characteristics and Requirements**

When analysing potential opportunities and application sectors, we need to segment the market in order to take into account the industry specificities in regard of the EURO-MILS proposition. We have split sectors in three domains, namely consumer, industrial and regulated domains, which share common characteristics and requirements.

##### **Consumer Domains**

In the consumer domains, manufacturers or operators focus on the consumers. Consumers and competition impose requirements that drive buying decisions: quality of service, price and time-to-market.

To fulfil those needs, manufacturers and operators invite their suppliers and system integrators to offer cost-effective products and systems that deliver high level quality of services.

Consumer markets are characterized by very large volumes<sup>33</sup> in the magnitude of millions of units. Product's turnover is important in the order of months or years. Because of the

---

<sup>33</sup> The worldwide smartphone market reached in 2013 another milestone, having shipped one billion units in a single year for the first time (source [IDC](#))



turnover, consumer oriented manufacturers create products that leverage the standard features of the hardware and COTS software.

From a cost perspective, product design and development costs can be leveraged by the number of product sold. Software costs are low as it can be duplicated. Hardware costs increase as the number of system sold increase.

### Industrial Domains

In the industrial domains, manufacturers or operators focus on professional customers i.e. companies or governments. Dependability and quality of service are the key requirements.

Industrial markets are characterized by volumes much smaller than in the commercial domains. Industrial products have a limited turnover with product lifecycle in the magnitude of 10 to 30 years.

Therefore, to limit the costs, industrial products mostly include standard embedded hardware operated by commercial off-the-self operating system and middleware. Developed by the system integrator, the applications are specific to the customer.

### Regulated Domains

In the regulated domain, suppliers, system integrators and manufacturers focus on creating secure products that need to get certified against security and safety standards.

An authority imposes security and safety requirements that need to be fulfilled by all stakeholders in the chain before the product is authorized to be operated. Embedded systems need to be certified before they can be deployed. In this domain, products with embedded systems, such as airplane or train controllers, often have long live cycles (decade).

The regulation authority can be national, European, international or even industry specific:

- Critical Infrastructure : European Programme for Critical Infrastructure Protection
- Defence : National Minister of Defence
- Avionic : European Aviation Safety Agency
- Space : European Space Agency

In the regulated domains, markets are characterized by limited volumes in the magnitude of ten thousands of units.

The certification process is slow and costly. To enable manufacturers to upgrade platforms to newer devices, substituting one certified component for another while maintaining certification of the entire platform would be a great benefit.

### Summary

Table 4 recaps the three common characteristics by domains





Attribute	Consumer	Industrial	Regulated
Units sold	1 M – 100 M	10 000 – 100 000	100 – 1 000
Development costs	100K € - 1M €	1 M € - 10 M €	10 M € - 50 M €
Lifetime	1 – 10 years	10 – 30 years	25 – 50 years
Cost sensitivity	0,05 €	10 - 100 €	>10 000 €





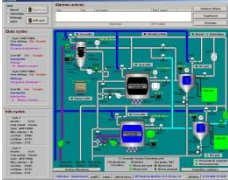



Attribute	Consumer	Industrial	Regulated
Maintenance	“never breaks”	Scheduled maintenance	Aggressive fault detection & maintenance
Safety	None	First levels	High levels
Security	None	First levels	High levels
User Assurance / Certification	By manufacturer	By manufacturer development team and standard organizations	By certification authority
Example	Smartphone	SCADA system	Nuclear power

Table 4: Embedded Systems Characteristics by Domains

### 6.1.2 Embedded Platforms Are Used Everywhere

Embedded systems span all aspects of our modern life. The following table lists some examples of embedded systems applications in various domains but the list could go on and on.

Embedded System	Application	Example	Domains
Home Appliances	Dishwasher, washing machine, microwave, Top-set box, security system, HVAC system, DVD, answering machine, garden sprinkler systems etc...		Consumer Industrial
Office Automation	Fax, copy machine, smart phone system, modern, scanner, printers...		Industrial
Security	Face recognition, finger recognition, eye recognition, building security system, airport security system, alarm system...		Industrial
Instrumentation	Signal generator, signal processor, power supplier, Process instrumentation...		Industrial

Embedded System	Application	Example	Domains
Telecommunication	Router, hub, cellular phone, IP phone, web camera...		Consumer Industrial
Automobile	Fuel injection controller, anti-locking brake system, air-bag system, GPS, cruise control...		Consumer Industrial
Entertainment	MP3, video game, smart toy...		Consumer
Avionic and aerospace	Navigation system, automatic landing system, flight attitude controller, space explorer, space robotics...		Industrial Regulated
Industrial automation	Assembly line, data collection system, monitoring systems on pressure, voltage, current, temperature, hazard detecting system, industrial robot...		Industrial Regulated
Personal	Cell phone, smartphone, personal data organizer...		Consumer
Medical	Scanners, electrocardiographs, electroencephalograph, blood pressure monitor, medical diagnostic device...		Industrial Regulated
Banking & Finance	ATM, smart vendor machine, cash register...		Consumer Regulated


Embedded System	Application	Example	Domains
Miscellaneous	Elevators, treadmill, smart card, security door....		Consumer Industrial Regulated

Figure 17: Domains of Embedded System Applications

These usages demonstrate a large variety of application domains which varies from very low cost to very high cost and from daily life consumer electronics to industry automation devices, from entertainment to academic devices, and from medical instruments to aerospace and transportation control systems. All given examples have a characteristic in common: they are or may be connected to a network and therefore require security.

### 6.1.3 Embedded System Market Description

According to different sources, the worldwide market for embedded technology was 89,2 billion € in 2011, and 104 billion € in 2013. The market will exhibit steady growth at a compound annual growth rate (CAGR) of 6% over the next 6 years and we can expect the market to reach 155.8 billion € by 2020.

The embedded technology market is made up of both hardware (integrated circuits and boards) and software. The majority of the revenue comes from the embedded hardware industry with a 93,6 billion € share in 2013. Projections leads this market to reach 140,2 billion € by 2020.

However, the highest growth rate in terms of revenues comes from the embedded software (operating systems, design automation and development tools). The software segment is expected to grow at a CAGR of 7.8%.

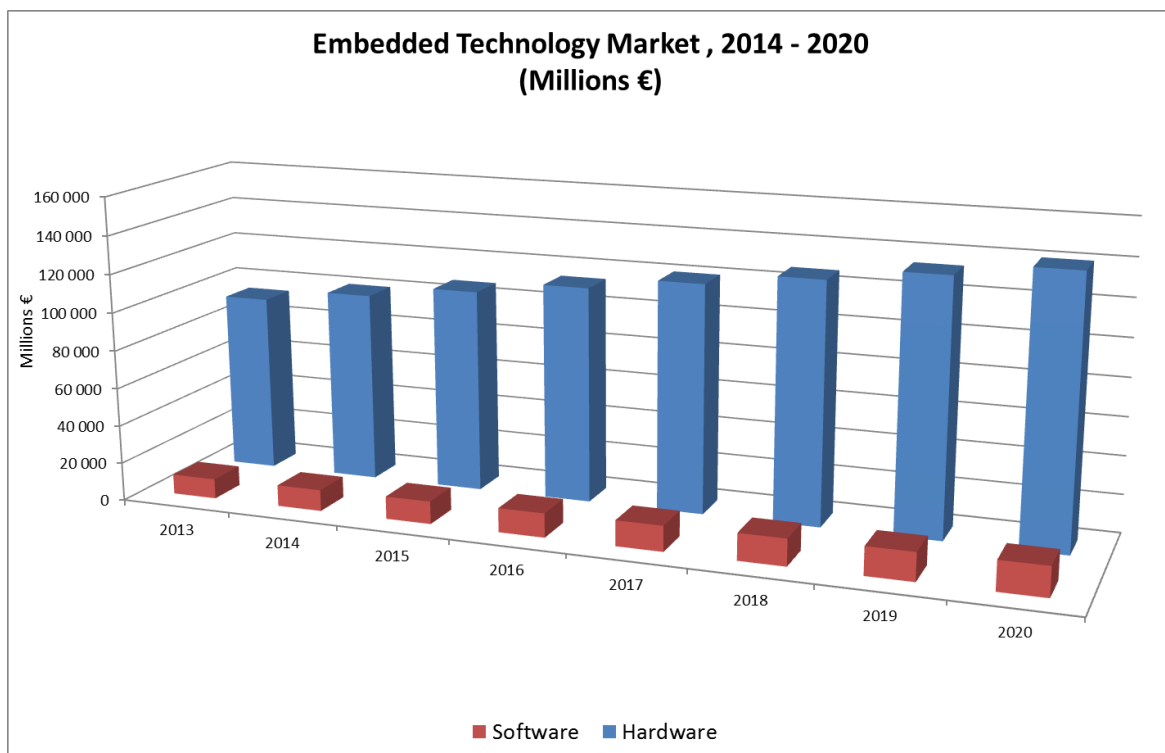


Figure 18: Embedded Technology Market

Markets trend analysis for different application areas indicates that in the last decades the Embedded Systems market has been growing faster than the traditional computing market:

- Approximately 2% of the sold microprocessors are used for IT and PC and 98% for the embedded systems such as cars, trains, medical devices, airplanes, household devices, traffic management systems, in mobile devices etc...
- Embedded systems accounted for 9.1 billion unit shipments in 2013 and are expected to rise to 11 billion units by 2017<sup>34</sup>.

In terms of regional distribution, the Americas (US mainly) has almost half of the total revenues. The other regions, Europe, Japan and Asia/Pacific equally share the rest. Europe has an average growth rate of 22%.

Europe is currently leading the world in industrial sectors such as consumer electronics, telecommunications, automotive, avionics, medical and industrial automation. The value added to the final product by embedded software is often orders of magnitude higher than the cost of the embedded devices themselves.

The value added to the final product by embedded software is much higher than the cost of the embedded device itself. For example, in the case of a modern car, over 35% of its value is due to embedded electronics. This accounts for 90% of new innovations and features in:

- engine management (improved efficiency and reduced emissions)
- safety features (like stability control, antilock braking and airbags)
- comfort (navigation and entertainment features)

Similarly, a smartphone has more features than those of a laptop from a few years ago with internet access, integrated digital camera, global positioning system, video and music player and, of course, a phone!

Embedded systems have a wide applicability. They add value to the final product they belong to. The application of embedded systems is increasing in all sectors. In the next five years, the share of embedded systems is especially expected to increase in the following segments: consumer electronics (41%), telecommunications (37%), automotive (36%), health and medical equipment (33%) and industrial automation (22%).<sup>35</sup>

## 6.2 Targets, Constraints, and Requirements of Reliable Embedded Platforms

Some ecosystems (defence, avionic, energy) serve customers from industries. Others (mobile, home automation, finance, electronics...) serve primarily consumers. Some like automotive serve industry customers that create products and systems bought by consumers.

For the main sectors integrating embedded systems, Table 5 specifies the required characteristics resulting from the evolution towards System of Systems. This table has been adapted from the Final Study Report of the study "Design of Future Embedded Systems" written by IDC on behalf of DG Information Society and Media of the European Commission with the business inputs of the industry panel members. Grey cell means that the characteristic is a key requirement for embedded systems in the considered sector. We indicate the requirements with respect of:

- Criticality exigencies: safety, security and certifications;

---

<sup>34</sup> "Intelligent Systems Transforming the Embedded Industry and Driving the Value Among M2M and the Internet of Everything" - IDC May 2013

<sup>35</sup> Source : Artemis Joint Undertaking

- Distributed architecture management & autonomy of systems;
- User needs: Human Machine Interface, and seamless connection/ interoperability;
- Technological drivers and challenges: multi-core processors & virtualization software, and energy management of small devices.
- Business drivers and challenges: Quality of service, Time to Market and costs

	Criticality Exigencies		Certification	Distributed Architecture	User Needs		Technological drivers		Business drivers		
	Safety	Security			HMI	Connectivity	Multi-core Virtualization	Energy Consumption	Quality of Service	Time to Market	Costs
Automotive											
Aerospace											
Industrial Automation											
Energy consumption point											
Energy Smartgrid											
Healthcare											
Communications											
Consumers											

Table 5 : Required Characteristics for Reliable Embedded Systems

### 6.2.1 Criticality

A system is considered critical when its malfunction for any reason whatsoever, could have serious consequences for the safety of the environment, individuals, businesses or property.

The criticality of a system naturally leads a strong need for risk reduction:

- Reducing the likelihood of a malfunction may have strong consequences
- Reduction of possible consequences of a malfunction.

Critical systems often have strong real-time exigencies as well as low energy consumption requirements.

Nuclear energy production, oil production and refining, chemicals, air and rail transport are the sectors with the highest criticality.

Three elements of criticality and therefore confidence in the systems must be distinguished:

- Dependability (confidence on the implementation of the functionalities)

- Safety (confidence on the absence of serious consequences, even in case of failure)
- Information security (trust in data confidentiality, availability, and integrity)

Some sectors such as Aerospace and Defence have a long and unique experience in Safety. There are more and more safety critical systems in transportation and many new areas such as energy, factory automation, and medical now share similar evolutions. Safety is an enabler of the market as users must trust the value chain of the system.

Information security is about trust in data confidentiality and integrity and in the inability to divert the system for other goals than those specified by the designer. When connected with communication systems, embedded systems must ensure confidentiality of data and must be able to face the proliferation of security threats and the increasing sophistication of attacks. Moreover the impact of missing security on safety can be very serious. The industrial domains (medical equipment, building telecommunications, home electronic, city infrastructures...) show that security is a critical exigency. In this context security is an enabler of trust for the client and damages caused by the security attack are important.

### **6.2.2 Quality of service**

Embedded systems are subject to limitations in terms of volume, weight, power calculation, memory, power and energy consumption. According to defined quality service level agreements, they have to achieve at best, that is without formal guarantee, various non-critical functions such as:

- Control of the physical world (measures, information transmission, and action);
- Optimization features (productivity, efficiency)
- End user interactions with limited interface, availability, or real-time performances
- Seamless connections to enterprise IT systems, including secure authentication
- 

### **6.2.3 Time-to-market**

The Time-to-Market, i.e. the cycle time between identification of a product opportunity and product deployment, can be quite long for embedded systems. For products that have a long lifecycle (avionic, energy production), it is important but not critical. But in short product lifecycle segments such as consumer products, it often makes the difference between profit and loss.

In the consumer area, time-to-market becomes critical because of increasingly competitive markets and consumer expectations for new products. Developers are confronted by greater design complexities and limited windows of opportunity. Finding a balance between the time-to-market and quality of a delivered product within a limited cost structure is a daunting task.

### **6.2.4 Costs**

Cost is almost always an issue. Costs of a system can be split in 3 parts

- Non-recurring engineering costs. They are onetime costs that the manufacturer supports once. They include the design costs, the product development costs and sometime the certification cost.
- Unit costs are all the costs required to manufacture one unit of the system, excusing the engineering costs. It includes the hardware and the software costs.
- Total costs are the summation of non-recurring engineering costs and the costs required to manufacture required units. Volumes have an impact on the total costs,

because copies of hardware have value proportional to their cost where copies of software have virtually no cost.

•

## 6.3 Ensuring Security

Based on the inputs of EURO-MILS industry panel participants as well as a review of the existing literature, we define the embedded system security value chain.

### 6.3.1 Key stakeholders

Production of embedded systems is split up into the production of components and platforms, and the integration of these components and platforms – together with application-specific (hardware or software) parts – to the final product. Typically, single components, such as single chip TV's, are used by system integrators that build devices that are included by manufacturers in consumer electronics appliances such as televisions.

The security value chain includes a high number of actors, interacting with different roles and responsibilities. Within the EURO-MILS context, each stakeholder perceives a specific value proposition. Understanding each opinion can give a collective view of:

- What is important to protect,
- What can go wrong,
- Consequences when it does go wrong,
- Who might try and attack them.

All value chain members can support each other, and define “good security practices” throughout the value chain:



Figure 19: Security Value Chain

Because they have different role, they analyse EURO-MILS and more generally secure embedded system value from a different viewpoint: development, usage, sale, production, or certification:

- Consumers use services provided by the secure products.



Consumers are individuals and represent the end users at the extremity of the value chain. They directly or indirectly use a product or a service provided by the operator and sometime in return produce information and data that can be used by the operator. They put a high requirement on the operator or the manufacturer to deliver a good value for money. This value for money does not only measures the cost of goods and services, but also takes account of the mix of quality, cost, resource use, fitness for purpose, timeliness, convenience, and specifically in our context, security. However, the security value is subjective, difficult to measure, intangible and misunderstood.

Readers and authors of this document are (also) consumers.



- Suppliers produce secure embedded systems



Hardware manufacturers produce the hardware part of the embedded system. They typically have tight constraints on both functionality and implementation. In particular, they must guarantee real time operation reactive to external events; conform to size and weight limits, budget power and cooling consumption, and meet tight cost targets. From a safety and security requirements, they need to provide low-cost reliability with minimal redundancy. New hardware include security specific features (e.g. ARM Trust zone).

Texas Instruments is a hardware manufacturer.



Software vendors produce the real time operating system and necessary middleware required to operate the hardware. Modern RTOS vendors offer the support of multi-core architectures with a resource and time partitioning model making the development of concurrent applications on multi-core platforms easier. From a safety and security requirements, they need to provide a validated trusted code base to support various applications with different level of criticalities.

SYSGO AG is a software vendor.

- System integrators develop secure embedded system applications



System integrators develop an application specific to the device that includes the embedded system. Applications are developed specifically for a specific device (embedded system and circuit board<sup>36</sup>) according to the manufacturer requirements. Reliable applications are developed according to industry best practices and standards, and sometime a certification process. Going through a rigorous qualification procedure to respond to safety and security requirements, partitioning may be needed to minimize certification costs.

Thales is a system integrator for the aerospace industry

- Manufacturers assemble secure embedded devices in their products



Product manufacturers assemble multiple devices and other parts to create a specific product. They face three business issues that impact their use of secure embedded systems. When few of a particular product are built (e.g. avionic), design costs of the application are of major importance. Conversely, production costs of the hardware are important in high-volume production (e.g. smartphones). Cycle time can be quite long for some industrial products and redesigning to accommodate changing form factors, control algorithms, or functionality requirements may be difficult. Last but not least, as a 100% secure product is impossible, they have to ensure they create the best possible secure product but plan for security updates. If the product has to be certified, an update may require a full recertification.

Airbus is an aircraft manufacturer.

- Operators acquire and operate secure products.



Operators are companies, government agencies, and other organizations. They acquire (rent or buy) secure products to operate them, providing services for their business or consumer customers. The ability to

<sup>36</sup> As the device must interact with the environment, often by monitoring and controlling external machinery, the device includes a circuit board dominated by non-digital components.

effectively provide information security services to protect the organization's information and technology assets has become an operational requirement in all businesses. Due to technology and business changes, they face today two new requirements. Leveraging the Internet of Things, they operate more and more distributed devices connected to their enterprise information systems putting a high requirement on securing the entire information chain. Consumer-oriented businesses have also specific requirements to protect their customers' data. The European directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data implies that the operators follow strict rules when processing personal data regardless of whether such processing is automated or not.

Lufthansa or Air France are airline operators. Deutsche Telecom or Orange are telecommunication operators.

### 6.3.2 Dealing with certification

However, just to claim that a product is secure is not an enough proof to provide trust for the user of this product. More formal processes may be needed to check the security level that product manufacturers thinks to reach and to maintain a chain of trust from the manufacturer (Automatic teller machine, smartphone) to the operator (banks, telecommunication) and to the final end-user. Indeed, without this assurance there would be serious economic risks for information processing systems that are essential in the day to day life (payment cards for the banking structure, SIM card in the world of mobile telephony, health card, protection of the networks with the firewalls, etc.). To satisfy the need of trust in the security of the IT products, the industries with the help of governments have thus set up the Common Criteria certification to ensure a security chain of trust. CC context adds two stakeholders in the security value chain:

- Evaluators perform an independent security evaluation of products for certification



Evaluators are accredited testing laboratories. They evaluate a product with respect to security requires identification of the customer's security needs and an assessment of the capabilities of the product. Based on a Security Target, a document provided by the supplier, the system integrator or the manufacturer that describes all security features included in the product, the laboratory tests the product to verify the described security features and evaluate the product against the claimed Protection Profile, a standard set of security requirements for a specific type of product.

T-Systems, in Germany or Thales Communication & Security in France are accredited CC evaluation laboratories

- Certification authorities issue security certificates



Certification authorities are industry or domain regulation authorities that require a certain level of security in the products operated in their area. They review the results of the test and evaluation to determine if the system meets their security requirements and can operate at an acceptable level of risk. The certification authority in view of the evaluation report, decides or not to issue the certificate.

European Aviation Safety Agency is the authority in charge of the European avionic industry.

### 6.3.3 Security Market Trends

The widespread deployment of embedded systems is changing our environment and all industrial activities and services. The emergence of the Internet of Things, joining the physical world to the Internet via embedded systems, amplifies significantly this evolution.

In established brick-and-mortar businesses (automotive, aerospace, telecommunications, security, energy, logistics ...), the embedded systems (hardware & software) are already accounting for nearly a third in the costs of global R & D product<sup>37</sup>.

Formerly reserved to critical environments, safety and security are becoming important requirements in areas of "non-critical" environments where quality of service and time-to-market requirements are keys. This trend results in the blurring of boundaries between domains embedded in so-called "critical" (aviation, rail, energy) and areas of "non-critical" systems (smart home, consumer electronics, e-health, digital city, smart-grid, etc...).

Industrial Sector	% of embedded system R&D in the final product	% of software R&D in embedded system
Automotive	56%	41%
Avionics / Aerospace	54%	30%
Industry / Automation	48%	55%
Telecom	58%	30%
Consumer / Home	62%	59%
Medical	53%	14%

Figure 20 : Embedded Systems Usage (source VDC 2007)

Coexistence and interactions on the same platform of critical and non-critical functions will lead to the adoption by different ecosystems of the same standard technologies and methodologies.

## 6.4 Virtualization for Building Independent Partitions

Modern electronic systems used in avionic and automotive domains but also healthcare, energy, etc... combine applications that have real-time and no real-time requirements and different levels of security. Using hypervisor-based systems, vendors can build partitioned systems where partitions are temporal and spatial isolated. They can use the appropriated OS for each application and even execute mono-core OS in a multicore platform.

Virtualization is a mature technology, and industrial risk is limited. Virtualization brings many technical advantages that many businesses are looking for.

- Consolidate previously separate functions to reduce system size, cost, and power
- Bring innovation to market faster while preserving legacy code
- Enhance security, safety, and availability through application isolation and software redundancy

Virtualization brings multiple business advantages

- It allows development of new products that require the coexistence of hard-real time applications with non-critical ones over the same hardware without compromising the critical aspects of the system.

<sup>37</sup> Software Intensive Systems in the future, TNO/IDATE, September 2006

- It allows development of new products and services that integrate multiple systems of different security levels in the same hardware with guaranteed security of the handled information.
- It simplify products architectures due hardware sharing, resulting in improved product competence.
- It lowers development equipment costs, reduce the size, weight and power consumption of products because of hardware sharing.
- It allows development of new products with real-time characteristics, based on existing non-critical legacy code. Re-use of non-trusted legacy code (e.g. code developed for Linux, C, etc.) at zero adaptation cost and man-time effort to implement safety critical applications.
- It increases robustness of the delivered applications, since they will be based on the safety critical and secure infrastructure the hypervisor ensures.
- It reduces the testing costs and increases testing quality, since the system under test will be possible to execute on the same environment with the production system, and under real use situations.

Device and systems manufacturers can integrate COTS operating systems alongside real-time operating systems into their projects to deliver a broader set of capabilities and develop innovative solutions to differentiate them from the competition. For example, a medical device manufacturer can develop a graphical user interface using Microsoft Windows for patient monitoring console while also implementing an RTOS to manage sensors and control with real-time performance, determinism and high reliability, both on the same physical single- or multi-core chip. Industrial control platforms users will be able to update or replace their hardware without changing the operating system or applications as they will only depend on what the hypervisor supports.

## 6.5 Certification To Increase User Confidence

As EURO-MILS is working on a Common Criteria certified platform, we analyse the business value of this certification.

### 6.5.1 A Key Security Standard

CC are considered *the* international market standard for IT security and provides a complete methodology, notation, and syntax for specifying security requirements, designing a security architecture, and verifying the security integrity of an IT product<sup>38</sup>.

Common Criteria impacts everyone that depends, uses, deploys, and manages IT secure products. CC addresses all the dimensions of information security development in providing:

- An opportunity for customers to specify their security requirements,
- An implementation guide for the developers,
- An evaluation strategy for evaluators to justify if the requirements are fulfilled.

---

<sup>38</sup> Hardware of software product

## **6.5.2 Stakeholders Business Value**

Although, consumers may not be aware of the certification and understand its impacts, CC gives the assurance that the application (e.g. e-signature), device (e.g. credit card) or system (e.g. car) they depend on will have the right commonly accepted level of security.

With the Common Criteria, the IT industry has a detailed set of security standards. Customers, system integrators, vendors, as well as evaluators and certification authorities have a common IT product security “language”. Vendors draw upon this language to describe the security features included in their products by describing which Common Criteria evaluations their products have passed. Similarly, customers and their system integrators use this language to identify and communicate their security needs, which enables vendors to design products that meet those needs. Certification authorities use this language to request specific security features in IT products and evaluators apply this language to perform their evaluation.

CC allows customers to apply a consistent, stringent, and independently verified set of evaluation requirements to their IT purchases. Although CC certification does not ensure that a product is free of security vulnerabilities, it does provide a higher level of security assurance through an objective process to ensure that the product performs as documented and that the vendor supports the product in the marketplace with processes to remediate flaws when they are discovered. Customers can compare their specific requirements against CC’s consistent standards to determine the level of security they require. They can also more easily determine whether particular products meet their security requirements.

CC certification provides vendors with a program that can help enable higher security in their development of secure products. CC provides a structured review process for developing more secure products that incorporates sufficient flexibility to address new and emerging threats. Although Common Criteria certification is just one of many factors that can contribute to providing effective security, vendors that embrace the opportunities afforded by the CC can help system integrators and customers build more secure IT systems.

CC is scalable to many different types of products and fulfills many different requirements for security assurance. Furthermore, CC enables vendors to build their IT products in such a way that they can more easily demonstrate that their products meet specified security requirements, and the evaluation process allows them to have their product security evaluated in a consistent and meaningful way by an impartial third party.

Evaluators will use CC recommendations and methodologies to prepare detailed reports about the security features of the products they evaluate. The CC evaluation process allows testing laboratories to evaluate security of products in a consistent and meaningful way.

And finally, the certification authority, often a government agency in charge of managing computer and communication security for the country, will use CC evaluations to increase confidence in the security of IT products used by the administration and regulated companies. By requesting CC-certified products, the authority also communicates government security needs to IT vendors.

## Chapter 7 Understanding Markets Requirements

Beyond the avionics and automotive markets, the EURO-MILS project has decided to analyse if other markets would value its propositions around:

- Security and Safety,
- Virtualisation and Partitioning,
- Certification and User acceptance.

As EURO-MILS project will deliver prototypes for the automotive and the avionics, we focused in the study on other relevant sectors for secure Embedded Systems including industrial automation, telecommunications, consumer electronics/ intelligent homes, and health/medical equipment. General trends as well as specific trends in each sector and their impact on market development were analysed. The analysis is based on quantitative and qualitative data collected from reference studies, interviews with experts within the EURO-MILS industry panel.

### 7.1 Industry Panel

#### 7.1.1 Creation

To get insights from the various industries on EURO-MILS value propositions, we started an extensive survey. Objectives of the survey were to understand the requirements in potential industries such as energy, medical, telecommunication, finance, smart homes, etc.

To start the survey we contacted by e-mail 245 professionals in various industries using a personalized invitation (see Figure 21).

Dear S█████ D█████

J█████ R█████ from SYSGO advised me to contact you.

I am Christophe Toulemonde, Director of JEMM Research, an IT European analyst and consulting company, member of EURO-MILS, a 3 year project co-financed by the European Commission.

The mission of the EURO-MILS project is to develop a solution for secure and safe embedded platforms. They will be based on proven technologies: certified hypervisor PikeOS running on standard hardware such as ARM Cortex A15 and QorIQ multi-core processors. Using some innovative virtualization technology, it will allow implementing both highly critical and less critical applications on the same platform. The solution will be certified against the Common Criteria, a very strict Security international standard. Two application prototypes, in automotive and avionics, will be built during the project, to demonstrate the secure capabilities of the solution.

One of the goal of the project is to evaluate the business and social values of such a trustworthy technology in other key markets such as Healthcare, Utilities, Transports, Finances or Telecommunications, just to name a few. As a key representative of your industry, your opinion is therefore highly valuable.

So I would like to have the opportunity to present you in more details the context and planned outcomes of this strategic European project. Then I would really be interested to understand your views about topics such as:

- Business requirements and potential usages for such a certified secure technology
- Business impact and social acceptance of security and safety for your industry
- Business value of security and safety for your customers and users.

Could we spend some time over the phone at your convenience to start a guided discussion about these topics? The discussion could take 20 minutes or more if you are interested to learn more.

If you don't feel comfortable with the topics or don't have time, can you refer me to someone in your company able to help me?

Thanks you in advance for your help.

Christophe Toulemonde

PS: Be assured that your answers are confidential and will be used in summary form only. I will send you the final report that will be published at the end of the project.

Links :

- EUROMILS [Web Site](#)
- EUROMILS [Announcement letter](#)

Figure 21: Industry Panel Invitation

### 7.1.2 Industry Panel Statistics

From this open invitation, we received 72 direct answers (29%). 53 declined the interview (22%) mostly because of lack of time or expertise on the subject. 22 referred to another person in their organization (9%). In final, 39 accepted the call (16%).

EURO-MILS Industry Panel	Numbers	Percentage
Contacted professionals	245	100%
Including references	22	9%
Answers received	72	29%
Declined	53	22%
Done interviews	39	16%

Figure 22 : Industry Panel Statistics

These good results<sup>39</sup> show that obviously the themes of EURO-MILS (Security and safety, virtualisation and partitioning, certification and user acceptance) are shared by many industries beyond avionics and automotive.

The panel includes contacts that worked for or provide products and services for industries listed in Figure 23.

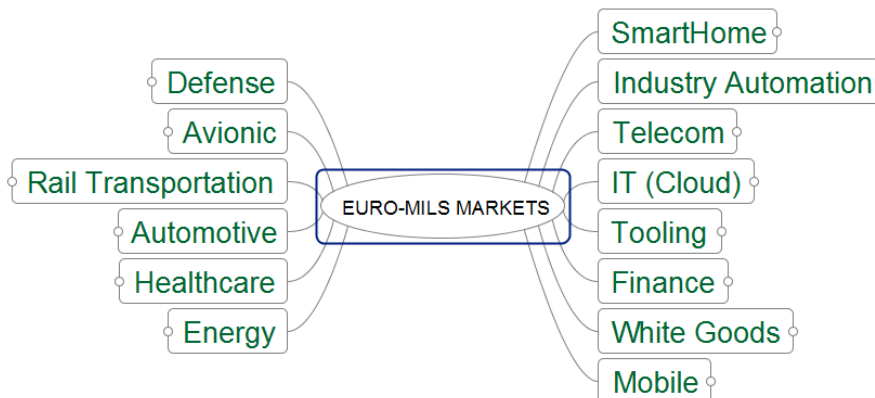


Figure 23: Industry Panel Markets

### 7.1.3 Interviews

Interviews were conducted from May to September 2013 with representatives of organizations or companies involved in the embedded system sector, from R&D labs to large users, by phone. All these organizations and companies are based in Europe with a wide diversity of interests and business models. Interviewees ranged from R&D managers to general, sales or marketing managers, professors, etc.

Interviews had two objectives: the first was to work on project dissemination as we used the opportunity of the discussion to present EURO-MILS. Second, interviews were used to gather quality data around EURO-MILS themes. Interviews were organized in a two-fold

<sup>39</sup> Email marketing analysis (for example 2012 Silverpop Email Marketing Metrics Benchmark Study) suggest that the average email open rate - number of measured opened messages divided by the number of delivered messages.) is around 21% in Europe. Although we didn't track the opening of the email, as we received 29% of answers, we can consider that our open rate was at least two times the average.

discussion starting with a presentation of the project EURO-MILS, followed by a guided conversation on EURO-MILS themes.

As a thread for the discussion, we created a questionnaire. Used only as a guide, it covers the following domains:

- Demographic data of the respondent (name, function, company size...)
- Industry information including security, standard and legal requirements,
- Enterprise value chain from consumers to suppliers including key stakeholders,
- Security, safety, and trustworthiness values and costs including certification,
- Embedded system usage including requirements (real time, integration, partitioning, interoperability...), development and implementation.

To pursue on dissemination, as a follow-up to the call, we sent to the Industry panel members a copy of the EURO-MILS presentation. We continue nowadays to inform them about EURO-MILS activities and results in a newsletter.

#### **7.1.4 Additional contacts**

Relevant trade fairs (*Embedded World* in Nuremberg, *RTS – Embedded Systems* in Paris, etc.) were visited to establish further contacts and get additional input. EURO-MILS presentations to specialized groups (Automotive working group, Smarthome) were made to foster discussion.

## **7.2 Data collection and analysis**

A specific review of the industry literature on the three main subjects (safety and security, virtualization and partitioning, user acceptance and certification) were made.

Main reports or sources for market valuations, growths, trends and a breakdown by product, solution or market application were

### **IDC**

- Design of Future Embedded Systems - 2012

Main coverage: evolution of the Embedded Systems Design (ESD) field towards Systems of Systems, with a specific focus on the industry viewpoint and the emerging opportunities able to improve European competitiveness.

### **Rapport Potier**

- Briques génériques du logiciel embarqué - 2010

Main coverage: Selecting priorities for mastering embedded software technologies in the French market

### **BITKOM**

- Eingebettete Systeme – Ein strategisches Wachstumsfeld für Deutschland - 2010
- Studie zur Bedeutung des Sektors Embedded-Systeme in Deutschland - 2008

Main coverage: Embedded systems market analysis as a strategic growth area for Germany

### **DECISION**

- World electronic industries 2006-2011.



Main coverage: embedded solutions, infrastructures markets, security and government markets, and medical solutions.

### **ARC Advisory group**

- Enterprise Resource Planning Worldwide Outlook.
- Automation Systems for Discrete Industries Worldwide Outlook.
- Automation Systems for Process Industries Worldwide Outlook.

Main coverage: factory automation products and an end users breakdown including power and environment and software expenses including ERP.

### **FAST**

- Study of Worldwide Trends and R&D Programmes in Embedded Systems in View of Maximising the Impact of a Technology Platform in the Area - 2005

Main coverage: an assessment of the current state of the embedded systems, an understanding of the basic drivers and effects of the ES market, and a comprehensive view of the future of embedded systems.

### **Press, Internet**

An extensive research on press article and studies available on the Internet has been done in order to help performing the analysis. Different market data sources were evaluated and expertized in order to adjust them with requested details for this study.

## Chapter 8 EURO-MILS General Perception

On the three EURO-MILS major themes (Security and Safety, Virtualisation and Partitioning, User Acceptance and Certification), and independently of their industry of origin, panel members have given some common feedbacks. In the following paragraphs, we give a summary of the received comments.

### 8.1 On Security and Safety

In this chapter, we elaborate around the comments received from our panel on security and safety business values.

#### ***8.1.1 Despite Understanding Ambiguities, Security And Safety Become Key Requirements***

For our panel, there is not one definition for security as well as for safety and there are still lots of ambiguities in the understanding of the concepts. Regulated industries (e.g. energy) often use security as a generic term that encompasses safety and information security. Some industries like avionic traditionally focused on safety and approach information security as a mean to improve safety.

Driven by market demand and competition, manufacturers targeting consumers (e.g. mobile) have listed information security as a secondary requirement, less important compared to costs or features.

Manufacturers targeting both industries and consumers are driven by security requirements either from a regulator or competitors delivering industry standard compliant products. Because of the growing demand of connected services and the rise of Internet of Things, information security is becoming a key requirement in these domains. The automotive industry is a good example of that phenomenon. In a very competitive environment, the car is more and more connected. And customers are asking for safety and security services such as emergency call, stolen vehicle tracking as well as GPS or infotainment services.

#### ***8.1.2 Systems Are Crossing The Line Toward Criticality***

Dependability of embedded systems targeted for industries with criticality requirements has been studied for many years with a special focus on safety. Several industry specific standards have been published to support safe systems (e.g., DO178B, IEC 61508, and more recently ISO26262). And to ensure the right level of safety, control authorities have enacted rules that must be strictly followed at the risk of refusal of approval of the product.

In markets more orientated towards consumers, embedded systems have historically been simple and used in isolation. However, the panel recognizes that some services they provide become more critical to their customers. Newer systems are becoming more complex, and starting to cross the fuzzy line from non-critical to criticality. Even without entering the right PIN code, a cell phone has to be able to call emergency numbers. And Internet access providers provide set-top boxes with a built-in feature capable of sending and receiving emergency alerts. They can be held as responsible in case of failure of the feature.

### **8.1.3 Some Markets Make Security A Priority**

Information security is a requirement for all members of our panel but its importance depends on the maturity of the industry they belong to.

Panel members from the consumer markets are aware of security but consider it less important than other requirements, mainly because consumers do not value it.

Smart home security is an interesting area. Members of our panel working in this domain recognize that security will become important in the near future but, as of today, it has a limited importance because of other priorities. The many stakeholders coming from different industries such as telecommunication, energy, white goods, construction must focus on either low level integration architecture or high level business models.

Currently, information security seems to be getting the same attention in industrial systems than in enterprise IT systems. Traditionally industrial systems have been used in isolation<sup>40</sup> where almost every enterprise IT system and most of home personal computers are connected to the Internet. But connectivity requirements are changing the game.

As today embedded systems are incorporated in systems that belong to global systems of systems. This overall architecture requires exchange of information between all partners. Security rapidly grows in relevance as embedded software communicates autonomously with other computing systems. A simple vulnerability in an embedded system may compromise the entire security of the system of systems it belongs to.

Even critical embedded application domains, such as avionic or nuclear, which have traditionally put dependability and safety as primary requirements to ensure that everything is done correctly and works as designed, are considering security very seriously. They are concerned by security for safety. With the development of new communication technologies and products leading to real-time integration, threats considerably increase and security requirements become a priority necessary to improve safety.

### **8.1.4 Consumers Do Not Care About Safety And Security**

Today, everybody is concerned by security but people don't make the link between the threat and the service or device they use. Even if they are concerned by significant possible failure modes and security exposures, consumers don't realize their misuse of the technology. It is interesting to see how the Prism scandal<sup>41</sup> will affect the security sensitivity of consumers. For example, there is an impact if a cell phone is not working when the user needs to call for emergency. If a domestic water heater overheats water, there are risks of causing burns. If a thermostat doesn't turn on when needed, it can cause household pipes to freeze. And there is a security concern if an app on a smartphone can transmit owner data without being explicitly authorized.

However, our panel agrees that consumers do not require safe or secure products as such. Concepts are not understood, threats and associated risks are not taken into account when buying a new device. There is still a lot of education and awareness around information security to be done before consumers consider security as a valuable feature of the product they are buying.

---

<sup>40</sup> Managers and engineers think that the SCADA or ICS equipment is not accessible from the Internet. However, a recent project ([SHINE](#)) has collected over 1,000,000 unique IP addresses that appear to belong to either SCADA and control systems devices or related software products.

<sup>41</sup> PRISM, a clandestine mass electronic surveillance data mining program launched in 2007 by the National Security Agency (NSA), was publicly revealed when classified documents about the program were leaked to journalists by Edward Snowden in April 2013.

The customer survey and the Big Data analysis confirm to some extent this vision from the industries, even if consumers are always reacting strongly to any security incident or problem publicly disclosed.

### ***8.1.5 How To Create Secure Products Without Slowing Down Business?***

Consumer-oriented markets are driven by technology innovations and consumer demand. To increase the demand, manufacturers create products that combine innovative features of high quality of service, on time to beat competition and at the right price. In this context, members of our panel recognize that security is less important because less valued by consumers. For years, manufacturers made the decisions regarding the level of security of the product to be sold. Today's consumer markets —especially evident in the mobile ecosystem— revolve around consumer preference for the device and its associated services. Creating secure products for consumers increase the time to market and the development costs for a characteristic not valued by the consumer. However, our panel also recognizes that security concerns become increasingly important as consumers are using their device in more security-sensitive services (e.g. debit or credit transactions in mobile, consumption data for billing transactions in smarthome, health data in eHealth). They are working on making safety and security simple and affordable for non-specialist teams of domain experts in terms of design, development, implementation, and verification. It should also be noticed that embedded systems used in consumer products are less regulated from a safety and security perspective.

### ***8.1.6 Data Privacy Will Impose Security In Consumer Products***

Although data privacy and information security are often used as synonyms, they are not at the same level. Information security is all of the practices and processes that are in place to ensure data isn't being used or accessed by unauthorized individuals or parties. Data privacy refers to the appropriate use of data. When organizations use information that is provided to them, the data should be used according to the agreed purposes. Information security is necessary but not sufficient to guarantee data privacy.

During our discussion, members of the healthcare industry highlighted the importance in their area of patient data they are manipulating. Today, this industry is paying special attention on the storage and transmission of these sensitive personal data in their connected home use medical devices. They also have to comply with strict security rules from the regulation authorities. And because of the revision of the European Data Protection Directive aimed at protecting individuals with regard to the processing of personal data and the free movement of such data, information security will become important to providers of products manipulating such personal data.

### ***8.1.7 Internet Of Things Will Have A Big Impact On Communication Security Requirements***

Looking at the Internet of Things in 2020 and its 26 billion identifiable devices<sup>42</sup> able to exchange data, information security will be at the top of the consumer requirements. However, up to now, embedded systems have not yet experienced as many widely publicized security problems as enterprise IT systems have. Recent events prove that the

---

<sup>42</sup> "[Gartner Says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020](#)". Gartner. 2013-12-12.

potential for widespread, significant impact to society and people is certainly there. What happens if malicious attackers gain control over the set-top box allowing the opening of the rolling shutters of the house?

Our panel members recommended separating in our analysis simple embedded systems and reliable embedded platforms. Simple embedded systems (e.g. a thermometer in a data center, a smoke detector at home) are very cost-sensitive and often do not have a price structure that permits high security. Simple embedded systems are definitively not a target of a EURO-MILS based platform. On the other hand, strategic components of the Internet of Things, reliable embedded platforms will be used as a gateway between the simple devices and the IT applications located in the Cloud. These platforms are a really good target for EURO-MILS offering multiple application support.

### ***8.1.8 Fear Is A Good Motivation For Safety And Security***

For some members of our panel, fear can be a good driver to highlight the necessity of safety and security measures. Security studies for aeronautic purpose have considerably accelerated since the terrorists 'attacks of 9-11.

The Stuxnet worm has help to raise in the SCADA industry key issues on standardising security and protocols and implementing methods to counter security risks.

In less mature markets, specifically consumer markets such as smart home or mobile, we have not encountered yet security incidents that can make big headlines in newspapers. As soon as connected embedded systems will be massively deployed into our homes and our pockets, security as well as data privacy concerns will become more scrutinized by the consumers.

## **8.2 On Platform Virtualization and Partitioning**

In this section, we summarize the different outputs from the panel members around the business value of the EURO-MILS platform (e.g. hardware and software) and especially regarding its virtualization and partitioning functionality. It should be noticed that those characteristics do not deliver direct business value but are the technical foundations for features that actually deliver the value. For example, virtualization can be used to support in parallel a critical application and a non-critical application. In the automotive space, both an effective braking system and a good infotainment system are selling points (business value) enabled by a common technical platform thanks to virtualization (technical foundation).

### ***8.2.1 It Is Becoming A Norm To Operate Independent Software Stacks With Different Criticalities On A Same Platform***

For all industries, one of the key benefits of virtualization is that it enables hardware consolidation, leading to significant reductions in system size, cost, and power. Virtualization provides a transition path for enabling new designs while maintaining legacy applications. Developers can also look to virtualization to help them take advantage of multi-core processors. And from a security viewpoint, virtualization, through application isolation, can significantly improve the security of these embedded devices by separating security-critical applications from less-critical applications.

There is a consensus in our panel on the need to install and operate independent environments (i.e. application and data) with different criticalities levels on the same embedded system. Even in consumer mass markets, we can find examples of this. Triple

play service is nowadays a market standard for Internet access providers and telecommunication operators. It allows the provisioning, over a single broadband connection, of high-speed Internet access and television, and telephone. And providers are pushing for quadruple play that integrates mobility as well. Also pushed by consumers, BYOD<sup>43</sup> is making significant inroads in the business world and requires a strong separation between personal and professional environment so that sensitive company applications and data can be protected to reside securely along unsecure applications and personal data.

### **8.2.2 Leveraging Hardware Security Capabilities May Be Complex**

The trend towards 2020 is the use of multi-core platforms in all sectors. Higher density of functions and multi-core chips can provide increasing capabilities with a good balance between performance and power consumption. This also responds to the trend of using more general purpose hardware when possible in order to lower the cost of systems.

Many members of our panel recognized that they are still adapting their environment to multi-core systems. RTOS require time to adapt to and scale on this new type of platforms. To improve performance, legacy real time applications designed for uni-processor need to move to true multi-thread with true parallelism. Programming for multiple cores increases complexity and requires specific tools and changes in software development habits. All these tasks require skills and expertise from the professional that need to be trained.

Some members of our panel discussed about the advantage of hardware and software, reflecting the *coopetition*<sup>44</sup> between chips makers and software vendors for supporting secure partitions and virtualization seems to be an interesting battle field:

- Today's hardware provides a safe execution environment as the basis for highly-protected system architectures, with minimal impact to the core power consumption, performance or area. For example, ARM's TrustZone technology provides a secure execution environment and basic security services such as cryptography, safe storage and integrity checking to help ensure device and platform security.
- From a software perspective, security is provided by the separation micro-kernel that serves as hypervisor of one or several guest operating systems. For example, SYSGO PikeOS intercept privileged machine instructions of the guest operating system and instead of running it directly on the hardware, first check the rights of the caller against the system configuration and other permission attributes before actual execution

### **8.2.3 Complexity Can Be A Barrier**

In consumer oriented industries (smarthome, mobile...), panel members are wondering how to design and control complex systems with increased quality of service, energy and space constraints in a reduced time-to-market at minimum overall cost. They are working to offer consumers mobility, living, communication, or transportation solutions that require more and more complex technologies. But for some areas, they are competing in markets where the average product life cycle can be less than a year<sup>45</sup>. Therefore, they need to develop their

---

<sup>43</sup> Bring Your Own Device (BYOD) refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

<sup>44</sup> This neologism describes cooperative competition between companies (here: hardware and software vendors) interacting together with partial congruence of interests.

<sup>45</sup> Not long ago, smart device manufacturer HTC estimated the average shelf life of a smartphone to be three years. Now, they figure it's only six to nine months

product using standardized components, refuse unjustified specifics, and concentrating on innovative features and functions that make a difference in the market.

Industrial control systems were avoiding complexity. For decades, enterprises have used SCADA systems to control their industrial systems. Reliable and flexible, they performed well, often implementing limited security features. But many of those critical components that operate today do so in a context that's completely different from the one they have been designed for. Despite the risks inherent to the connection on the Internet and while newer systems may include improved security, many SCADA devices remain deployed for 10 years or more, often in remote areas, resulting in very slow migration to newer, more secure devices.

It should be noticed that EURO-MILS virtualization technology can lower the complexity. In embedded systems, software complexity is the core problem to security and safety assurance. Using a EURO-MILS platform —implementing a micro-kernel based virtualization— applications are no longer forced to unconditionally trust a huge monolithic kernel containing a lot of complex functionalities that the application may or may not need. Instead, each subsystem can choose the amount of code that it wants to trust, thus providing more stability and helping to reduce the complexity of the whole system.

#### ***8.2.4 High Volume Markets Need To Keep Costs Under Control***

For high volume market (portable music players, mobile phones...), minimizing cost is usually the primary design consideration according to the panel. Their engineers typically select hardware that is just “good enough” to implement the necessary functions. And the cost equation is not simple to solve: if manufacturing cost depends mainly on the hardware components of the product, the development efforts increase exponentially as the complexity of the products under design increases and, last but not least, development time must be shorter and shorter to meet time-to-market requirements.

Therefore, the design methodology used by our panel members favour re-use of software components and early error detection. But, as this was mentioned by one of our interviewed, secure development methodologies should become a norm.

### **8.3 On User Acceptance and Certification**

In the following paragraphs, we recap the arguments of the panel members around user acceptance and certification business value.

#### ***8.3.1 Consumers Don't Get Security***

Our panel members agree on the fact that end-users don't understand information security and data privacy and therefore show limited interests for those concepts. This is slowly changing as information security is becoming a business value. There are more and more information in non-specialized newspapers about security leaks and enterprise data breaches. Sensitive domains like banks are educating their customers about information

security<sup>46</sup>. Mobile industry is working hard to provide smartphones designed to provide a very high level of security for their professional customers<sup>47</sup>.

But there is still a long way to go. Nobody but specialized layers reads end-user license agreements (EULA). By ignoring the words of the agreement and clicking the button at the end, we may be agreeing to all kinds of unfair terms such as *"You grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook (IP License)."*<sup>48</sup> But do 1.3 billion active Facebook users<sup>49</sup> really agree on the terms? Do they care about the privacy of their personal data? What about the race between "password" and "123456" for the title of the most common password<sup>50</sup> used in consumer applications (email, merchant sites...) found on the Internet?

In the following chapters, we have somewhat verified this assumption from our Industry panel through our consumer survey and our Big Data analysis.

### **8.3.2 User Acceptance Do Not Imply Certification**

Here again, according to our panel, we can split the market in three categories. Members from the regulated industries (e.g. avionic, nuclear...) require certification of their products. Members of the consumer markets (e.g. mobile, smart home, personal health...) don't rely on certified products as there is no such an authority that governs the market. Product certification impacts its costs and its time-to-market and is not valued by consumers.

Between the regulated and the consumer markets, there is another category where certification is not mandatory but where security (and safety) gives a real business advantage. Such industries do not rely on independent certification to highlight a specific quality of their products. When buying a new car, consumers will look to a brand (e.g. BMW) capable of producing a safe and secure car rather than looking at a specific label. Of course, before a product is allowed to be sold in a particular country, it has received a Certificate of Conformity, a declaration by the automaker that the vehicle has met a minimum set of regulatory, technical and safety requirements compliant with a given approved type. But consumers are not aware of the certificate and don't know the delivering authority.

On the other side, technology-empowered consumers today have access to more information on brands than ever before. They are more likely to recommend, pay a premium for and prefer a brand they trust over others similar to it<sup>51</sup>.

### **8.3.3 Costs And Length Of Certification Vs. Security Requirements**

A security evaluation is a time consuming and bureaucratic process. It impacts the lifecycle and time-to-market. Going through certification will eventually make the product a costly one and late on the market. The highest costs of a security evaluation come from the internal development team of the product vendor requiring extensive time and effort. On one side, costs of evaluation need to be compared to the costs of lost opportunities due to lack of

---

<sup>46</sup> For example, HSBC bank [provides free of charge](#) a security software that locks down the link between the customers devices and the bank so that fraudsters can't listen in.

<sup>47</sup> For example, BULL, a French computer company, has announced in October 2013 a family of secure mobiles and smartphones that ensure confidentiality of voice, SMS, e-mail and data communication.

<sup>48</sup> See Facebook [Statement of Rights and Responsibilities](#)

<sup>49</sup> Source : Facebook [Key Facts](#)

<sup>50</sup> Source : ["Worst Passwords" list 2013](#) – Splashdata - 2013

<sup>51</sup> Source: ["Trust, Not Buzz, Builds Health And Beauty Brand Resonance"](#) - Forrester Research, July 2013



certification, not to mention the cost of losing market share to a competitor who attains validation first. On the other side, this time consuming process may be a showstopper because by the time the work is completed, the product in evaluation may become obsolete. In some cases even minor changes to the product result in costly recertification which often results in only earlier versions of the product with the certification.

Depending on the industries, our panel members were cautious about the costs and the length of the security evaluation compared to the benefits they could get. For some panel members oriented toward consumer products, Common Criteria certification is a process unable to respond to rapidly changing developments in information security technologies. The business value derived from the certification, an acknowledgement that the product delivers state-of-the-art security mechanisms, does not warrant the cost (time and money).

In 2006, the US Government Accountability Office published a report<sup>52</sup> on Common Criteria evaluations that summarized a range of costs and schedules reported for evaluations performed at levels EAL2 through EAL4.

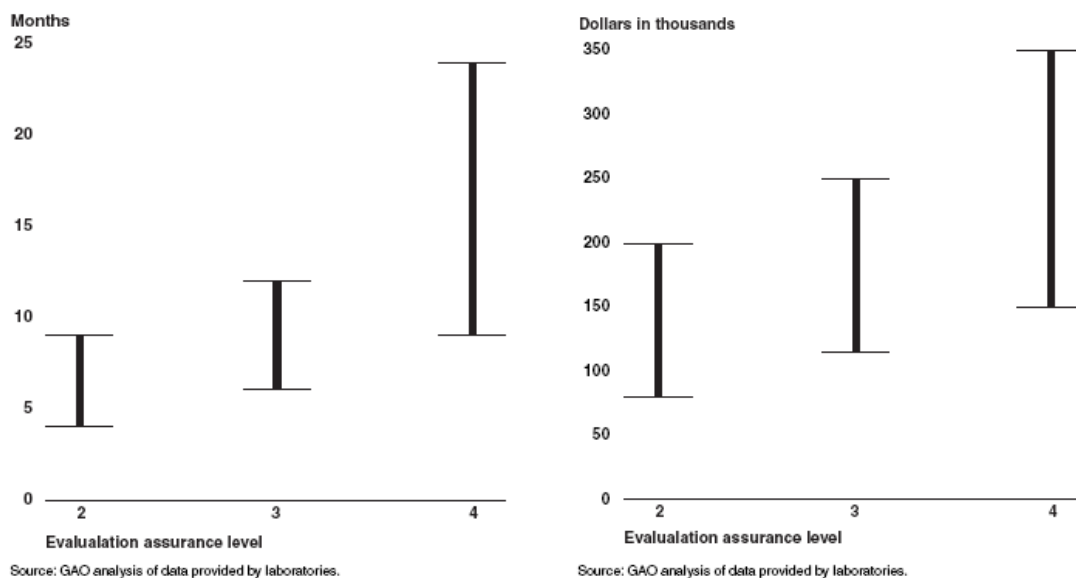


Figure 24 : Impact on Costs and Schedules of CC Evaluations

### 8.3.4 Complexity Of Certification

Members recognize that security certification is a complex process. Common Criteria certifications can be very daunting for internal resources working for the validation process: engineers who manage the process, documentation and communications with the lab and scheme. Also, there is a great deal of documentation required for the evaluation, even at lower assurance levels, and become more complex at higher EAL levels.

On a technical level, the evaluation complexity increases also with the multicore environment and the virtualization. One of the challenges is dealing with the dynamic nature of new threats that appear on a day to day basis. For Common Criteria this has been an issue, as soon as a product is modified, the certification is lost – or need retesting under a certification maintenance programme.

<sup>52</sup> [“INFORMATION ASSURANCE National Partnership Offers Benefits, but Faces Considerable Challenges”](#) –United States Government Accountability Office – March 2006

On the other hand, as a member noticed, the formalism of the certification forces the organization to develop products with rules, methods, processes that lead to high quality products not only from a security perspective but also from a quality of service perspective. That can be an added business value.

## Chapter 9 EURO-MILS Industry Views

When analysing EURO-MILS potential opportunities and application sectors, we segment the market as follows<sup>53</sup> in order to take into account the industry specificities:

- Automotive, including electronic control units in chassis systems, power train electronics, body electronics/security systems, information and computing systems, e.g. for traffic control, and, for example, collaborative active safety systems, autonomous driving;
- Avionics / Aerospace, including commercial aircraft, military aircraft, and satellite systems, and, for example, mission critical information systems;
- Industrial Automation, including manufacturing and process controls, motion controllers, operator interfaces, robotics, HVAC and other controls;
- Transport, water, environmental protection, including, for example, climate change impact, ecosystem monitors;
- Health and Medical Equipment, including patient monitoring equipment, medical therapy equipment, diagnostic equipment, imaging equipment, surgical systems, and, for example, remote patient monitoring, health care for healthy people;
- Energy consumption point (home/building) technology, including intelligent Home, and, for example, net-zero energy buildings, unified safety/security/enterprises networks;
- Communications, including infrastructure, services and end devices, and, for example, integrated container;
- Consumer Electronics, including set-top boxes, Internet access devices, home audio/video, and white goods;
- Energy, including, for example, —smart|| management of energy distribution and consumption.

In the following section, automotive and avionic sectors will not be detailed as they are already the focus of the EURO-MILS Project.

### 9.1 Home Automation

#### 9.1.1 Market description

Home automation<sup>54</sup> is the use of one or more computers to control basic home functions and features automatically and sometimes remotely<sup>55</sup>. One simple definition has been developed by the DTI Smart Homes Project: "A dwelling incorporating a communication network that connects the key electrical appliances and services, and allows them to be remotely controlled, monitored or accessed."

A home automation system may include centralized control of lighting, heating, ventilation and air conditioning, appliances, security locks of gates and doors and other systems. It also

---

<sup>53</sup> This market segmentation is inspired from the segmentation used in the study "Design of Future Embedded Systems" done by IDC on behalf of DG Information Society and Media of the European Commission – IDC 2012

<sup>54</sup> In our discussion, home automation and smart home are synonyms

<sup>55</sup> <http://whatis.techtarget.com/definition/home-automation>

includes various devices, appliances, and systems located inside the house, such as major to small appliances<sup>56</sup> or consumer electronics.

Through the integration of IT with the home environment, systems and appliances are able to communicate in an integrated manner, connected through a home network controlled by a personal computer, and may allow remote access from the Internet.

Home automation brings convenience and comfort, cost savings, energy efficiency, safety and security.

There are a profusion of solutions marketed by several brands. The emerging capabilities of the smarter home enable services throughout many consumer industries. The five service areas already demonstrating early adoption are:

- Entertainment and communication

Beyond the traditional television, set top boxes are now constantly connected to the Internet and offer a wide range of online services such as phone and email services but also videos, music, online shopping and various web services
- Healthcare

Home automation can help elderly people in increasing the ease and safety in performing domestic tasks and to improve communication. Home automation are geared to accommodate people with special needs, including older people and those with physical disabilities and chronic illnesses.
- Energy management

Home automation holds the potential for increasing energy efficiency, decreasing costs of energy use, decreasing the carbon footprint by including renewable resources, and transforming the role of the occupant.
- Housekeeping and maintenance

Connecting home appliances together allow for combining their controls and key functions in order to operate, maintain or repair them. It encompasses appliances that can dial up customer service on their own for troubleshooting to systems that work with a smartphone to let customer monitor and control everything from anywhere.
- Safety and security

Many homes have deployed centralized alarm services using sensors and cameras that can notify the homeowner, selected neighbours, or the police and fire departments in case of a problem. They can also empower family members to remotely check on the safety of children and the well being of elders. Insurances offer discount for homes with such installations.

### **9.1.2 Market Size and Projections**

According to a study<sup>57</sup> released by Juniper Research, the worldwide smart home market will reach \$71 billion by 2018 — up from \$33 billion in 2013. And according to market research

---

<sup>56</sup> Major appliances (aka white goods) include dishwasher, refrigerator, stove, washing machine, and dryer. Small appliances (aka brown goods) are portable machines such as television and wireless sets; microwave ovens; coffee makers; and personal computers

<sup>57</sup> <http://www.juniperresearch.com/reports.php?id=694>

firm MarketsandMarkets<sup>58</sup>, the total European smart homes market is expected to reach \$13.81 billion by 2020 at a double digit CAGR from 2013 to 2020.

The major drivers for the European smart homes market are the regulatory initiatives and the mandatory measures taken by European Union, and energy & cost saving, reduced carbon emissions, ageing population, security and convenience. The major restraints for the European smart homes market are the lack of standardization and initial high costs of the smart homes systems and economic slowdown in the European region that is inhibiting the market growth. Assistance of power line communication and smart-grids are the key opportunities for the global smart homes market.

### **9.1.3 Home Automation Market Players**

The home automation market is seen as a required strategic move for all players (utilities, telecommunication, manufacturers, insurance specialists, healthcare, and service providers). Utilities and telecommunication providers are in a key position as they provide access to the homes and physically connecting home to the grid of resources (Energy, Internet). Appliances makers and consumer electronics are pushing to offer value-added services. Automation and data management technology providers (software editors, system integrators, engineers, designers) are entering this market. And several types of new entrant are positioning themselves in the home automation arena.

Some of the key European players in this market include utilities such as EDF (France), RWE (Germany), Iberdrola (Spain), Enel (Italy) telecommunication providers such as Orange (France), Deutsche Telecom (Germany), Vodafone (UK), appliances makers such as , automation technology providers such as Siemens (Germany), Schneider Electric (France), ABB (Switzerland), Ingersoll-Rand (Ireland), Tyco International (Switzerland), Legrand (France), Hager (Germany), Jung (Germany), and Tyco (Switzerland).

Major global companies such as Apple, Google, Microsoft and now Samsung are pursuing home automation strategies as they would like to become the all-in-one smart-home provider, allowing them to cash in on device installed in the house, plus access valuable personal data about their customers. But industry analysts foresee a fractious market, with many providers, for the foreseeable future.

From all those players, development teams dealing with the embedded platform (hardware and operating system that support applications) are the key group interested by EURO-MILS

This market currently lacks standardization and interoperability of solutions. In 2014, we have seen a lot of announcements in that directions showing that the industry is working on creating interoperability standards but main players are trying to preserve their ecosystem.

- Through the HomeKit software platform, Apple is offering a way to integrate control of home automation devices with iOS devices such as iPhones or iPads
- Google's subsidiary Nest has launched network technology for connected home, encouraging makers of "smart" home gadgets (locks, light bulbs...) to use Thread, a standard for devices to communicate on a network.
- Dell, Intel and Samsung Tuesday introduced a home automation alliance called the Open Interconnect Consortium to create an open-source standard for machine-to-machine communication.
- The Qualcomm-led AllSeen Alliance, which counts LG and Microsoft as two of its 51 members is a similar tentative to a home automation standard.

---

<sup>58</sup> <http://www.marketsandmarkets.com/PressReleases/european-smart-homes.asp>

If home automation market is on the strategic agenda on the supplier side, it is still in its infancy on the demand side as potential end customers question its benefits driving a low adoption rate. The growth of connected home technology and applications open many opportunities. But in order to make the most of these opportunities and ease consumer adoption of new services, the industry must overcome the technological challenges of:

- Heterogeneous home networks
- Multiple ecosystems based on different technologies, protocols and standards
- Proliferation of connected devices
- Explosion of cloud-networking services
- Large number of players with unclear and overlapping value propositions.

#### **9.1.4 Market and EURO-MILS Adherence**

To analyse the adherence between home automation and EURO-MILS, we have focused our discussion with the industry panel members on the gateway that bridges home to the network of services.

The gateway<sup>59</sup> (i.e. cable TV adapters, Internet Service Provider box, or Utility Smart meter) is connecting the local network of sensors, appliances and devices to the Internet or the energy grid.

##### **9.1.4.1 Virtualization Value**

One of the first adherences of EURO-MILS project to the home automation market belongs to its virtualization capability. Networked embedded devices enable the integration of information from the real world to the virtual world where applications live using a home gateway.

Because of the heterogeneity of the devices and systems, the gateway must support different applications, operating systems and communication environments, therefore requires virtualization. But it also requires independence as services may have different service level agreements. For example, “triple-play” services that allow bundling voice, video and data provide services with different criticality levels (i.e. unavailability of the video service may have less impact than unavailability of the voice service preventing tenants to call emergency).

##### **9.1.4.2 Security Value**

The home automation market encompasses multiple ecosystems based on different technologies, protocols and standards. Therefore it is difficult to define a global information security strategy that covers the entire domain. But with the advent of Internet, information security is becoming a critical research topic. And a secure platform such as EURO-MILS makes a lot of sense.

#### **Vulnerability to hackers**

Once a device is connected to the home network, it becomes vulnerable to hackers. A simple google search will show a lot of horrific stories in the press that explain how hackers are targeting home devices. It is increasingly important for device vendors to ensure that reasonable security methodologies are adopted early in product development cycles.

---

<sup>59</sup> Nowadays a complete computer with the appropriate programming, connected to the various devices and systems to be controlled and using a high-speed connection to the service provider

Information security is being part of the quality of service, the performance seen by the users of the networked device.

### **Data privacy**

European and national data protection authorities set strong requirements on the collection, storage, and use of personal data. Privacy problems in relation with cloud computing become difficult due to the very distributed nature of the cloud. A related difficulty is that many users do not spontaneously request privacy. Therefore, there is value in a platform that ensure privacy by segregating uncontrolled apps (ex: games) from a secure environment (healthcare services)

### **Single point of failure**

Gateway becomes a mission-critical piece of equipment. Being central to the home environment, it also becomes a single point of failure. The gateway is a critical component of a complex home automation system that would provoke a total systems failure in case of malfunction. Therefore, gateways should be designed with high availability and reliability requirements. The smartphone used to control the home automation environment is another single point of failure

### **Mandatory requirements**

Regulatory initiatives are encouraging the development of the home automation market: the European commission has set an 80% target of European homes to be equipped with smart meters by 2020. And in this large market, some areas will make difference using secure products:

- Safety and Security services, obviously, need to rely on a secure infrastructure
- Healthcare, particularly home care services for seniors that can help them maintain their independence and stay at home for as long as possible, is another area where European, national or local government agencies will require secure products to be deployed<sup>60</sup>.

#### **9.1.4.3 Certification Value**

Consumers don't get security but understand its impact. They change their behaviour with the service providers after security breaches<sup>61</sup>. For that same reason, companies delivering services on the gateway can't afford to have security breaches in their solutions. Recent incidents<sup>62</sup> have shown that they are very sensible on the topic. Correctly marketed, a security-certified platform has an important impact on user assurance.

In home automation, major objections of consumers are based on safety issues in a broad sense<sup>63</sup>. Instead of insurance guarantees for the appliances users expect a high tech solution that prevents any damages. In fact the safety issue could be used as a sales argument, if manufacturer can prove, using a certification label, that its appliances are safer than conventional ones.

---

<sup>60</sup> Vice-President of the European Commission Nellie Kroes: "None of us is getting any younger. But we all want to know that we will not lose our dignity, respect and independence as we age. The EU is investing in new technology that can support the silver generation – adding not just years to our life, but also life to our years!"

<sup>61</sup> Data breaches have a significant and measurable impact on customers' trust and spending habits, according to an [Interactions study](#). (June 2014)

<sup>62</sup> [Target data breach](#) puts the credit card numbers and personal information of millions of the retail giant's customers into the hands of cybercriminals in late 2013.

<sup>63</sup> « Consumer acceptance of smart appliances » - EU project "Smart Domestic Appliances in Sustainable Energy Systems (Smart-A)" - 2008

Home automation user acceptance does not imply today a formal certification. However, this domain has close link with other domains where security and safety are extremely important. Regulations around safety and security continue to evolve as the global landscape changes to encompass new threats. Regulatory bodies across energy or healthcare industries are leveraging existing successful standards and processes and enhancing them to cover the growing number of threat vectors for safe and secure system operation.

Finally costs and length of the certification may seem incompatible with the time-to-market and the economics of this industry. Both aspects have to be minimized to allow “certified” products be competitive against non-certified products. Composite certification methodologies, as defined by the EURO-MILS project, are certainly an interesting option. An EURO-MILS platform can be certified at a given evaluation assurance level for use in a domain where security certification make sense or is required (i.e. Energy, Healthcare) and allow a safe support for non-critical applications.

## 9.2 Smart Meter

Increasing demand for smart devices such as smart electricity and water meters is a significant driving force for the embedded device market. Smart meters facilitate monitoring and management of energy consumption and ensure two-way communication with the utility. The usage of multicore processors in embedded systems in order to facilitate low power consumption and higher efficiency is also a major growth driver.

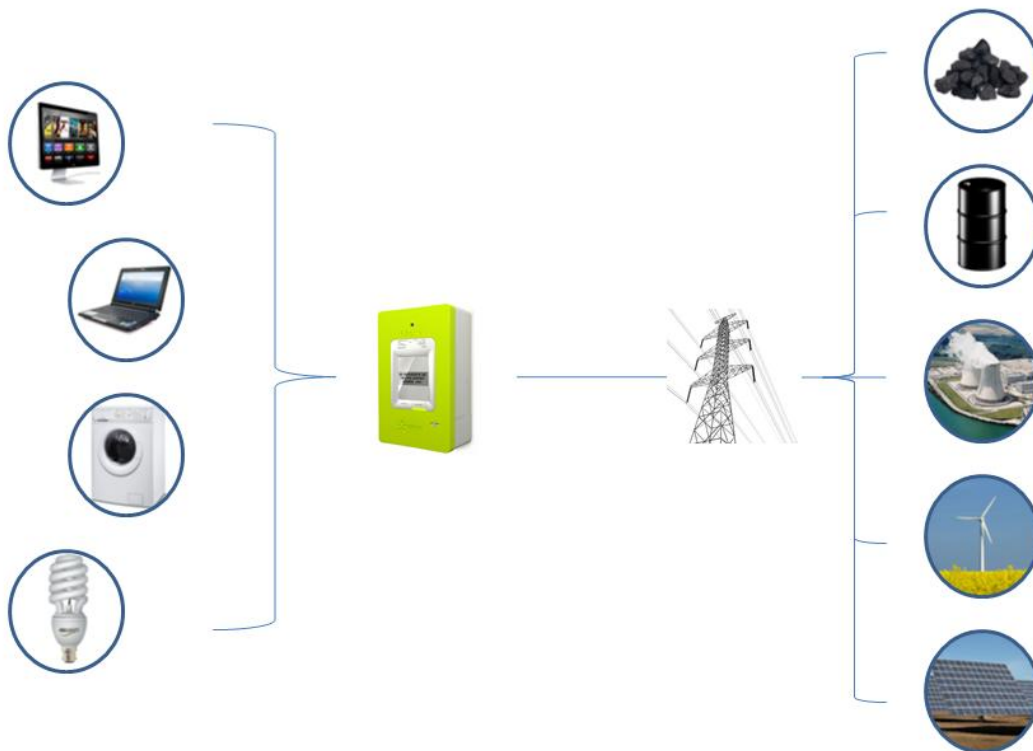


Figure 25 : Smart Meter Linking Consumers To Producers



### **9.2.1 Market description**

Smart grids and smart meters are fundamental components of the European energy strategy. A smart grid<sup>64</sup> as an upgraded electricity network to which two-way digital communication between supplier and consumer, intelligent metering and monitoring systems have been added. Smart metering is an inherent part of a smart grid. It consists of an electronic meter that records consumption of electric energy and communicates that information to the grid operator and energy supplier for monitoring and billing purposes. Smart meter interfaces with other devices, such as in-home displays, smart thermostats and appliances, home area networks, advanced control systems, and more.

Thanks to this information, the grid operators can better plan the use of infrastructure and balance the system, for instance in terms of integration of renewable. Smart meters provide power companies with means to better balance energy production for the grid between peak and off-peak hours. Also, it allows them to offer different billing rates for different times of the day, rewarding people for using more of their power load in off-peak times. The result could be lower power bills for homeowners.

On the side of the user, consumers are able to directly control and manage their individual consumption. A smart meter provides energy consumption in real time, allowing homeowners see the usage of power and watch instantly how different activities affect the total outcome. The consumers with smart meters installed have reduced their annual energy consumption by around 10%. As on average EU households pay 640 € per year in electricity, they could save more than 60 € per year with a better management of their consumption thanks to smart meters.

### **9.2.2 Market Size and projections**

The market research and consulting firm, Frost & Sullivan, has forecasted smart meter market revenues<sup>65</sup> to increase from \$318 million in 2010 to \$1.93 billion in 2017. During the same period, units sold will increase from 2.9 million in 2010 to 30.5 million in 2017.

Worldwide shipments of smart meters are expected to peak to grow from 94 million annually in 2014 to 116 million in 2023<sup>66</sup>. In Europe, large projects that will account for some 93 million new meters by the end of 2020 are in the works.

The prospects for the smart meter market in Europe over the next decade are extremely positive, thanks largely to the EU Directive. With most countries in the EU yet to start their smart meter deployment, growth is forecast to increase strongly year-on-year for the entire decade. A report by the European Commission<sup>67</sup>, released in June 2014, measures progress on the deployment of smart meters across the EU. To date, Member States have committed to rolling out close to 200 million smart meters for electricity and 45 million for gas by 2020 at a total potential investment of €45 billion. Penetration stood at 22 percent at end-2013 and is expected to rise to 60 percent by 2019. By 2020, it is expected that almost 72% of European consumers will have a smart meter for electricity while 40% will have one for gas<sup>68</sup>.

---

<sup>64</sup> [http://ec.europa.eu/energy/gas\\_electricity/smartgrids/doc/20110412\\_memo.pdf](http://ec.europa.eu/energy/gas_electricity/smartgrids/doc/20110412_memo.pdf)

<sup>65</sup> Source Frost & Sullivan: [Europe to Experience Five-Fold Growth in Installed Base of Smart Meters by 2017](#)

<sup>66</sup> Source Navigant Research: [Smart Electric Meters, Advanced Metering Infrastructure, and Meter Communications: Global Market Analysis and Forecasts](#)

<sup>67</sup> Source [Benchmarking smart metering deployment in the EU-27 with a focus on electricity](#)

<sup>68</sup> The European Commission has downgraded its target for 80 percent of households to have smart meters installed by 2020 to 72 per cent as just over half the member states are committed to meeting the 2020 deadline.

Estimates vary, but the cost of a smart metering system averages between €110 and €250 per customer, while delivering benefits per metering point of €160 for gas and €309 for electricity along with, on average, 3% energy savings.

### 9.2.3 Market Players

Europe is a push market where the smart meter and smart grid markets are legislation driven. There is region-wise disparity due to the different regulatory challenges faced by each country, thus having a direct impact on implementation. The competition among manufacturers, utilities, ICT, network, remote monitoring and automation companies is high and it is forecast to increase along with new participants entering the market.

The European market is currently dominated by a mix of European and North American players. Leading the pack is US-based Echelon and Itron, Landis & Gyr from Switzerland, Elster (Germany), Sagemcom and Maec (France), Vattenfall (Sweden). Other key players include Xemtec, Secure Together, Kamstrup, and Iskraemeco.

An essential requirement for the successful deployment of smart metering is the standardization of the new technologies and systems with manufacturers and users co-operating to enable the effective integration of each individual component. Probably the most important standardization activity in recent years is related to the European Commission mandate 441<sup>69</sup> and accepted by CEN, CENELEC and ETSI to develop an open architecture for utility meters involving communication protocols enabling interoperability (smart metering).

Enel : A rollout almost completed in Italy

It's over 10 years now that Enel, the Italian utility, has begun with the installation of electricity smart meters, data concentrator devices and remote metering management system.

Enel replaced old electromechanical meters with electronic ones, installing 32 million of them in only five years. Today this project, so called Telegestore, represents the largest and most widespread remote management infrastructure in the world and is a benchmark for all energy distribution companies:

- Over 32 million devices installed directly by Enel Distribuzione in Italy;
- 4 million devices supplied to other national distribution companies;
- 13 million electronic meters that Endesa is installing in Spain;
- Over 1 million devices supplied to other European utilities.

Here below the main figures of Telegestore in 2010:

- 330 million readings a year;
- Over 1 million annual contractual operations managed remotely without on-site assistance;
- 30,000 tonnes of CO2 emissions saved each year thanks to the efficiency of remote management, as companies no longer have to use polluting vehicles for assistance and consumption readings.

The PRIME Alliance is working on providing an open interoperable standard for advanced meter management and smart grid. The framework will allow multiple vendors to be

<sup>69</sup> <http://www.cen.eu/cen/Sectors/Sectors/Measurement/Documents/M441.pdf>

operational within the same distribution network in one common system architecture. Membership includes utilities, meter and semi-conductor chipset manufacturers, IT, service and consultancy companies, research establishments and other smart grid industry related companies.

### 9.2.4 Market and EURO-MILS Adherence

The Commission has recommended ten common minimum functional requirements for energy smart metering systems<sup>70</sup>. These functionalities capture the essential elements that a smart metering set-up should have to benefit all stakeholders —the consumer, the metering and system operator — while enabling, in a secured and safe environment, commercial aspects of supply/demand and the integration of distributed generation.

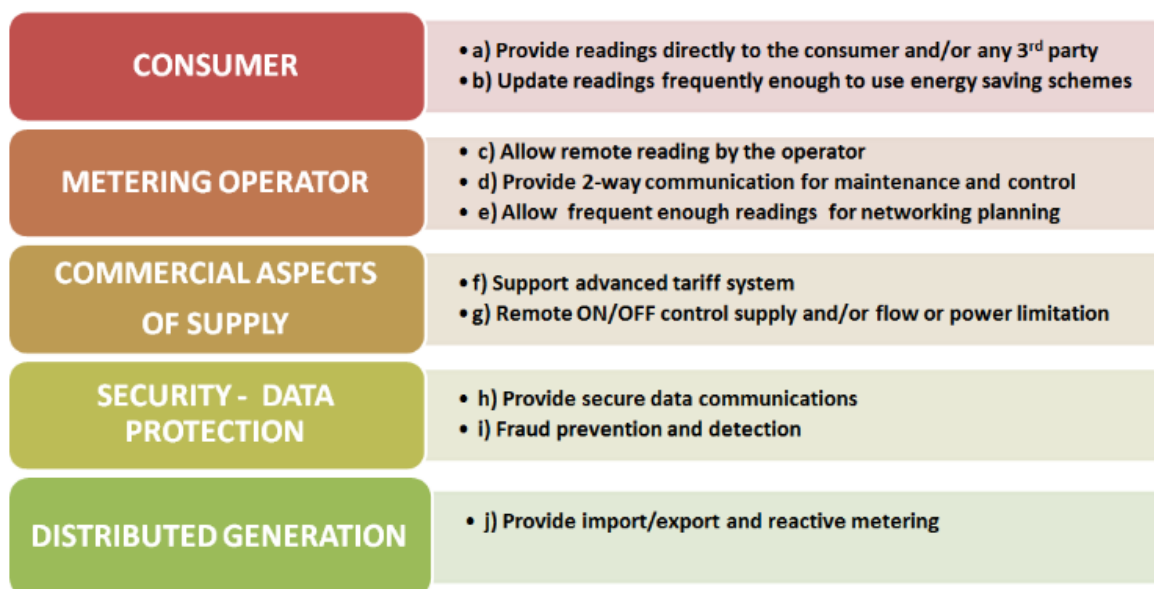


Figure 26: Functional Requirements For Energy Smart Metering System

The EURO-MILS platform offers the right set of building blocks to support the ten common functional requirements for smart meters.

#### 9.2.4.1 Virtualization Value

EURO-MILS virtualization allows to securely specializing partitions to specific requirements. It allows a software architect to build multiple partitions on top of the EURO-MILS platform that can host real-time operating systems, run-time environments or APIs along with their world of application programs. For example, a partition could be allocated to support the graphical user interface application (req a), another independent partition would offer secure 2-way communications allowing secure exchange of real-time data with the grid (req d), a partition to manage securely the local storage (req f) and a partition, leveraging real time capability of EURO-MILS, would control the metering feature to update reading frequently (req b). This would allow turning off the highest source of consumption during the times the unit consumption of energy has a higher price compared to the other hours and turning it back on when the tariff is lower.

<sup>70</sup> Source EU Report: [A joint contribution of DG ENER and DG INFSO towards the Digital Agenda, Action 73: Set of common functional requirements of the Smart Meter](#), October 2011.

### 9.2.4.2 Security Value

The end-to-end smart metering system has many areas of potential threat and risk:

- Home devices;
- Microgeneration devices (such as solar panels and domestic wind turbines);
- Communication links between home devices and the smart meter;
- The smart meter;
- Communications links between the smart meter and the data communication company
- The data communication company
- Communication links between the data communication company and suppliers, network operators and third parties; *f*
- Suppliers, network operators and third parties

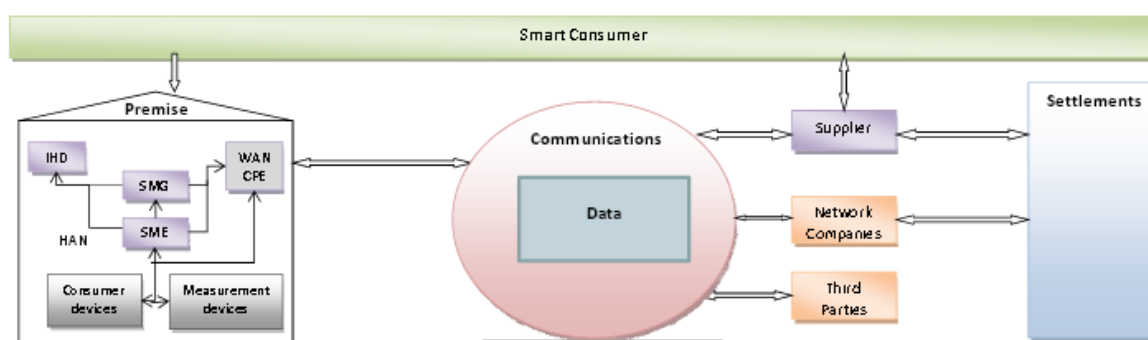


Figure 27: Security Compliance Framework

To be accepted by consumers as well as providers, the smart meter infrastructure must develop a privacy and security compliance framework to ensure:

- Integrity and availability of the data transferred across wireless communications is maintained;
- Metering and communications equipment is tamper proof and has appropriate tamper alarms;
- Meters are only accessed by authorized persons and only for those activities for which they are authorized, through appropriate security controls;
- Meters can resist infiltration from unauthorized access and have their software updated to prevent emerging risks;
- Assurance around the development and maintenance of metering systems;
- Authorized data controllers protect data and access to data that has been communicated from the meter

Building a platform that supports security and data protection (req h and i) as well as remote metering (req c) requirements needs an underlying platform such as EURO-MILS:

- Encryption of the data sent or received by the meter
- Authentication procedure between meter and local / remote reader
- Prevention of read and write (modify) the program code stored in the meter electronics

### 9.2.4.3 Certification Value

Finally, although today no official certification is required, consumers' data protection concerns and the rise of cyber risks will drive strong regulations. Consumer organizations are concerned that patterns and profiles could be mined for marketing and advertising, or price

discrimination, and is asking the European Commission to consider legislating to protect consumers. They want the government to make sure consumers only give information beyond that required for billing and regulatory purposes with explicit consent and full understanding of what the data is being So data privacy and information security could be enforced by certification.

On the security side, the ability to connect and disconnect gas and electricity supplies remotely into the system will allow consumers to switch easily between providers and fight energy theft, but the function could create a "strategic vulnerability" to blackouts from "a nation state attacker, a terrorist or even a criminal group"<sup>71</sup>. Authorities will require companies to fulfil a set of data security requirements to combat identified risks before they can gain licenses to provide smart metering services. Companies will have to carry out security risk assessments, and there will be annual checks from independent data security auditors.

Again, this is an interesting area where security certified products such as the EURO-MILS platform can make a difference.

## 9.3 Healthcare Information Technology

### 9.3.1 Market description

Smaller, faster, smarter and connected are the attributes that describe embedded systems development but also sum up the trends affecting the medical market. Medical devices have been shrinking from room-sized to handheld-sized devices, perform more tasks more quickly and accurately than ever before, and are becoming connected tools to interoperate with other devices.

eHealth, where the EURO-MILS Project offers value, is defined by the World Health Organization as the use of information and communication technologies for health<sup>72</sup>. For the European Commission, eHealth means using digital tools and services for health. It covers the interaction between patients and health-service providers, institution-to-institution transmission of data, or peer-to-peer communication between patients and/or health professionals<sup>73</sup>.

In its broadest sense, eHealth is concerned with improving the flow of information, through electronic means, to support the delivery of health services and the management of health systems. Using ICT-based tools and systems gives patients more information, and more involvement in their healthcare, they improve access to health advice and treatment and can make national healthcare systems more efficient.

---

<sup>71</sup> Source : "On the security economics of electricity metering" - Ross Anderson and Shailendra Fuloria  
Cambridge University Computer Laboratory

<sup>72</sup> <http://www.who.int/ehealth/en/>

<sup>73</sup> [http://europa.eu/rapid/press-release\\_MEMO-12-959\\_en.htm](http://europa.eu/rapid/press-release_MEMO-12-959_en.htm)

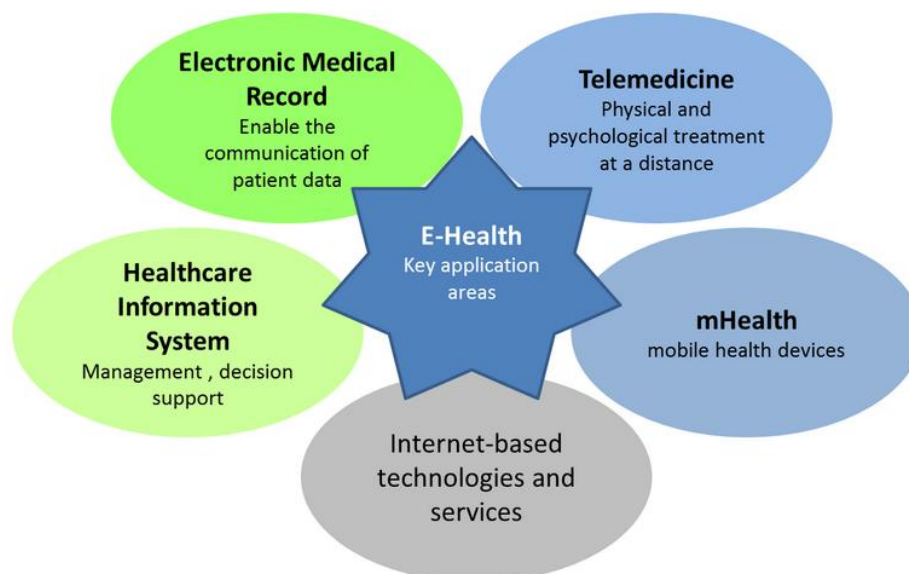


Figure 28: eHealth services

eHealth encompasses a range of services at the edge of medicine and information technology, including:

- Electronic medical record (EMR), a systematic collection of electronic health information about an individual patient being shared between different healthcare professionals (GPs, specialists etc.),
- Telemedicine, a remote management of patient condition that permits communications between patient and medical staff, and transmission of medical, imaging and health informatics data. Telemedicine platforms can be deployed directly in the patient's home.
- Healthcare Information Systems (HIS), the management of administrative tasks surrounding health.
- mHealth, the use of mobile devices for collecting health data (including real-time monitoring patient data), and delivering healthcare information to practitioners, researchers, and patients.

Type	Date	Auteur	Profession / Spécialité	Titre
CR d'admission	03/01/2011	CABINET M. SPECIALIS... SPECIALISTES1705.RVBE...	Médecin - Pneumologi...	tgh
CR de bilan fonctionnel (par suite de médical)	03/01/2011	CABINET M. SPECIALIS... SPECIALISTES1705.RVBE...	Médecin - Pneumologi...	erit
CR d'anesthésie	27/12/2010	CABINET M. SPECIALIS... SPECIALISTES1705.RVBE...	Médecin - Pneumologi...	kund27_titre

Figure 29 : French Electronic Medical Record

The eHealth industry initially supported the work in hospitals and clinics mainly for diagnosis and treatment purpose. It is undergoing a fundamental shift as demand increases for services outside hospitals and medical clinics.

Many healthcare systems today are deployed outside the data center or hospital network—in mobile locations, community clinics, and even in patients' homes. Remote patient monitoring reduces the number of visits of a patient to clinics. Home care systems help the healthcare professionals and providers to manage patients' treatment after their discharge from hospital. In addition increasing aging population and growing concerns of chronic diseases are also boosting the market for eHealth.

There are many embedded systems used in healthcare such as diagnostic systems (e.g. imaging or monitoring systems), or interventional systems. Healthcare embedded systems are developed following generic requirements of:

- Unattended mode  
They are special-purpose devices, and equipment that must run unattended healthcare applications and manage data in a self-contained manner.
- Safety and Security  
They have to be protected from physical hazards (radiation, voltage, heat/cold, moving parts). They also need to be secure to avoid any clinical errors
- Ease of use  
They need to be easy to learn not only for experienced operators and efficient in routine use
- Image and signal quality  
They need to provide excellent images or signals that are easy to control and reproducible.
- Connected  
They must be able to connect to the medical infrastructure, such as EMR across care providers, HIS, departmental systems (e.g., cardiology, radiology...), picture archiving systems, or clinical decision support systems.

### **9.3.2 Market Size and projections**

In 2010, the global medical device market was estimated<sup>74</sup> around \$296.81 billion with Europe representing around \$90 billion.

The size of the global eHealth market varies largely depending on the methodology and definition of what can be classified as eHealth. Estimates of recent market research range from \$96B to \$160B, with 5 year growth rate of 12% - 16% from 2010 to 2015.

The global market for telemedicine is set to grow from €7.2bn in 2010 to €19.3bn by 2016<sup>75</sup>. Another estimate has evaluated the telemedicine market growth from \$9.8 billion in 2010 to

---

<sup>74</sup> Source : Frost & Sullivan

<sup>75</sup> Source : ["eHealth can provide 'triple win' situation"](#), Neelie Kroes, EU VP for the digital agenda, April 2014

\$11.6 billion in 2011, and expected a continuous expansion to \$27.3 billion in 2016, representing a compound annual growth rate of 18.6%<sup>76</sup>.

According to GSMA, the global mHealth market will be worth approximately \$23 billion by 2017. Beyond mHealth, the digital health and wellness market enabled by digital technologies (mobile applications, devices) is also rapidly growing. The convergence between wireless communication technologies and healthcare devices and between health and social care is creating new businesses. Around 100,000 health and wellness apps are already available across Apple's AppStore, Google Play and on other global platforms. So far, more than 200 million individuals have downloaded wellness apps.

The Healthcare industry faces some major challenges where eHealth is seen as providing answers:

- Providing for an ageing population with increasing prevalence of chronic illness, which is increasingly expensive to treat;
- Improving patient safety and reducing errors;
- Supporting patients to become informed consumers who take an active role in their own health care.

There are many incentives for transformation of the Healthcare industry. First, Healthcare spending has increased dramatically over the past half century<sup>77</sup> and is estimated to reach 6% of GDP by 2020 in OECD countries<sup>78</sup>. The rising proportion of older people is placing an additional constraint on healthcare spending. Public authorities are creating plans to cut healthcare costs. And improvements in technological capabilities of medicine are expected to play a large role in that matter.

Another trend is a strong demand to reduce market fragmentation and lack of interoperability. Because health is such an information intensive sector, it is currently estimated that redundancy and inefficiency account for 25-40% of costs. eHealth is capable of providing increased efficiency in data handling and information transfer. Medical systems operate in a context of other systems that today are not integrated and users have to deal with heterogeneous disparate healthcare IT and embedded systems.

Specifically on embedded systems, companies working on imaging systems are improving performance of their devices with strong increase in data rates, sophistication of processing algorithms, and advance user interfaces to ease the use of the device. The embedded systems are today more and more connected to bring to its users the gathered heterogeneous medical mass of knowledge.

### 9.3.3 Market Players

The key players in the market are McKesson Corporation (U.S.), Epic (U.S.), Cerner Corporation (U.S.), Carestream Health, Inc. (U.S.), Athenahealth, Inc. (U.S.), Siemens Healthcare (Germany), Medical Information System, Inc. (U.S.), Allscripts Healthcare Solutions Inc. (U.S.), GE Healthcare (U.K.), Agfa Healthcare (Belgium), NextGen Healthcare Information System, LLC (U.S.), Phillips Healthcare (The Netherlands), Hewlett-Packard (U.S.), among others.

---

<sup>76</sup> According to BCC Research study of March 2012, quoted in "[eHealth Action Plan 2012-2020 - Innovative healthcare for the 21st century](#)" – European Commission - December 2012

<sup>77</sup> Spending in the U.S. health care sector totaled \$2.7 trillion in 2011, up by a factor of 3.9 from the \$698.3 billion (in 2011 dollars) spent in 1980 – Source : 2013 Economic Report of the President "[reducing costs and improving the quality of health care](#)" – The White House

<sup>78</sup> Price, Waterhouse, Coopers study, HealthCast 2020: Creating a Sustainable Future, 2006



Instrument companies or departments like GE Healthcare, Phillips Medical Systems, Siemens AG, McKesson Provider Technologies are concentrating on medical right from small microprocessor controlled blood pressure monitoring systems to severely complex ECG, EEG systems.

On the IT and software side, large multinational consulting and system integration companies such as CSC<sup>79</sup> or IBM<sup>80</sup> have developed a strong healthcare practice. Global software vendors such as Oracle or SAP are developing solutions that integrate enterprises applications to the medical domain. For example, Philips and salesforce.com have announced in 2014<sup>81</sup> a strategic alliance to deliver an open, cloud-based healthcare platform, leveraging Philips' medical technology, clinical applications and clinical informatics and salesforce.com's expertise in enterprise cloud computing, innovation and customer engagement.

Digital health care has become one of the fastest growing trends over recent years as demand for health care and support grows around the world. A survey<sup>82</sup> from the Consumer Electronics Association (CEA), the organizers of Consumer Electronics Show in Las Vegas, conducted last year revealed that 33 per cent of mobile-device owners have used their devices to track some aspect of their health in the past 12 months. Consumer electronics companies (Nintendo, Apple...) are now active in the wellness space. They are strong in term of branding and driving consumer loyalty and can create new markets for health devices. They may struggle with distributing through healthcare professionals lacking relationships and have little experience working with regulators.

To reduce market fragmentation and improve interoperability in establishing a system of interoperable personal connected health solutions, the Continua Health Alliance<sup>83</sup> is an industry coalition that includes more than 200 companies that span technology, medical device, and health care delivery that are collaborating to establish a system for interoperable personal health solutions. The goal of the alliance is to develop design guidelines that enable the medical device supply chain to take advantage of interoperable sensors, home networks, telehealth platforms, and health and wellness services.

Integrating the Healthcare Enterprise (IHE) is another initiative by healthcare professionals and industry to improve the way computer systems in healthcare share information. IHE promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care. DICOM is an IT standard that is designed to ensure the interoperability of systems used to work with medical images and derived structured documents as well as to manage related workflow. Health Level-7 or HL7 refers to a set of international standards for transfer of clinical and administrative data between hospital information systems. it is a messaging standard that enables clinical and medical applications to exchange data.

In Europe, COCIR, a trade association, represents the medical imaging, health ICT and electromedical industries and promotes harmonization of regulatory frameworks, supported by state-of-the-art international standards.

---

<sup>79</sup> [http://www.csc.com/health\\_services](http://www.csc.com/health_services)

<sup>80</sup> <http://www-935.ibm.com/industries/healthcare/>

<sup>81</sup> <http://www.salesforce.com/company/news-press/press-releases/2014/06/140626.jsp>

<sup>82</sup> <http://www.thenational.ae/business/industry-insights/technology/digital-health-care-set-to-star-at-consumer-electronics-show-in-las-vegas>

<sup>83</sup> <http://www.continuaalliance.org/>

### **9.3.4 Market and EURO-MILS Adherence**

#### **9.3.4.1 Virtualization value**

Devices that use medical imaging are today prevalent in healthcare delivery. Ultrasound, digital radiography, MRI and CT images are helping practitioners make diagnostics. Embedded multi-core parallel processing and virtualization, as provided by the EURO-MILS platform, are key features for building devices that provide speed, resolution, reconstruction capability and high bandwidth to images and real-time diagnostics. Multiple processing cores allow for the use of complex algorithms that may address higher resolution and performance quality. Virtualization allow multiple applications run simultaneously — a user interface runs on one core, while another can be completely dedicated to performing the complex reconstruction computations.

The EURO-MILS platform can also provide the building blocks to support mHealth. When patient care moves from a hospital to a doctor's office or to a home monitoring environment, it requires creating an infrastructure that takes monitored data (e.g. glucose level monitoring, ECG, blood pressure), gathers it and delivers it in real time for analysis or saved in patient's electronic medical records.

#### **9.3.4.2 Security value**

The Healthcare industry is now witnessing a gradual emergence of cyber security related risks to patient safety and privacy. These risks have consequently caused healthcare providers, from device manufacturers to hospitals, to dedicate substantial resources for the purpose of discovering and mitigating cyber security risks. And the EURO-MILS platform can be a key element in the overall security architecture.

#### **A Regulated Platform**

Medical devices are often deployed in critical settings to administer treatment, causing changes to the patient's body, potentially as a result of external directives.

The EURO-MILS platform is answering the requirements of safety of medical devices. European and national administrations regulate medical devices to provide reasonable assurance of their safety and effectiveness. Privacy and security issues are still majors barriers to large adoption of mHealth from practitioners and patients. As devices support connectivity, they need to provide security and privacy as called for by regulations. In fact, how well devices can meet the security requirements at the target price points will be a pacing factor for the adoption of these devices by the market.

#### **Where Security Is Key**

For medical devices, the immediate problem presented by these technologies is the threat to privacy and the protection of personal information. However, the security risk presented, be it through malfunction or deliberate attack is less widely recognized. Security attacks on medical devices have so far been relatively rare, but as they become common, incentives increase to attack them for profit. But increased attention is given to security vulnerabilities in standalone medical devices. Regulation of security measures (i.e. using certification) must kept pace with the rapid development of this field. With the introduction of interoperability, medical devices are increasingly more connected to and dependent on each other. They will likely offer more attack avenues. A hacker needs only to take over the weakest device in the environment to gain a full control and then reach other devices through the existing trust relationships in the environment. With its embedded security design, the EURO-MILS platform can be an excellent foundation to build the secure environment.

## **That Is Connected But Private**

Patient data are increasingly collected from devices and applications, exchanged with practitioners, and stored in EMR. They are an invaluable source for medical analysis. Patients want health professionals to incorporate data from health devices into diagnosis and treatment decisions. They recognize that monitoring data, when combined with a range of other inputs, enables health professionals to see a more complete picture that can be used for better diagnosis and threats diseases. However, privacy cannot be breached, a survey from IBM<sup>84</sup> reveals that privacy and security are top expectations, but consumers are also keenly interested in sharing their health data. Patients and practitioners will prefer the more “traditional” options if there are no security standards that guarantee safe interoperability, data safeguarding, and protection from intrusion. By allowing multiple partitions (e.g. one partition for the imaging application, one partition managing the data encryption for communication), the EURO-MILS platform can participate in the secure transmission of data between embedded devices and HIS.

### **9.3.4.1 Certification Value**

The medical space requires strict revision controls and longevity of the product. Consistency of medical device is vital, since it must be qualified by regulatory agencies and pass certifications. In Europe, market approval for medical devices is achieved via a decentralised procedure of CE marking, whereby quality and safety is addressed, and registration of the product. Certification by placing the CE-mark is a requirement for selling most medical products and equipment in the EU.

In this context, the security certification of the EURO-MILS Platform is an asset as it proves that device makers have incorporated security features into their products to limit access to only trusted users, determined trusted content, and used fail-safe and recovery devices.

## **9.4 Mobile**

### **9.4.1 Market description**

The mobile phone market consists of all analog and digital handsets used for mobile telephony. Historically, a mobile phone is a phone that can make and receive telephone calls over a radio link while moving around a wide geographic area. Today, a smartphone is a mobile electronic device that runs an advanced operating system, is open to installing new applications, is always connected to the Internet, and provides diverse functionality to the consumer. In addition to telephony, smartphones support other services such as text messaging, MMS, email, Internet access, short-range wireless communications, business applications, gaming, and photography.

From a consumer perspective, the smartphone is becoming the digital extension of its owner. Over the past decade, smartphones have radically changed many aspects of people everyday lives, from banking to shopping to entertainment. The device is used as a personal wallet, a health monitoring system. It operates the house and the car. It manages all personal data from airline transportation ticket to medical data. However, all of this raises serious issues about hacking and personal privacy that haven't yet been fully addressed.

In our study, we focus on smartphone as it is becoming the standard device. According to Gartner, in the third quarter of 2014, smartphones accounted for 66 percent of the total

---

<sup>84</sup> <http://public.dhe.ibm.com/common/ssi/ecm/en/gbe03398usen/GBE03398USEN.PDF>

mobile phone market, and Gartner estimates that by 2018, nine out of 10 phones will be smartphones.

The smartphone market is rapidly changing, with constant product introductions. It is characterized by quickly evolving technology and designs, short product life cycles, aggressive pricing, rapid imitation of product and technological advancements, and highly price sensitive consumers.

### 9.4.2 Market Size and projections

As with many electronics industries, the smartphone industry is rapidly changing and highly competitive. New and distinctive products are being developed continuously, and released almost weekly. For this reason, the landscape of the market can change dramatically from one year to the next, or even from one month to the next. It is also a relatively young industry and some of the major players today (for example, Xiamin now world's third largest smartphone maker) hardly existed ten years ago where some former leaders (Blackberry) have become niche players today.

According to data from the International Data Corporation, the worldwide smartphone market grew 28.2% year over year in the fourth quarter of 2014, with shipments of 377.5 million units. For the full year, the worldwide smartphone market shipped a total of 1.3 billion units. This is a 27.7% growth from the 1.0 billion units of shipments in 2013.

Shipment (M units)	2014	2014 Market Share	2018	2018 Market Share	2014-2018 CAGR
Android	1 060	82,3%	1 498	80,0%	9,0%
iOS	178	13,8%	240	12,8%	7,8%
Windows Phone	35	2,7%	105	5,6%	31,4%
Other OS	14	1,1%	30	1,6%	20,4%
Total	1 288	100,0%	1 873	100,0%	9,8%

Table 6: Worldwide Smartphone Forecast by Shipments, 2014 and 2018 – Source IDC

Value (US\$M)	2014	2014 Market Share	2018	2018 Market Share	2014-2018 CAGR
Android	255 102	66,6%	275 248	60,9%	1,9%
iOS	116 540	30,4%	152 626	33,8%	7,0%
Windows Phone	7 782	2,0%	19 033	4,2%	25,1%

Other OS	3 480	0,9%	4 862	1,1%	8,7%
Total	382 904	100,0%	451 769	100,0%	4,2%

Table 7: Worldwide Smartphone Forecast by Value, 2014 and 2018 – Source IDC

The European smartphone market was worth \$62.4 billion (59.0 billion €) in 2014, up 1.7 percent year on year. Growth in smartphone shipments to Europe came despite the market's already high adoption of smartphones, which analyst reports attributed mostly to the recent release of Apple's iPhone 6.

### 9.4.3 Market Players

The smartphone market is among the largest and fastest growing markets in the world of consumer electronics. It is currently dominated from a hardware device perspective by Samsung Galaxy and Apple iPhone brands. However global brands are facing competition from smaller manufacturers targeting this lucrative smartphone market. Across Europe there is an accelerating trend of fragmentation in the handset market as smaller brands gain real traction. Established brands like Motorola and Sony are showing resurgence and newcomers to the European market such as Huawei and Wiko are challenging the established names.

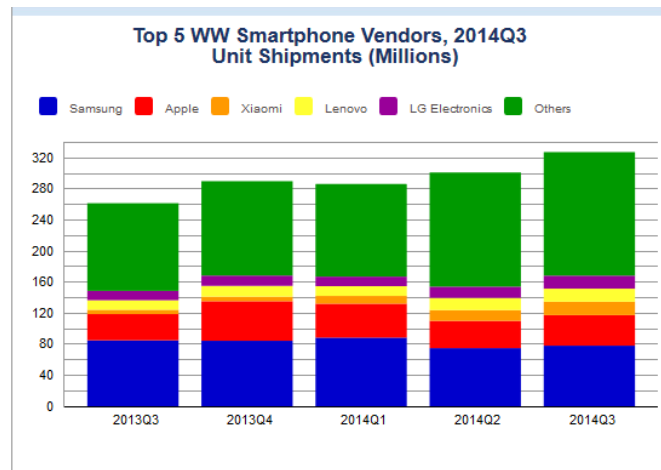


Figure 30: Top Five Smartphone Vendors, Q3 2014 – Source IDC

From an operating system perspective, Android smartphones lead the race followed by Apple iOS. Windows and BlackBerry are at a distant 3rd and 4th position.

Operating System	2014 Units	2014 Market Share	2013 Units	2013 Market Share
Android	1 004 675	80,7%	761 288	78,5%
iOS	191 426	15,4%	150 786	15,5%
Windows Phone	35 133	2,8%	30 714	3,2%
Blackberry	7 911	0,6%	18 606	1,9%
Other OS	5 745	0,5%	8 327	0,9%
Total	1 244 890	100.0%	969 721	100.0%

Table 8: Worldwide Smartphone Sales by OS - Source Gartner Mars 2015

European device makers such as Nokia, Ericsson or Siemens have been ceding the mobile handset market to global brands such as Samsung and Apple. But new Europeans players are getting back in the game. Startups such as France's Wiko and Spain's BQ are gaining share with smartphones that cost less than half as much as the flagship offerings. The new entrants, also including Kazam in Britain and Archos in France, are aiming to emulate the success of China's Xiaomi Corp., which has become the leader of its home market in just five years. Wiko boosted its share of the French market five-fold in 2014. BQ tripled its portion of the Spanish market.

### Ultra-secure Smartphone

Ultra-secure smartphones is becoming an interesting niche market for device makers. As claimed by one vendor, there is only one level of higher security, and that is not using a mobile phone at all.

In France, two companies are working on Android devices that should be more secure to spying attacks than the average mobile offerings found in carrier stores. The electronic systems company Thales SA is releasing an enterprise software system called Teopad that works on existing consumer Android smartphones and tablets, and virtually separate them in two: one side for personal use, and the other encrypted for sensitive business applications. The software is based on technology from the company's military-grade phone called Teorem, already used by 14,000 top civilian leaders in the country and French armed forces. The TEOPAD security solution from Thales has received CSPN<sup>85</sup> certification from ANSSI.

The Bull division of the French IT services group Atos takes another approach with the ruggedized smartphone Hoox m2. According to the vendor, the smart phone is fully secure and ensures high-level security using biometric fingerprint and code-based authentication, as well as encryption of all voice calls, texts, emails and data stored and exchanged. Hoox m2 is based on an Android kernel where all non-necessary elements have been removed. In January 2015, Bull has announced that its Hoox m2 secure smartphone has been

<sup>85</sup> The Certification Sécritaire de Premier Niveau (CSPN - First Level Security Certification) is a French lightweight security certification, alternative to Common Criteria certification.

approved<sup>86</sup> for use with data classified as 'Restricted Information' (' Diffusion Restreinte') by the ANSSI.

Based on Samsung Galaxy S3, Deutsche Telekom's SiMKo 3 security smartphone has successfully withstood testing by the German Federal Office for Information Security (BSI). Especially build for employees of ministries and federal authorities, the mobile device incorporates a L4 high-security microkernel as its operating system for transmitting classified information. The SiMKo 3 devices have two distinct compartments: a private compartment and a secure work compartment. The work compartment is a completely separate phone running a hardened version of Android in a virtualized environment based on an in-house developed bare metal hypervisor. A crypto card is also used to encrypt communication and information stored on the device.

Another German company, GSMK Cryptophone, builds secure cellphones. Running a modified version of Android, they allow for completely secure, end-to-end communication with most, if not all, of the smartphone features the security-conscious crave. However, both parties in the conversation need have to have their own Cryptophones.

In January 2014, the secure-communications provider, Silent Circle, headquartered in Switzerland and the Spanish smartphone manufacturer Geeksphone announced work on a mobile device—the Blackphone—that facilitates secure messages and calls. Though running on Android, the latest version of the smartphone, Blackphone 2, is equipped with Silent Circle's PrivateOS, an enterprise-orientated, highly secure layer that sits on top of Google's OS. This gives users a "Spaces" UI, which keeps the different areas of the user's mobile life encrypted and compartmentalized.

The Finnish company Elektrobit presents the EB Tough Mobile smartphone, designed and built for demanding mobile security and public safety markets. The Android-based smartphone incorporates a hardware-based security platform, with hi-security features such as tamper-detection and firmware and hardware integrity check. This dedicated hardware is essential for building layered mobile security solutions. The mobile hardware platform enables also integration of customer's own and third party software security solutions. It incorporates a special security platform with features like tamper-detection as well as integrity check to ensure end-user security and privacy.

The Defense, Space & Security Division of the US aerospace company Boeing is collaborating with BlackBerry to provide a secure mobile solution geared toward users in the defense and security communities. The smartphone, named Black, has embedded hardware security features, can be configured through software policies, has modularity capabilities, and features two slots for SIM cards. The phone can self-destruct if it is tampered with.

Sikur, a tech Brazilian start-up, announced at the 2015 Mobile World Congress in Barcelona, the GranitePhone. The phone runs a forked version of Android that provides users with encrypted messaging services, encrypted phone calls. It is totally locked down and cannot be altered. It communicates securely with any other Android device or iOS device that is running Sikur's software

#### **9.4.4 Market and EURO-MILS Adherence**

Increasing numbers of users spend most of their digital lives on smartphones and tablet mobile platforms. That is why the mobile platform becomes more and more attractive to cybercriminals. The immense volume of traffic together with the growing adoption of platforms such as Android has opened up new security threats. The complexity and volume

---

<sup>86</sup> It should be noticed that theses approvals from ANSSI for Hoox and from BSI for SiMKO 3 are not formal certifications for the Common Criteria.

of threats to the detriment of consumers continue to increase. Mobile malware, SMS spam, cyber-attacks and unlawful eavesdropping are an ever-increasing problem for enterprises, consumers and mobile network operators around the globe.

The security firm McAfee<sup>87</sup> predicts that mobile attacks will continue to grow rapidly as new mobile technologies expand the attack surface. The growing availability of malware-generation kits and malware source code for mobile devices will lower the barrier to entry for cybercriminals targeting these devices. Untrusted app stores will continue to be a major source of mobile malware. Traffic to these stores will be driven by “malvertising,” which has grown quickly on mobile platforms.

One major theme at 2015 Mobile World Congress was security. In the aftermath of the Snowden leaks and countless hacks on major corporations, the world at large is more concerned with privacy and personal security than ever before.

Therefore, there is an increasing need for securing the smartphone and the EURO-MILS technology can provide value to that matter.

#### 9.4.4.1 Security Value

The value of mobile security is important for users as well as mobile apps developers.

Mobile devices have become essential tools for home to enterprises users and digital trust is an imperative for them. Therefore, mobile security has become increasingly important, particularly when it relates to the security of personal and business information. Communication device as well planning and organizer tool, mobile phones have become a source of new risks as they collect and store sensitive information and also connect in real time to enterprise information systems.

As the traditional mobile application development processes stress on convenience more than security, this makes mobile applications a good target for hackers. Mobile app developers must ensure that their applications follow the secure programming practices and vulnerability responses that provide the right level of protection required. They must create, test and deploy their apps using best practices<sup>88</sup> such as use secure data transmission and storage mechanisms, implement proper session management, validate all trusted and untrusted inputs and implement strong authentication mechanisms.

To offer maximum security in their apps, developers can rely on a secure platform such as EURO-MILS that implement in its architecture security principles that cannot be breached. Because of its ability to run in parallel trusted and untrusted processes, the platform ensures that all critical services (communication, storage, authentication...) can be run in a secure mode.

#### 9.4.4.2 Certification Value

There is a market for security certified communication products for the government and local administrations as well as very sensitive businesses such as defence or homeland security. Reinforced by the recent revelation of global surveillance programs, there is also a nascent market for a privacy certified products for the consumers, although not yet mature. Finally, smartphone certification may also become more important as diffusion of mobile payment

---

<sup>87</sup> [McAfee Labs Report Previews 2015 Developments in Exploits and Evasion](#)

<sup>88</sup> Jointly with the OWASP mobile security project, the European Security agency ENISA has produced a document for developers of smartphone apps as a guide to developing secure apps. It may however also be of interest to project managers of smartphone development projects. ([Smartphone Secure Development Guidelines](#))



method by smart phone causes new changes of the means of payment which has been changed cash to plastic card. Security requirements in mobile payment methods may impose certification.

We can also illustrate the value of certification by citing mobile hardware and software that have been evaluated and granted security labels and certificates.

FIPS 140-2 security standard is used to accredit the cryptographic algorithms that protect sensitive data inside products like smartphones. Microsoft Windows Phone 8 has received the accreditation. Cellcrypt, the UK provider of voice call encryption has also been granted FIPS 140-2 certification to its cryptographic module Ccore, a technology used in a range of Cellcrypt products including mobile phone and gateway applications. In the US, the National Institute of Standards and Technology (NIST), which examines and tests mobile devices for security and validation purposes, granted the Apple mobile platform FIPS 140-2 certification (Level 1).

Common Criteria also enter the mobile world. In November 2014, the National Information Assurance Partnership (NIAP) validation team has published a Common Criteria report<sup>89</sup> of the evaluation of LG G3 Smartphone solution provided by LG Electronics Inc. It presents the evaluation results, their justifications, and the conformance results. The evaluation determined that the product is both Common Criteria Part 2 Extended and Part 3 Conformant, and meets the assurance requirements of EAL 1.

More generally, from the common criteria viewpoint, major obstacles for evaluation are the lack of platform assurance and obligation of user guidance. Smartphone platforms offer basic means of isolation. The smartphone user can review a set of permissible operations before application installation, e.g. as much as 74 permission types in Android.

Finally, the US Government's Common Criteria Evaluation and Validation Scheme has made available new Protection Profiles<sup>90</sup> targeted to mobiles. The Mobile Device Protection Profile (MDPP) contains the security functional requirements for mobile devices such as smartphones and tablets. The Mobile Device Management Protection Profile (MDMPP) includes the security functions to be evaluated including key protection, protected communications, mobile device configuration, and administration.

#### 9.4.4.3 Virtualization Value

Most conventional smartphones have a market life of just six to eight months before being replaced by a successor. This leaves little time to develop and test suitable security mechanisms, leaving them with inadequate protection.

EURO-MILS virtualization software enables two completely different profiles on a single device:

- A personal profile with access to the public cloud for social networks, navigation, telephony and much more.
- A professional profile with secure on-the-road access to all business resources

The personal partition can accept the latest innovative or trendy app and follow the market innovation cycle. On the other hand, the professional partition may only support enterprise validated apps and completely enforce security of the enterprise environment.

From a security perspective, mobile virtualization may be more adequate than the most common mobile security approach, containerization. Mobile containers are used to encrypt and separate sensitive apps in one area of a device, but the apps still have to communicate

---

<sup>89</sup> [https://www.commoncriteriaportal.org/files/epfiles/st\\_vid10593-vr.pdf](https://www.commoncriteriaportal.org/files/epfiles/st_vid10593-vr.pdf)

<sup>90</sup> <https://www.niap-ccevs.org/pp/>

with the device's hardware (e.g., the screen or keyboard) to function in the same namespace as other, unprotected apps.

The virtualization software forms a layer between the hardware and the smartphone's open and secure application systems. Separating the hardware from the software allows users to access consumers' applications such as Facebook or Twitter, while protecting sensitive enterprise applications. These are safely hosted at a secure data center and provisioned via a VPN tunnel using an integrated smart card. Segregating hardware and software ensures rock-solid security despite the hectic smartphone innovation cycle. With mobile virtualization, IT departments can simply install mobile device management solutions on corporate OS instances, and allow employees to retain full freedom over the rest of their phones. IT can lock-and-wipe a corporate OS instance without having any effect on the rest of the device. It becomes easy to encrypt corporate data and enforce effective security policies without compromising personal choice and privacy.

## 9.5 Industrial Control Systems

### 9.5.1 Market description

An Industrial Control System<sup>91</sup> (ICS) is an information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes

ICS are typically used in industries such as electric, water and wastewater, oil and natural gas, transportation, chemical, pharmaceutical, pulp and paper, food and beverage, and discrete manufacturing (e.g., automotive, aerospace, and durable goods.). Based on data received from remote stations, automated or operator-driven supervisory commands can be pushed to remote station control devices. The devices control local operations such as opening and closing valves and breakers, collecting data from sensor systems, and monitoring the local environment for alarm conditions.

SCADA systems are highly distributed systems used to control geographically dispersed assets, often scattered over thousands of square kilometres, where centralized data acquisition and control are critical to system operation. They are used in distribution systems such as water distribution and waste water collection systems, oil and natural gas pipelines, electrical power grids, and railway transportation systems.

DCS are used to control industrial processes such as electric power generation, oil refineries, water and wastewater treatment, and chemical, food, and automotive production. DCS are integrated as a control architecture containing a supervisory level of control overseeing multiple, integrated sub-systems that are responsible for controlling the details of a localized process.

PLCs are industrial computer control systems that continuously monitor the state of input devices and makes decisions based upon a custom program to control the state of output devices. While PLCs are control system components used throughout SCADA and DCS systems, they are often the primary components in smaller control system configurations used to provide operational control of discrete processes such as automobile assembly lines and power plant soot blower controls. PLCs are used extensively in almost all industrial processes.

---

<sup>91</sup> Source: [NIST Special Publication 800-53](#), Rev 4, Glossary.

### Distinction between IT and Control Systems<sup>92</sup>

There is an important distinction between mainstream IT and ICS. IT uses “physics to manipulate data” while an ICS uses “data to manipulate physics.” The potential consequences from compromising an ICS can be devastating to public health and safety, national security, and the economy.

Information Technology	Industrial Control
<b>Performance</b>	
<b>Non-Realtime</b>	Realtime
<b>Response must be reliable</b>	Response is time critical
<b>High throughput demanded</b>	Modest throughput acceptable
<b>High delay and jitter accepted</b>	High delay and/or jitter is a serious concern
<b>Reliability</b>	
<b>Scheduled operation</b>	Continuous operation
<b>Occasional failures tolerated</b>	Outages intolerable
<b>Beta testing in the field acceptable</b>	Thorough testing expected
<b>Risk Management</b>	
<b>Data integrity paramount</b>	Human safety paramount
<b>Risk impact is loss of data, loss of business operations</b>	Risk Impact is loss of life, equipment or product
<b>Recover by reboot</b>	Fault tolerance is essential
<b>Security Architecture</b>	
<b>The central server is the critical device for protection (not the edge client)</b>	The edge device, such as the PLC or smart drive controller, is considered more important than a central host such as a data historian server

Table 9: Distinctions between IT and Control Systems

The design and operation of ICS and IT systems are different. IT professionals design their system with extensive security checks and controls. In part because of limited computing resources ICS designers try to build systems that allow reliable, safe, and flexible performance, but paradoxically, increase cyber-vulnerability. This results in trade-off conflicts between performance/safety and security. These differences in fundamental approaches

<sup>92</sup> Source “Assuring Industrial Control System (ICS) Cyber Security Joe Weiss PE, CISM Applied Control Solutions, LLC” ([http://csis.org/files/media/csis/pubs/080825\\_cyber.pdf](http://csis.org/files/media/csis/pubs/080825_cyber.pdf))

lead to conflicting technical, cultural, and operational differences between ICS and IT that need to be addressed.

Initially, ICS were isolated systems running proprietary control protocols using specialized hardware and software. As ICS are adopting IT solutions to promote corporate business systems connectivity and remote access capabilities, and are being designed and implemented using industry standard computers, operating systems (OS) and network protocols, they are significantly less isolated from the outside world than predecessor systems, creating a greater need to secure these systems.

### **9.5.2 Market Size and projections**

SCADA systems are widely used to monitor and control industrial processes and infrastructure in manufacturing plants. The market is expected to witness significant growth over the next years as there is huge potential from renewable energy sector, high investments in infrastructure for sectors such as oil and gas, power (transmission and distribution), and water and wastewater management. Cyber security threat is considered as an important restraint. The market research and consulting company MarketsandMarkets<sup>93</sup> projects that the total revenue of the SCADA market is expected to reach up to \$11.16 billion by 2020, at an estimated CAGR of 7.24 % from 2014 to 2020.

According to another market research company<sup>94</sup>, revenue from transmission and distribution SCADA devices will grow from \$913 million in 2012 to more than \$1.5 billion in 2020. Utilities have a growing interest in smart grid investments that reach beyond meter reading and extend to automation technologies that actively monitor transmission and distribution grids and take autonomous action to improve reliability and efficiency. Such devices, which operate at substations and individual distribution feeders, are key elements of this shift.

The global DCS market will reach US\$19.8 billion, growing at a 3.9% CAGR from 2012 through 2018, according to Transparency Market Research<sup>95</sup>. The report observes that a vast majority of distributed control systems were set-up in the 1980s in industrialized nations such as Europe and North America. Most of these systems are now older than two or three decades and are reaching the fag end of their recommended lifecycle, creating a whole new market for replacement and upgrades.

Finally, the PLC market<sup>96</sup> earned revenues of \$10.37 billion in 2013 and estimates this to reach \$14.58 billion in 2018. The largest market for PLC hardware and directly associated software and services remains Europe, Middle East and Africa, whose size was estimated at \$4.2 billion in 2011. From 2010 to 2016, EMEA's PLC market is forecast to grow at a CAGR of 7.8%. In Europe, the need to enhance efficiency, comply with regulations as well as improve safety and control capabilities are driving the uptake of PLC.

---

<sup>93</sup> Source: [SCADA Market by Components \(PLC, RTU, HMI, Communication Systems\), Architecture \(Hardware, Software, Services\), Application \(Oil & Gas, Power, Water & Wastewater, Transport, Manufacturing, Chemicals\), and Geography - Analysis & Forecast to 2013 - 2020](#) - MarketsandMarkets – May 2014

<sup>94</sup> Source: Report “[Smart Grid SCADA Systems](#)” - Pike Research – February 2013

<sup>95</sup> Source : Report “[Distributed Control Systems Market - Global Industry Analysis, Size, Share, Trends And Forecast 2012 – 2018](#)” - Transparency Market Research – January 2015

<sup>96</sup> Source: Report “[Global Programmable Logic Controllers Market](#)” – Frost & Sullivan – January 2015

### **9.5.3 Market Players**

Key players in the ICS market are Siemens AG, Rockwell Automation, Emerson Electric Co., GE Intelligent Platforms, ABB Ltd., Schneider Electric, and Alstom. Such established companies have the dominating share in the ICS market worldwide. Although smaller players are providing increasing competition to the big established players, the dominating share in the market will still be held by the latter. These players operating in the market generally provide the entire package of ICS solutions to their clients, including the provision of hardware, software and services.

The market is characterized by mergers and acquisitions in order to gain competitive advantage. For instance, ABB acquired Power One Global in April 2013. In 2014, Schneider Electric acquired Invensys to reinforce its industrial automation capabilities, confirm its positions in key energy-intensive segments and strengthen its software offering.

### **9.5.4 Market and EURO-MILS Adherence**

ICS systems were designed around reliability and safety, not security. Now these systems are becoming increasingly interconnected with IP networks and have become vulnerable to Internet threats. ICS security market is expected to experience significant growth over the coming years due to the growing demand for process automation and remote control. It has thus forced the companies to expand their existing infrastructure and also to deal with a variety of security challenges such as cyber-attacks, insider criminal activities and global competition.

#### **ICS and Critical Infrastructure**

There has been a significant rise in attacks on critical infrastructures all over the globe. These cyber-attacks on the facility networks enable the hackers to control the processes and compromise the integrity of critical information. To safeguard the processes and the critical infrastructures, almost every country and the related companies are turning towards robust security solutions.

The ICS-CERT<sup>97</sup> reports that they responded to 245 attacks against U.S. based ICS between October 2013 to September 2014, with nearly one-third of the incidents focused on systems governing energy production and distribution.

---

<sup>97</sup> Source: [Incident Response/Vulnerability Coordination in 2014](#) - Industrial Control Systems Cyber Emergency Response Team - US Department of Homeland Security – February 2015

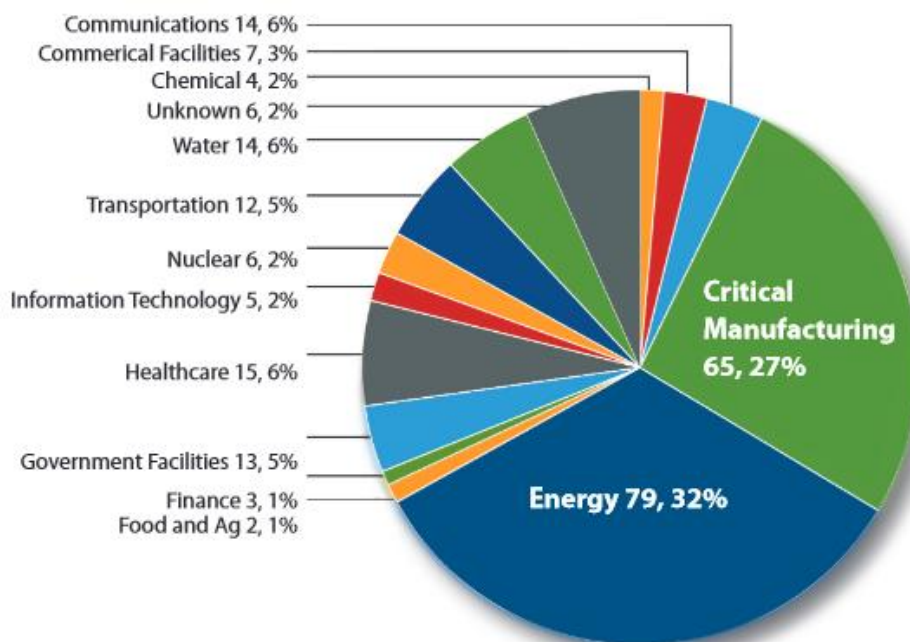


Figure 31: FY 2014 incidents reported by sector (245 total) - Source: ICS-CERT

Security of critical infrastructure is also important for the European and national authorities. Recent deliberate disruptions of critical automation systems prove that cyber-attacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social wellbeing. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level. Since 2011, the European security agency ENISA has launched new activities in the three areas: Industrial Control Systems/SCADA, Smart Grids and Smart Metering, and Dependencies of Maritime Transport to ICTs.

The recommendations call for the creation of the national and pan-European ICS security strategies, the development of a Good Practices Guide on the ICS security, fostering awareness and education as well as research activities or the establishment of a common test bed and ICS-computer emergency response capabilities. The agency has also proposed a series of recommendations<sup>98</sup> towards the development of certification schemes for ICS cyber security professionals.

#### 9.5.4.1 Security Value

According to security experts, the main problem related to ICS is that they were not designed to be connected to the Internet and therefore the principal issues related to security aspects were not considered during their development phase. Providing robust security for ICS has long been a goal and frequently a mandated requirement in a variety of industrial market segments. Evolving security standards, a limited understanding of security architecture fundamentals and missing technologies to reasonably secure legacy applications has challenged the industry for well over a decade. But recent advances in multicore processor technology, hypervisor partitioning, and embracement of the IEC 62443 security standard now provide a viable and certifiable approach for ICS systems. It has also become paramount that critical infrastructures balance the needs of ICS reliability and safety with cyber security. In this context, the EURO-MILS platform, providing natively security features by design, has strong arguments to provide in the ICS security discussion.

<sup>98</sup> Source : [Certification of Cyber Security skills of ICS/SCADA professionals](#) - Enisa – February 2015

### 9.5.4.2 Certification Value

As security is now an important concern for ICS professionals and national authorities, security certification will appear quickly on their radar. First, certification is not new in many industrial domains. In areas such as avionics, transportation, similar certification requirements exist for products and plants concerning functional safety (IEC61508, IEC61511). They cannot put on the market products that do not receive the required certificates. Modern societies depend completely on utilities such as oil, water, and electricity, and these systems have become vulnerable to online attacks. Therefore, the cyber security and resilience of ICS is of utmost importance to society as a whole, to utilities and other critical infrastructure operators, and to organizations that use ICS.

Security certification may be soon a prerequisite to ensure a better security as it is today with safety certification. The European security agency Enisa has given the recommendation<sup>99</sup> to use the security framework model of Common Criteria to protect ICS : *“a security framework model adapted for ICS could be defined, based on existing efforts such as Common Criteria or FIPS. Member State existing certifying organisms would be responsible for the certification process based on this security framework.”*

However, ICS security is hard. It requires a large investment in terms of money, resources, and time. For example the cost of having a commercial software product undergo a Common Criteria evaluation can be very important. Using a certified composite platform such as EURO-MILS can lower the cost of certification. The isolated partitions of EURO-MILS allow manufacturers to use COTS for non-sensitive functions and combine them with highly protected partitions that require high level of security. Of course, manufacturers need carefully analyze what is the added value of the product that received the certification. A certified product has to be time-consumingly recertified after each update. That implies that certified products are always several generations behind the most up-to-date system version but ICS systems certified today will be around for a long time. EURO-MILS, with its multiple independent partitions allows updating parts of the system without impacting from a security perspective the other components.

### 9.5.4.3 Virtualization Value

The virtualization capability of the EURO-MILS platform is also a great value for the ICS domain. Virtualization in the ICS area allows reducing hardware, infrastructure and facilitation costs.

But there are also other significant reasons for virtualizing the ICS environment. Virtualization enables better integration of ICS components into the existing virtualized IT environment. As the line between ICS and IT is blurring, it is important that the two departments collaborate on solutions compliant with both process control and IT needs with for instance the integration of cyber security. All industrial processes are constantly subject to change. On relatively stable hardware, changes are often required on application level. EURO-MILS virtualization can simplify the adaptation of the component into the updated process flow. Working in a real-time environment with high production demands and hazardous conditions makes seamless implementation a high priority. This is where virtualization becomes significantly useful, since the test environment can be run virtualized, reducing costs and being able to downsize the environment when the test phase is accomplished. There is an increasing demand for virtualization since this is commonly used at corporate level mainly applied on the less critical processes where communication loss for a short period of time is

---

<sup>99</sup> Source: [Protecting Industrial Control Systems. Recommendations for Europe and Member States](#) – Enisa – December 2011

allowed. However, virtualization offered by EURO-MILS technology is adaptable in the field of real-time automation that is a key requirement for industrial control systems.

## Part III: Social Acceptance

In the previous section, we analysed the business value of a reliable embedded platform from a business perspective. In this part, we continue the analysis from another perspective: the social acceptance of the developed technology. The reliable secure platform that EURO-MILS project has created is used by businesses such as aircraft manufacturers, automobile companies, medical systems manufacturers or consumer electronics vendors, to name a few, as a fundamental component of innovative solutions that are commercialized in different countries.

It means that the products have to be accepted and bought by the consumers as well as to conform to the legal requirements issued by authorities. The following chapters discuss the implications from the consumer viewpoint.

To understand the consumer's viewpoint that leads to social acceptance of the developed technology, we ran a survey across Europe to understand the value of security for consumers. They were asked questions about security and secure products to understand their appetite for technology advanced products and their perception of usefulness of secure products. To complete this survey, we performed a Big Data analysis where we listened consumers' comments on security and technology.



# Chapter 10 Social Survey: Questioning the Consumers

First step in our analysis, we questioned directly the European consumers about security and secure products.

In June and July 2014, EURO-MILS launched a survey towards European “end-users” of connected devices.

First objective is to explore the understanding of security in the consumer market. Information security incidents are reported almost daily in the news. But for ordinary individuals, and even SMEs and professional firms, although this made cyber risk intriguing, it also reinforced a feeling that information security and cyber issues are somehow remote from daily life: interesting but not really threatening.

In the context of EURO-MILS, we want to analyse the social value of secure products as well as understanding the user assurance

In summary, we created a survey to answer questions such as:

- Do consumers understand information security and its impact in their daily life?
- Do consumers evaluate the risks associated with the product/service?
- Do consumers value security in choosing/buying a product/service?
- What is the impact of consumer trust and perception of security on the acceptance of a product/service?
- Is security perceived as a key value of a product as important as its price or its design?
- Why would a consumer choose a secure product against a non-secure product?
- What are the key attributes of a secure product that will convince the consumer?
- What are the characteristics (label, certificate, authority...) that ensure customers the product they want to buy has the right level of security?

## 10.1 Social Survey Methodology

To run the survey, we choose to partner with Netmedia Europe, a B2B online publishing house targeting IT Decision Makers. As it has more than 12 million European unique users per months on their web sites and an email database with more than 800 000 contacts, it was the right partner to help us to contact a large European end user base. However, we took into account in our survey analysis that most of the respondents were technology savvy as our partner is targeting professionals in the IT industry.

We created a questionnaire that we translated in English, German, French, Italian, and Spanish. This self-administered questionnaire was then submitted to the readers of the online IT publication using a call to action sent by email.

We used SurveyMonkey, a cloud-based online survey development tool, to create and publish our survey using Netmedia Europe consumer database.

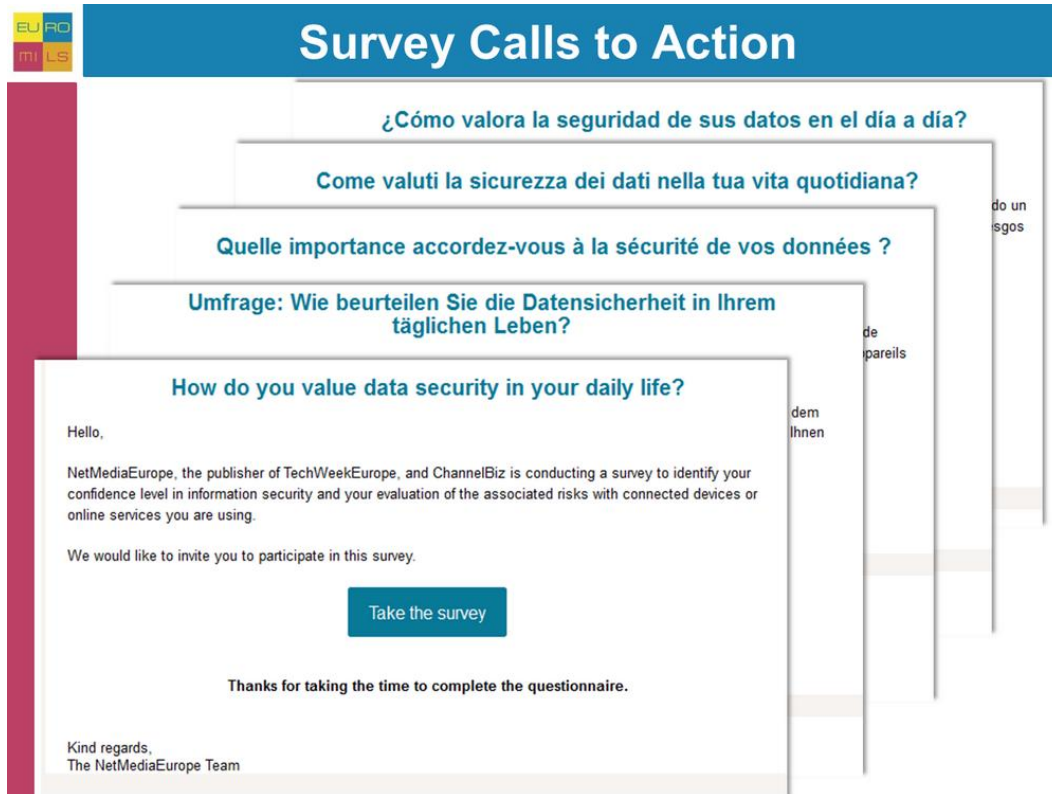


Figure 32: Social Survey Call To Action

Accepting the invitation to participate in the survey, the reader would read the objectives of the survey and start the on-line questionnaire in its own language.



Figure 33: Social Survey Introduction Page

## 10.2 Social Survey Questionnaire

This section presents the English version of the questionnaire used for the survey. This questionnaire has been translated in German, French, Italian, and Spanish. Each version has been used in the on-line survey tool.

### 10.2.1 English Version of the Social Survey Questionnaire

#### EURO-MILS Questionnaire:

Funded by the European Union, the EURO-MILS project develops solutions for designing, implementing and certifying secure embedded systems. Embedded systems are the most common form of computers in use today and are embedded in all kinds of electronic equipment and machines. They need to be reliable (Would you be confident to drive a car that presents a real risk to life in having a computer system that could be turned off remotely or make instruments give false reading?) and secure (Would you accept to rely on smart meter devices that could be hacked to provide fake energy consumption data?).

The objectives of this questionnaire are to analyse the social value of secure products and understand the user assurance (How do you value information security and its impact in your daily life? How you evaluate the associated risks with the product or service you are buying? ...)

Thank you for answering the short following questionnaire.

#### 1. Security awareness

For each of the following statements, would you say you strongly agree, somewhat agree, somewhat disagree, strongly disagree or do you have no opinion

1. My personal smartphone data is protected using all available means (password, encryption, backup, ...).
2. As everyday objects are becoming smarter and communicating, I am concerned about the protection of my personal data.
3. I am very careful about granting access to device information (location, phone number, SIM card serial number, apps used, phone state...) to applications installed on my smartphone.
4. Installed regulations to prevent misuse of consumers' personal data are not strict/strong enough.
5. I don't mind disclosing personal data in return for free online services (such as email service, photo sharing).
6. I am worried about the data security practices of companies whom I provide my personal / financial information.

#### 2. Your security practice

For each of the following statements, would you say you strongly agree, somewhat agree, somewhat disagree, strongly disagree or do you have no opinion

1. On my personal PC/tablet, I have set up periodical backups to avoid losing my music/photos/emails and tested their recoveries.
2. When I receive my bank account statement, I check carefully each line item to ensure that my bank made no mistakes.
3. I protect my personal data on my main used Internet web site accounts by changing passwords at least once a month and/or using a different password for each site.

4. I will change my provider (ISP, online banking...) if I don't get maximum availability (24x7) for the proposed service.
5. I always avoid online purchase on Internet sites not using encrypted connection for payment.
6. I never access my bank account using a public network because of lack of security.

### 3. Privacy

To what extent are you concerned about the following risks when sharing personal information online? (Very concerned somewhat concerned, somewhat not concerned, not at all concerned, don't know)

1. The data may be hacked and used to steal money from me.
2. By sharing data I may be targeted by marketing campaigns in the future.
3. The government or government agencies may obtain access to my personal data.
4. Current or future employers may gain access to personal data that I would not wish to share with them.

### 4. Trust in secure products and services

For each of the following statements, would you say you strongly agree, somewhat agree, somewhat disagree, strongly disagree or do you have no opinion

1. I avoid to buy products/services out of concerns for the security and privacy of my personal data.
2. My energy consumption statement is/will be more reliable when done via a smart meter than via a manual readout.
3. I have elected to use electronic bank statements.
4. A driverless car is frightening because I think I can react better to any type of incidents/dangers than a computer.
5. I am not afraid of using a transportation system operated without a driver (e.g. London Victoria line, Paris RATP Ligne 14, Nuremberg U-Bahn...).
6. I feel confident that my bank has put specific measures in place to prevent online banking fraud.

### 5. Security Value

Please select the three most important criteria of choice when buying a new technology product:

- innovative features
- Company image
- price
- personal recommendation
- durability and portability aspects
- performance
- media influence
- post-sales service
- security features

## 6. Security expectations

Here is a list of devices that may be connected to the Internet and are accessible remotely. Please indicate what your three main security expectations are:

	Information theft	Identity theft	Device malfunctioning	Device unavailability	Data loss	Financial loss	Safety risks	Others
Smartphone								
Television								
Connected Watch								
Connected Glasses								
Car								
Healthcare device								
Smart-meter								
Home Refrigerator								
Room Thermostat								
Surveillance video camera								
Bathroom scale								

## 7. Trust

How secure do you believe your personal / financial information is in the hands of the following organizations? Very secure, somewhat secure, somewhat unsecure, very unsecure, don't know

1. Social Networks
2. Online retailers
3. Banks/financial institution
4. Charities
5. Doctors' offices/hospitals
6. Family and friends
7. Employer
8. Government/government agencies

## 8. Security assurance and Certification

Information security becomes important in the Internet of Things. To ensure that the device you are buying has the best level of security, please indicate the three most important criteria you rely on

1. A security label given by national government authority.
2. The manufacturer of the product/service.
3. A declaration of conformity certifying that the device complies with EU directives.
4. A security evaluation performed by an independent commercial security company.
5. Feedbacks and personal recommendations given by other users.
6. Advices form the retailer.
7. Product reputation read in the press.

## 9. Security and Safety

For each of the following domains, which statement (advantage or drawback) is more important for you?

eHealth: The eHealth concept covers a range of services/products that are at the edge of healthcare and information technology, such as enabling the communication of patient data between different healthcare professionals.

1. Being able to share my health information with my doctor using my smartphone is a great improvement.
2. For fear of hacking, I am very concerned of using a new computerized medical device (pacemaker, insulin pumps...) that requires an Internet connection.

Smart Home: Smart homes are Internet connected. Electric meters, alarm clocks, home refrigerators thermostats, video cameras and other connected gadgets and appliances are accessible remotely.

1. I am afraid that these technologies open a window into my house to unauthorized people (hackers, cops...).
2. Using my smartphone to control everything (lighting, curtains, heating...) in my house remotely is great.

Automotive: Modern cars offer Internet connections to personal mobile devices everywhere just like home.

1. I am concerned about possible negative interference such as performance aspects when doing intensive download to the car driving applications.
2. I appreciate receiving automatically messages such as traffic alerts or car service notices.

Avionics: Airline companies are progressively allowing passengers to connect to Internet using their personal computers/smartphones/tablets during flights.

1. I am concerned about possible negative interference such as virus infection from my personal device to the plane control applications.
2. I appreciate being able to surf the Web or write emails during the flights.

Internet of Things: To allow personalization of their services, companies offering connected devices require personal and financial information from their customers.

1. Due to the growing complexity of managing personal information, I rather trust professional service providers to secure it rather than doing it on my own.
2. I am worried about the data security practices of companies whom I provide with my personal information.

10. Here is the last optional question for IT savvy people: Security by design

When you install a new application program from the Internet (such as a calendar application, a software phone, a photo processing software) on your personal device (PC, smartphone or tablet), pick one or several of the following affirmation that represent your behaviour:

- I trust the device that it is able to protect my personal data from malicious applications
- I chose applications based on their reputation (personal recommendation, applications recommended by operating system manufacturer or press etc.) to avoid malwares.
- I have installed a malware scanner as additional measure of protection
- I verify digital signatures as additional measure of protection
- I use virtualization as additional measure of protection
- I use other techniques as additional protection
- I don't care
- I have never installed application programs over the Internet that operate on my personal data

Thank you for your time!

Note: The EURO-MILS project has received funding from the European Union's Seventh Framework Programme ([FP7/2007-2013]) under grant agreement number ICT-318353

### 10.2.2 Sample of the On-line Version of the Social Survey Questionnaire

How do you value data security in your daily life?

0%  100%

**Page 1**

**\*To what extent do you agree or disagree with the following statements concerning your security awareness?**

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree	No opinion
My personal smartphone data is protected using all available means (password, encryption, backup ...)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
As everyday objects are becoming smarter and communicating, I am concerned about the protection of my personal data	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am very careful about granting access to device information (location, phone number, SIM card serial number, apps used, phone state...) to applications installed on my smartphone	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I am worried about the data security practices of companies whom I provide my personal / financial information	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

**\*Please indicate how much you agree or disagree with each of the following statements concerning your security practice?**

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree	No opinion
On my personal PC/tablet, I have set up periodical backups to avoid losing my music/photos/emails and tested their recoveries	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
When I receive my bank account statement, I check carefully each line item to ensure that my bank made no mistakes	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I protect my personal data on my main used Internet web site accounts by changing passwords at least once a month and/or using a different password for each site	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I will change my provider (ISP, online banking...) if I don't get maximum availability (24x7) for the proposed service	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I always avoid online purchase on Internet sites not using encrypted connection for payment	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
I never access my bank account using a public network because of lack of security	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Figure 34: On-line Questionnaire (Page 1-a)



**\*To what extent are you concerned about the following risks when sharing personal information online?**

By sharing data I may be targeted by marketing campaigns in the future

The government or government agencies may obtain access to my personal data

Current or future employers may gain access to personal data that I would not wish to share with them

**\*To what extent do you agree or disagree with the following statements?**

Strongly agree    Somewhat agree    Somewhat disagree    Strongly disagree    No opinion

I avoid buying products/services out of concerns for the security and privacy of my personal data

My energy consumption statement is/will be more reliable when done via a smart meter than via a manual readout

I have elected to use electronic bank statements

A driverless car is frightening because I think I can react better to any type of incidents/dangers than a computer

I am not afraid of using a transportation system operated without a driver (e.g. London Victoria line, Paris RATP Ligne 14, Nuremberg U-Bahn...)

I feel confident that my bank has put specific measures in place to prevent online banking fraud

**\* Please select the three most important criteria of choice when buying a new connected device:  
Check at most 3 answers**

Innovative features

Company image

Price

Personal recommendation

Durability and portability aspects

Performance

Media influence

Post-sales service

Security features

<< Previous    Next >>    Exit and clear survey

Figure 35: On-line Questionnaire (Page 1-b)

## 10.3 Social Survey Demography

In these sections, we explain the demography of the survey.

### Geographies

Geography	Nbr	%
Benelux	47	8,59%
France	99	18,10%
Germany	94	17,18%
Italy	97	17,73%
Spain	114	20,84%
UK	96	17,55%
Total	547	100,00%

We received 547 questionnaires from the six geographies:

Apart from Benelux which is a bit less represented, we have a uniform distribution of answers with around hundred respondents by main western European countries.

## Company Size

Company Size	Nbr	%
1	99	18,10%
2-9	95	17,37%
10-49	68	12,43%
50-99	35	6,40%
100-249	47	8,59%
250-499	44	8,04%
500-999	26	4,75%
1000-4999	42	7,68%
5000 or more	91	16,64%
Total	547	100,00%

We have a uniform set of companies from small and medium businesses to very large enterprises.

## Industry Sectors

Business Area	Nbr	%
Banking, Finance, Insurance, Brokerage	31	5,67%
Computer and Information technology (hardware, software, services)	178	32,54%
Consumer Electronics	4	0,73%
Education	29	5,30%
Healthcare / Medical	13	2,38%
Automotive	9	1,65%
Manufacturing/Industrial	51	9,32%
Public Sector / Government	55	10,05%
Retail/Wholesale	23	4,20%
Services for businesses or individuals	104	19,01%
Transport, Logistics	12	2,19%
Travel, Hospitality, Entertainment	9	1,65%
Utility	2	0,37%
Other	27	4,94%
Total	547	100,00%

All industries are represented with a preponderance of the IT sector (targeted by our media partner).

## Age of the respondents

Age	Nbr	%
Under 26 years old	16	2,93%
26-35	63	11,52%
36-45	123	22,49%
46-55	179	32,72%
Over 55 years old	166	30,35%
Total	547	100,00%

The ages of the respondents are representative of the European workforce with a maximum between 35 and 55.

## Role

Role	Nbr	%
President, Managing Director, Chairman, CEO	96	17,55%
CIO, CTO, IT Director, Head of Systems	64	11,70%
CISO, Security Officer, Head of Security	7	1,28%
COO, Head of production	10	1,83%
Database / Storage Manager	17	3,11%
Developer, analyst, programmer	52	9,51%
Engineer, Project manager	41	7,50%
Head of IT support / helpdesk	13	2,38%
Head of office automation systems or micro computing	13	2,38%
IT architect	8	1,46%
ICT consultant	92	16,82%
IT Technician, Support, Helpdesk	77	14,08%
Network / Telecommunications Manager	29	5,30%
R&D Manager	13	2,38%
Webmaster, Designer	7	1,28%
Other:	8	1,46%
Total	547	100,00%

Most of our respondents have an IT role in their company.

It is important to notice that, although we targeted IT Professionals in our survey, the questionnaire is asking questions around their personal life not their professional life.

## 10.4 Social Survey Analysis

In the following sections, we highlight the principal results of the survey.

### 10.4.1 Security Awareness

In the first set of questions, we want to understand the security awareness of our panel.

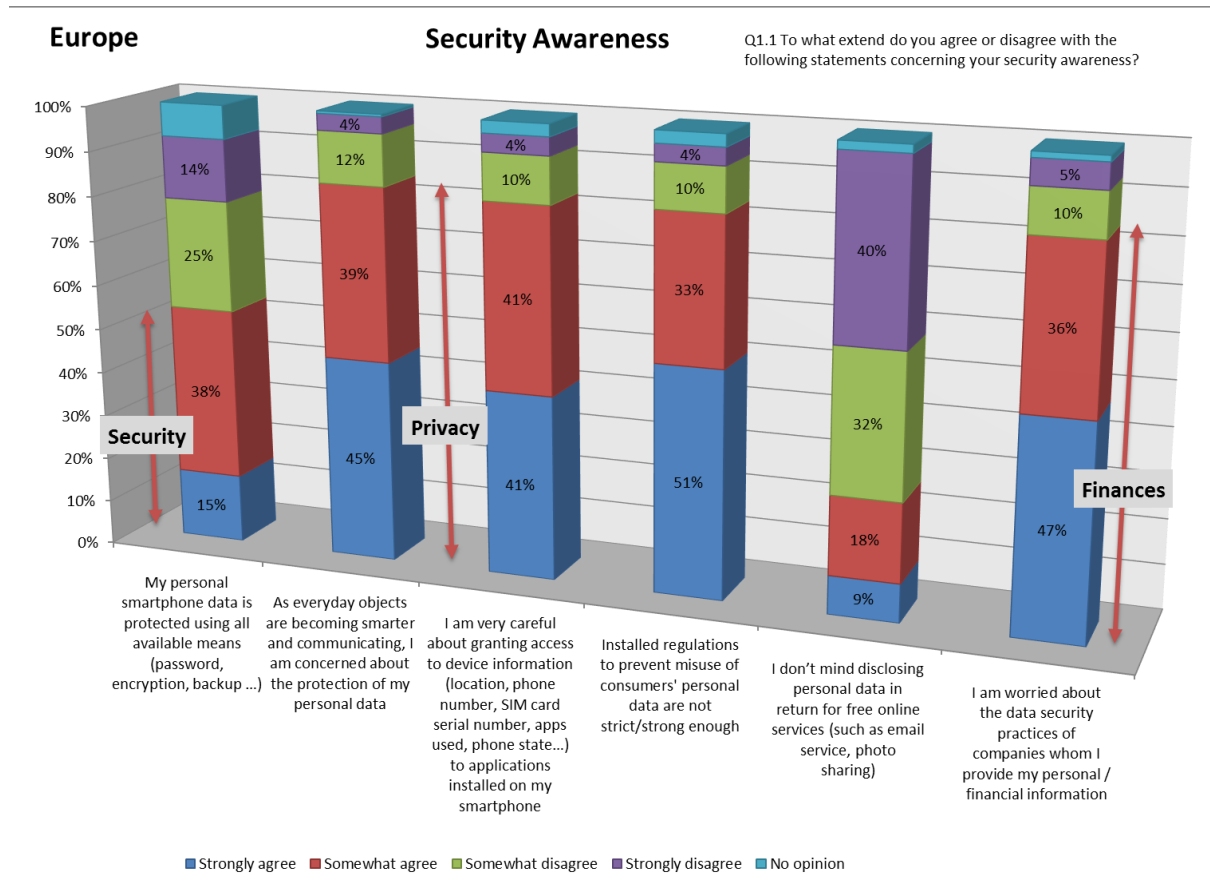


Figure 36: Security Awareness

As expected, people are more aware of personal data protection (*statements 2 and 3*) than information security (*statement 1*). People understand better what data protection means rather than what has to be done to secure devices than contain personal data. However people is also very concerned on how the companies are protecting their personal financial data (*statement 6*).

Almost all of our respondents (90%) think that existing regulations on personal data protection are not strong enough (*statement 4*). It can be correlated with a recent Eurobarometer published by the European Commission showing that trust in digital environment remains low. Two-thirds of the respondents (67%) say that they are worried about having no control over the information they provide online, while only a few (15%) feel they have complete control<sup>100</sup>.

Finally, to add a perspective to this never ending discussion, our panel of consumers understand clearly the business model of companies offering free services (*statement 5*) and the hidden counterparts around personal data. But their practices may differ (see 10.4.2 below).

<sup>100</sup> [Eurobarometer Survey](#) – European Commission – 24/6/2015

### 10.4.2 Security Practices

Being aware of security matters is important, we now explore how our panel deals with security on a daily basis.



Figure 37: Security Practices

Our IT oriented panel declares strong security practices. Most of them perform periodical backups of their devices (80%). That is in line with the adoption of Cloud storage solutions such as Google Drive, Dropbox or iCloud offered by the main players in the web industry. It is also interesting to compare the agreement with this statement against the feeling on free services asked in the previous question.

84% of our respondents check carefully their bank account statements to ensure that their financial institution made no mistakes. One of the main characteristic of security, integrity of the processes or services is still questioned. Although most of the financial transactions are handled now electronically without human interventions using wire transfers or credit cards, consumers are still worried that a hacker could jump into the process and corrupt it.

Responses on the third statement on password management are interesting. More than half (60%) change their password required to access main Internet web site at least once a month and use a different password for each site. However, we have to confront these positive statements with the reality where password '123456' is absolutely the most common password found on the Internet<sup>101</sup>. What is noteworthy here is that the number of people using those common passwords has dramatically decreased.

<sup>101</sup> SplashData's [yearly list](#) of the worst passwords on the internet (as compiled by more than 3 million leaked passwords from 2014)

Availability, another member of the classic Information Security triad (see 2.2 Security), is also required by consumers. 60% of our panel would change their eBusiness provider if they don't get maximum availability.

The two last statements about encryption and public network show that consumers are mostly aware of security risks. These good scores are showing that information and education to consumers on the use of digital resources are effective.

### 10.4.3 Personal Data Protection

Personal data protection is an important matter for European citizens. However moving toward a connected life requires more and more information sharing between consumers and companies.

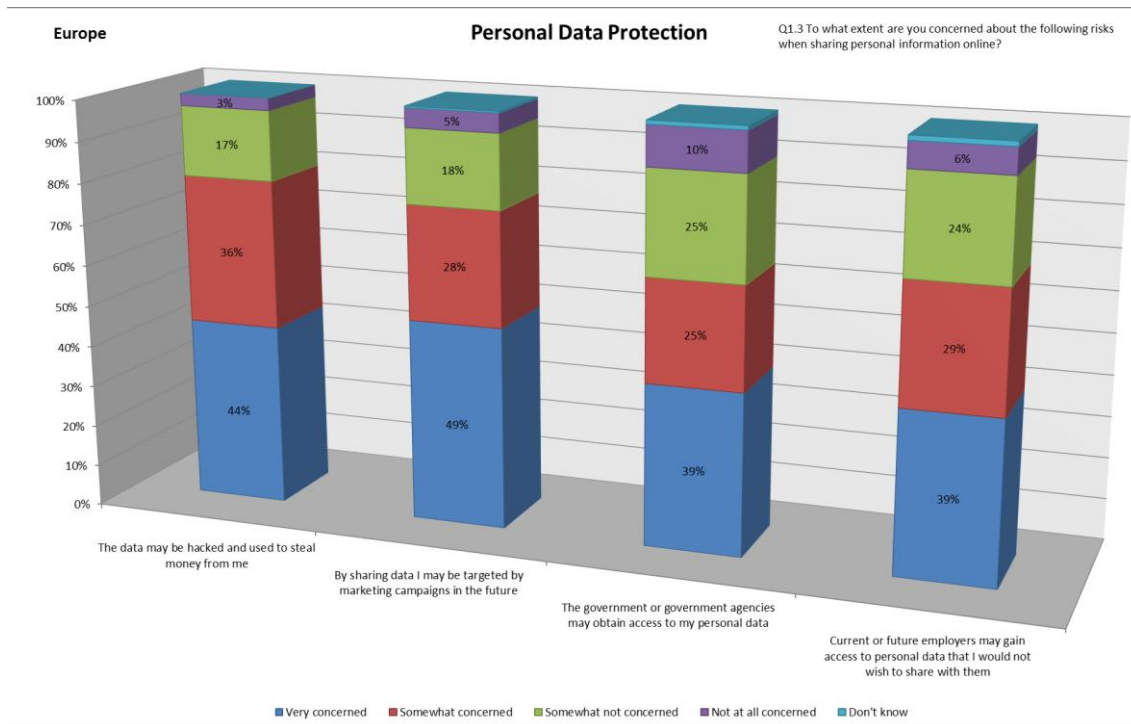


Figure 38: Personal Data Protection

The majority of our panel is concerned with sharing of personal data because it may financial losses (80%) or being targeted by unsolicited marketing campaigns (77%). Our panel makes also a clear distinction between personal and professional information. 68% want to control information passed to the employers. More than half of our panel (64%) is also concerned by the possibility of national authorities to access personal data without being consulted.

### 10.4.4 Confidence in Security Mechanisms

Here are some questions about confidence in security mechanisms for different devices or services.

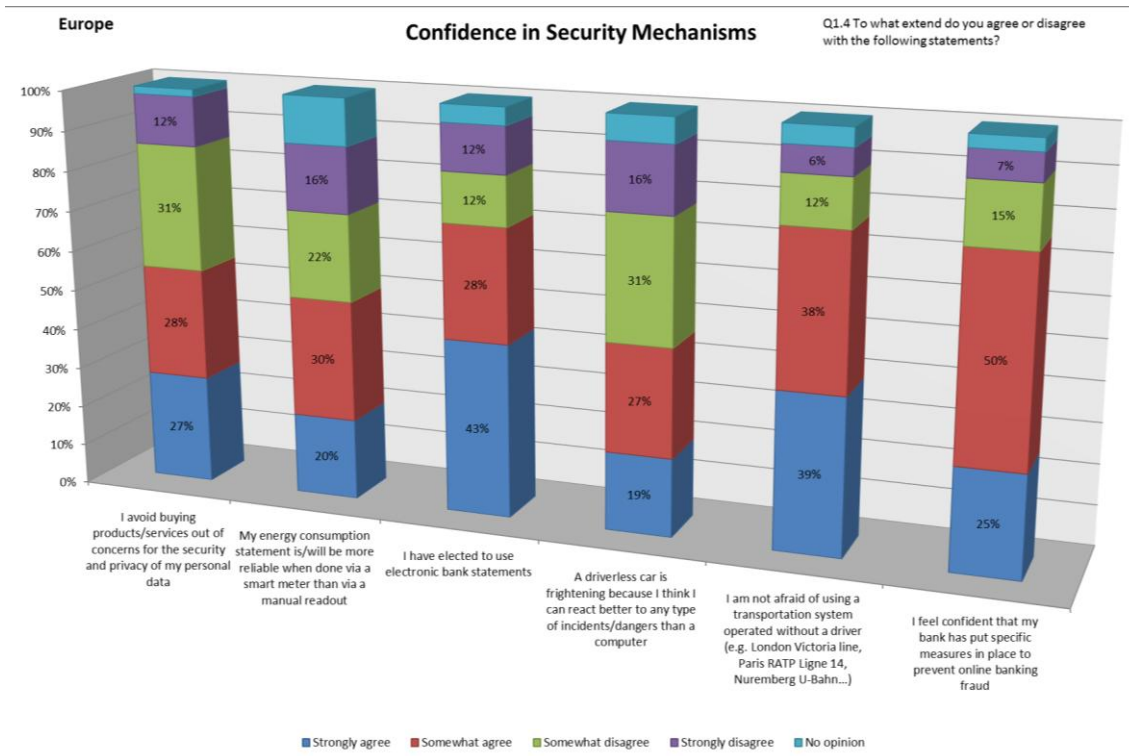


Figure 39: Confidence in Security Mechanisms

Will the many prototypes of autonomous cars find their market? If technology is today enough reliable in this area, people (at least half of our panel) are still afraid of using such self-driving cars. Interestingly the same panel members, by an overwhelming majority (77%), use without any fears automatic transportation system operated without a driver that exist in big cities or airports.

Our panel is confident in the security measures implemented by their financial institutions. They can be trusted to prevent frauds.

However, when dealing with personal or financial payment such as the energy bill through a smart meter, our panel members show a limited concern.

### 10.4.5 Criteria of Choice

Is security a criteria of choice when buying a new connected device? How does security compare to other features such as price or performance?

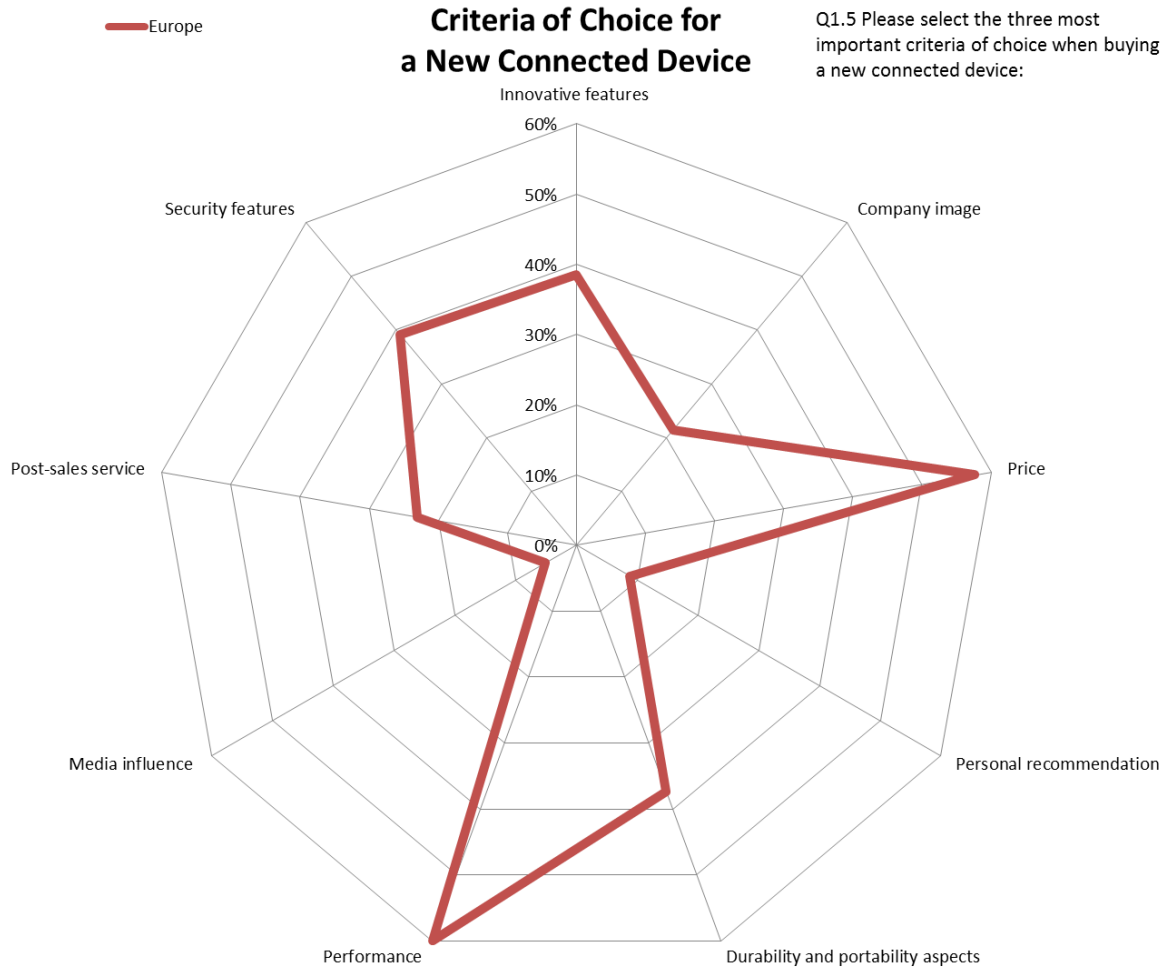


Figure 40: Criteria of Choice for a New Connected Device

Low price and good performances are the two main criteria evaluated by consumers when buying new connected devices such as a smartphone. Security comes to the podium at an interesting third place just before innovative features and durability aspects. External factors such as company image or post-sales service are lagging behind.

Media influence is very low as well, and, more surprisingly, personal recommendations.



Table 10: Criteria of Choice for a New Device

Criteria of Choice for a New Device	
By Age	Security Features
Europe	39,12%
Under 26 years old	12,50%
26-35	20,63%
36-45	28,46%
46-55	47,49%
Over 55 years old	47,59%

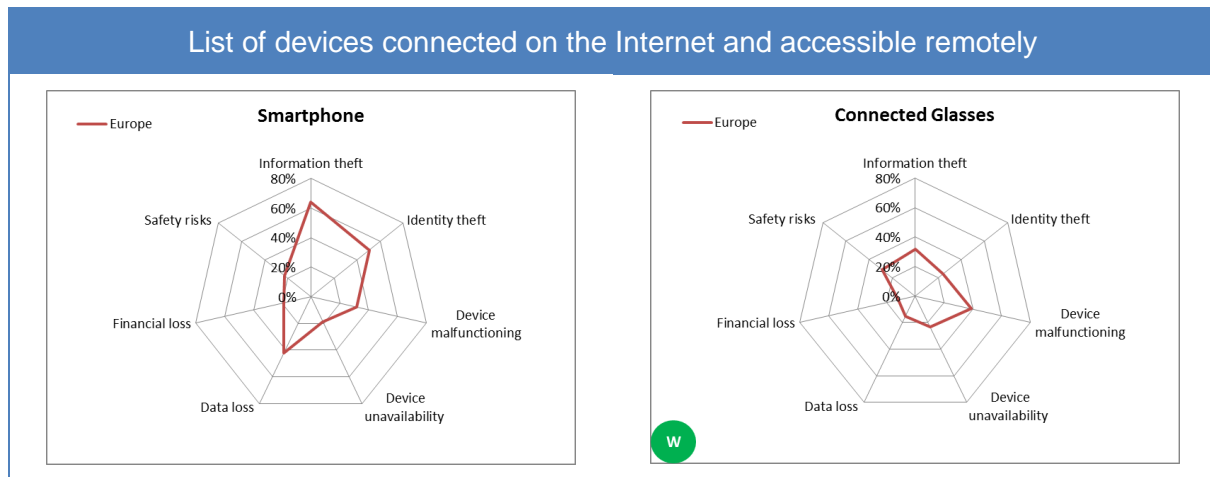
It is also interesting to notice that although there is no perceptible difference between countries on the criteria hierarchy, there is a strong difference for security due to the age of the buyer. Young consumers do not value security when buying a new device where older people do.

### 10.4.6 Main Security Expectations

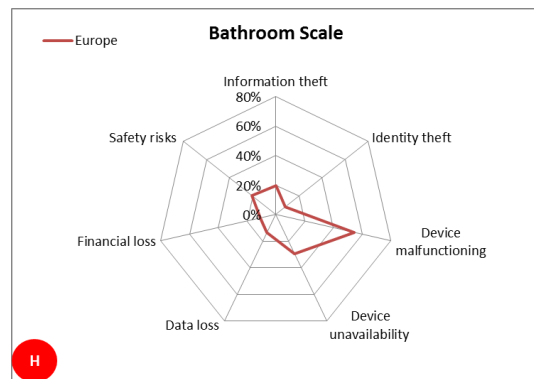
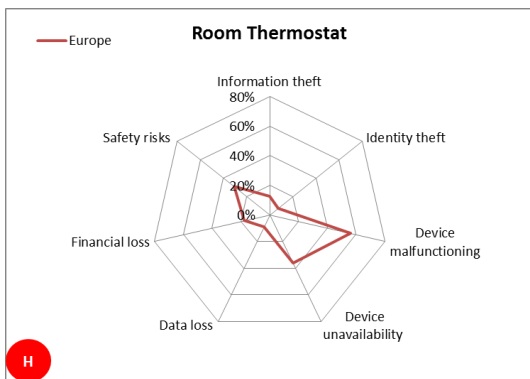
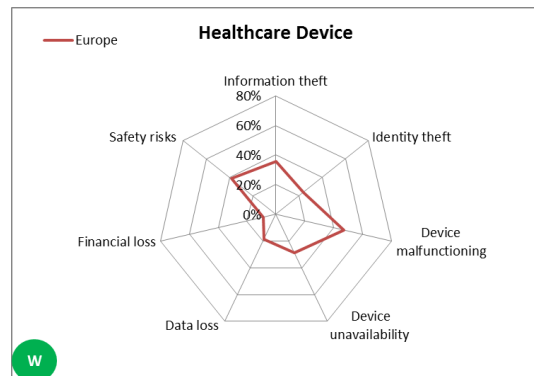
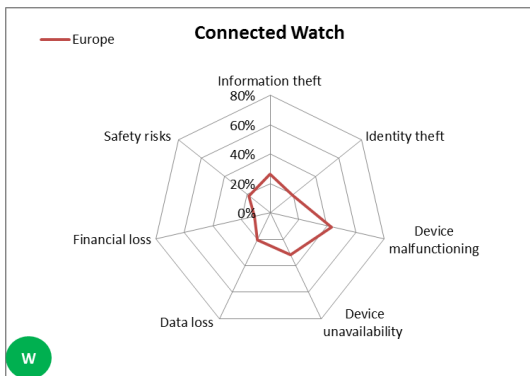
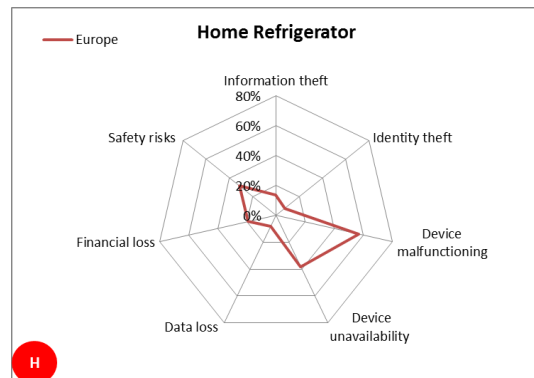
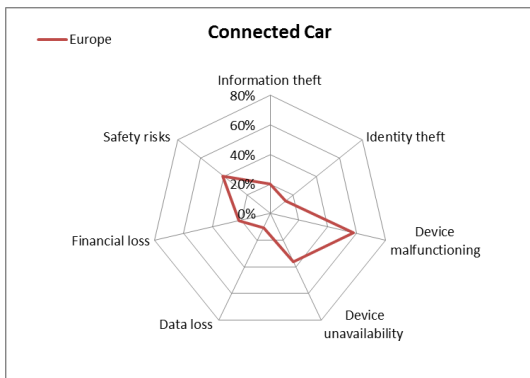
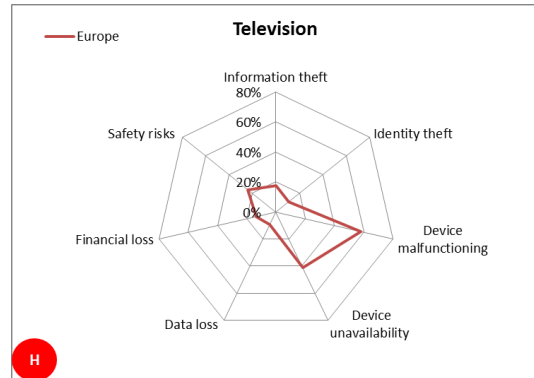
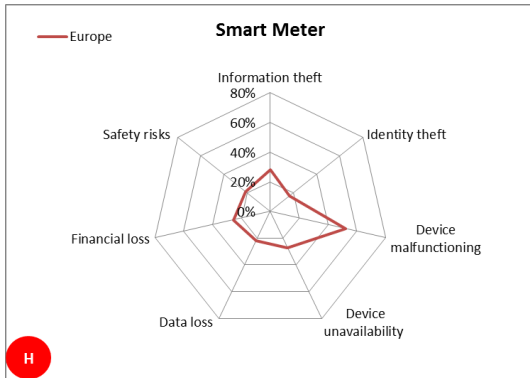
For various types of devices that may be connected to the Internet and accessible remotely, we asked our panel what were the three main security expectations. We proposed the following risks:

- Information theft
- Identity theft
- Device malfunctioning
- Device unavailability
- Data loss
- Financial loss
- Safety risk

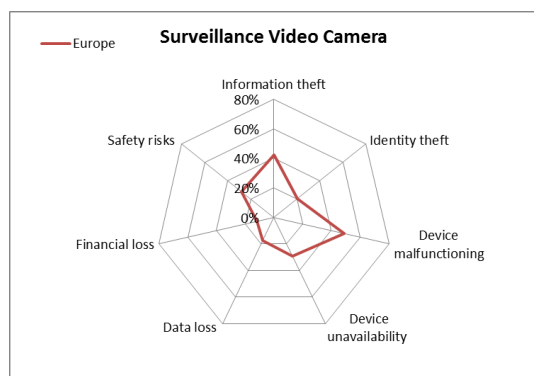
Table 11: Security Expectations on Selected Connected Devices



List of devices connected on the Internet and accessible remotely



## List of devices connected on the Internet and accessible remotely



Legend:



In house device



Wearable device

Analysing these results, we can highlight some interesting trends:

- In general, results are pretty much similar and do not show any notable difference when splitting data by age and/or country.
- Financial loss is not perceived as a security risk for connected devices and therefore not taken into account. Although all the proposed devices will sooner or later have links with financial transactions, it is not a risk perceived by our panel.
- Safety risks are also underestimated. More surprisingly, even the 'safe and secure' characteristics of a car is evaluated by our panel as important as these for a home refrigerator.
- The panel has the same common security expectations for the devices that connect the house to the Internet. Availability and integrity are the two most important requirements far beyond others with the notable exception of the smart meter. Consumers may be not aware that the smart meter could play the same role as the set top box in the smart house providing the complete set of services to the homeowner.

The risks of identity theft and (personal) data lost for in house devices are not important for our panel members. They probably trust the companies involved in the communication chain (device manufacturer, Internet service provider, service provider) in securing the entire connection.

- All wearable devices show a similar profile in term of responses. Security requirements are limited. The correct functioning of the device is more important than its availability. These devices are in a very early phase of adoption and the market of wearables is still maturing. Requirements may change in the future.
- In Europe, connected cars should function correctly (58%). However, and that is a main exception to what was written previously, German respondents put less importance into that requirement (34%) where Italians consider it is the most important (73%). Is it a sign of German quality?
- Smartphone has a unique profile due to its mass adoption and its ubiquity in our daily life. Our respondents care about confidentiality (information and identity thefts) more than integrity and availability. Although we can run financial transactions with our smartphone, it is not a risk that is considered. Safety, again, is also not a problem.

### 10.4.7 Trust in Data Privacy Enforcement

Which organisation is perceived as protecting correctly our personal data?

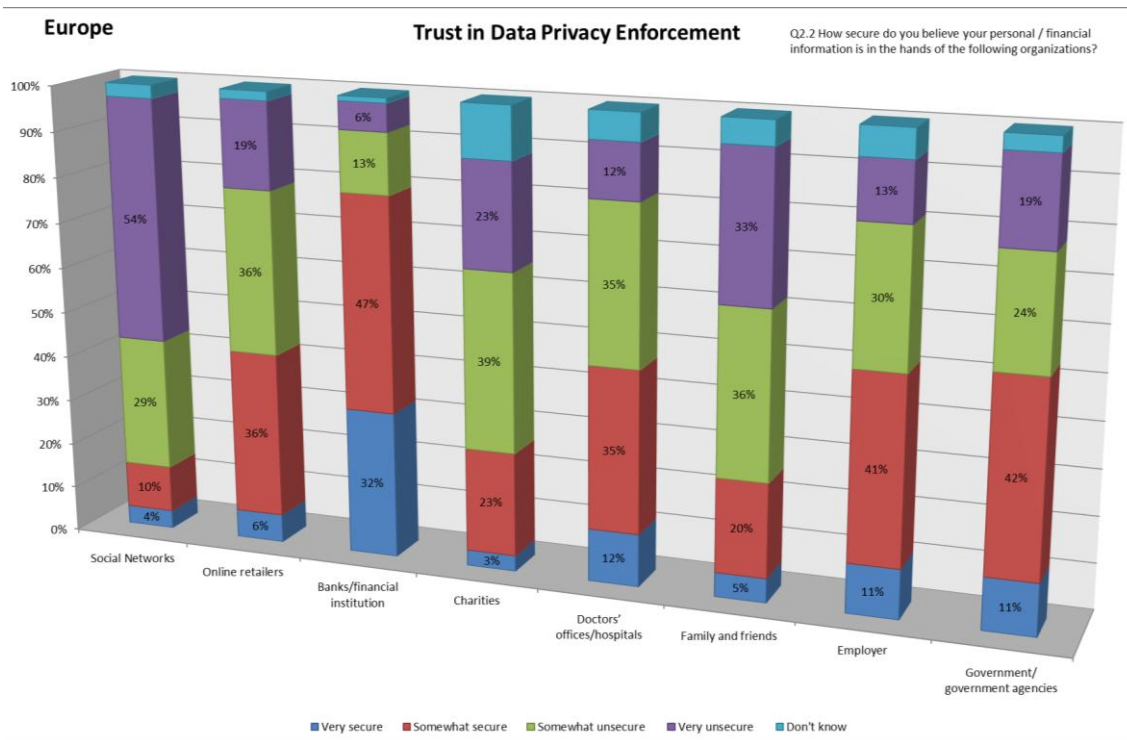


Figure 41: Trust in Data Privacy Environment

Banks/financial institution	80%
Government/ government agencies	53%
Employer	51%
Doctors' offices/hospitals	47%
Online retailers	43%
Charities	26%
Family and friends	26%
Social Networks	14%

When combining 'Very secure' and 'Somewhat secure' answers, banks and financial institutions are clearly ahead in the list where social networks rank last among proposed organisations when dealing with personal and financial data.

### 10.4.8 Decision Factor

As Information security becomes important in the Internet of Things, we ask our panel who would give them confidence that the device they want to buy would have the right level of security.

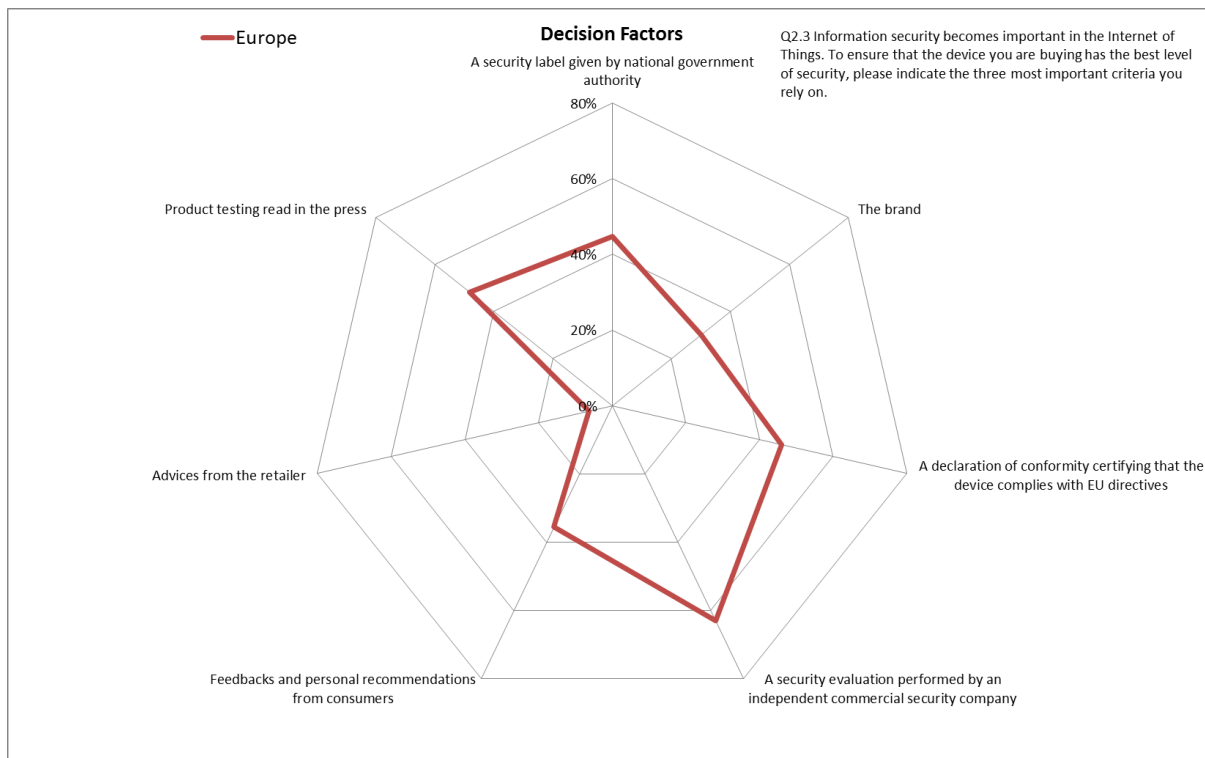


Figure 42: Decision Factors

Results confirm that the most important advisor is an independent security company performing a security evaluation. Tests published in specialised publication come in second. Placed almost equal in third position come a declaration of conformity certifying that the device complies with EU directives and a security label given by national government authority.

In the project context, it shows that the CC certification, performed by an independent certification authority that is backed by European and national authorities is a great value to reinforce consumer confidence in the security characteristic of the products they want to buy.

### 10.4.9 Trust in Technologies

Throughout history technological innovations have often led to greater efficiency in our daily lives. Modern information technology enables us to be connected to the world. Despite the fact that it is early days for the Internet of Things, it has the potential to touch every aspect of our lives - from our bodies to our communities to our work places to a fully connected world. It also promises to improve our well-being, raise our quality of life, increase productivity, and foster better cooperation and collaboration.

Statement	Agree
Concerning Internet connection during a flight, I am concerned about possible negative interference, such as virus infection from my personal device, to the plane control applications	44%
Concerning Internet connection in a car, I am concerned about possible negative interference to the car driving applications in case of intensive download	57%
For fear of hacking, I am very concerned of using a new computerized medical device (pacemaker, insulin pumps...) that requires an Internet connection	58%
I am afraid that smart house technologies may open a window into my house to unauthorized people (hackers, burglars...)	70%
I am worried about the data security practices of companies whom I provide with my personal information in order to allow personalization of their services through connected devices	82%

Figure 43: Trust in Technologies

We therefore asked our panel how much they trust various technologies used in their daily life.

On average, our panel is rational with technology. Respondents trust it.

But about half of the panel thinks that there is security exposure by using technologies in plane or car.

When their health and personal data are concerned, our panel members are somehow even more worried.

And their main concern is not about technology itself but how companies implement and use technology. Because all recent news about leaks and exposure of personal data published continually in the press, they are very concerned of protecting their personal information.

### 10.4.10 Security Mechanisms Awareness

The last question was possible due to our specific IT-oriented panel.

We wanted to understand better what mechanisms people were using to secure their personal device (PC, smartphone or tablet) when installing a new application program from the Internet (such as a calendar application, a software phone, a photo processing software).

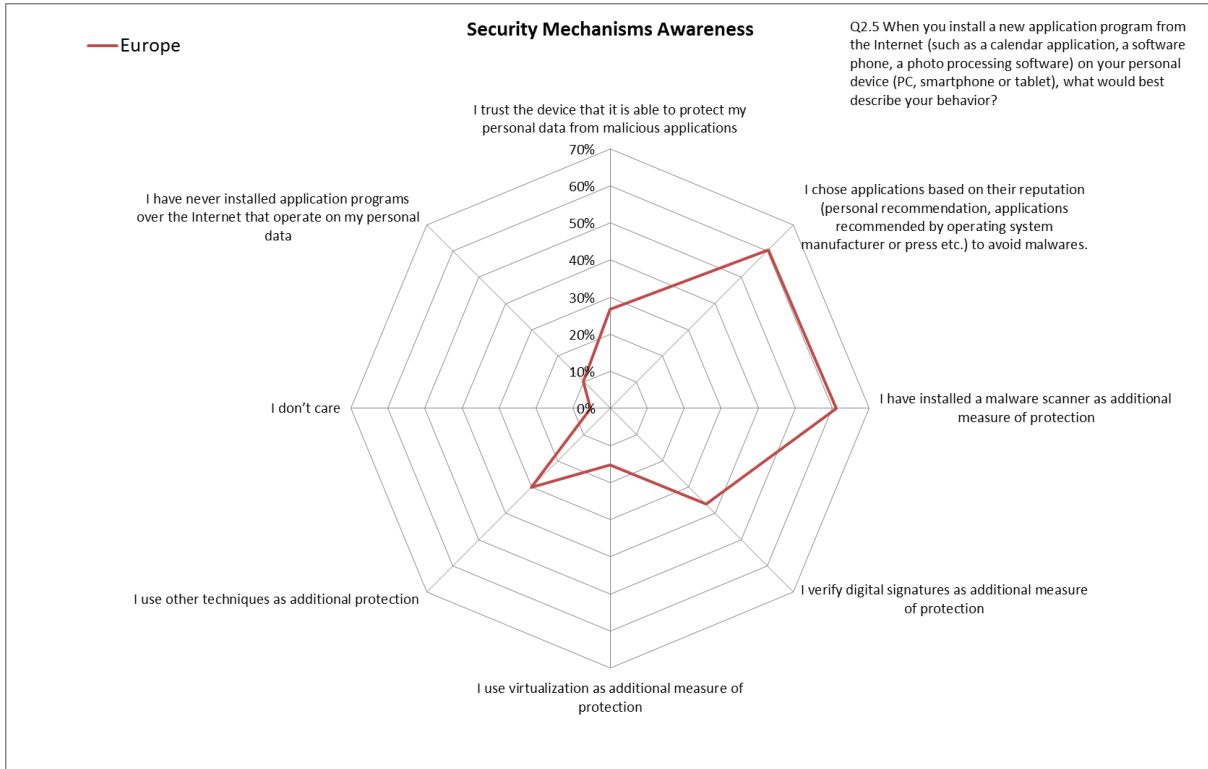


Figure 44: Security Mechanism Awareness

Good news!

Everybody care. 95% of the respondents try to protect their device. They first use trusted devices able to protect their personal data and use applications *certified* not to be malwares. Antivirus and malware scanners help them to reinforce security.

Other means of protections such as digital signature, virtualisation, and others are too technical for average users and not implemented at a large scale.

# Chapter 11 Big Data Analysis: Listening to the Consumers

To further dive into our knowledge of the customers, we wanted to supplement our existing work with social media and consumer information data sources to gain direct customer insights.

Today, more and more contact points with the consumer are digitalized and the barrier between on and offline communication disappear. It is therefore possible in a strategic planning perspective to listen to what consumers are saying in their digital life (social networks, forum, tweets...). We performed a Big Data analysis where we listened consumers' comments on security and technology. The objective was to answer questions such as:

- Does security sell?
- For connected devices, how present is security in the consumer's purchasing decision?
- How are European markets different in that regard?

The development of content creation technologies and social networks has simplified the broadcasting and sharing of content between consumers/citizens. Analysing public web content (online conversations, product reviews, news articles etc.) on the subject of security in connected devices can give us a good insight of the market and its evolution.

For time and budget reasons, we choose to limit our analysis in three ways: first we focused on three key European markets: Germany, France, and the United Kingdom. Then, we also decided to select a well-established market segment. The smartphone segment hit a record high in 2014 in terms of units shipped and market value as seven out of ten people in Western Europe now have a smartphone<sup>102</sup>. Finally, we centred our analysis specifically on the customer journey analysing online conversation on smartphone purchases.

Even if the scope is voluntarily restricted (device, markets, process), the smartphone example is significant enough to make this analysis relevant on security awareness and needs of European consumers regarding connected devices.

We couldn't apply the same level of analysis to another market segment for time and budget reasons as already mentioned, but we decided to make a first level of data analytics on the automotive market. The result of this study is described in the last chapter and concludes this investigation.

## 11.1 Big Data Analysis Methodology

In this chapter, we explain the environment, methodology and tools used.

---

<sup>102</sup> Source IDC : [Smartphones Hit a Record High](#), February 2015



### **11.1.1 What is Big data**

Big data is data being generated by us and everything around us at all times. We create a lot of data in our digital life. On the web, every digital process and social media exchange produces it. Things also create a lot of data. Systems, sensors and mobile devices, the key components of the IoT, produce and transmit “little data” that are collected and gathered in high quantity to become some type of big data where treatment can apply.

Big data is high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing that enable enhanced insight, decision making, and process automation<sup>103</sup>. Volume<sup>104</sup> refers to the amount of data, variety<sup>105</sup> to the number of types of data, and velocity<sup>106</sup> to the speed of data processing.

To make sure there is no confusion, please notice that the type of Big Data we used for the analytics is different from the Big Data that will be part of the IoT paradigm (even if in the future some overlap is expected). In our study, we focused on social media data, information created and curated by individual users and collected from public spaces, such as:

- Social media networks: Tweets, posts, favourites, sentiment
- Social search: keyword analysis and hashtag tracking
- Long-form publishing platforms: blogs, wikis, and social opinion sites such as Yelp
- Public multimedia content-sharing platforms: SlideShare, YouTube, Flickr, etc.

### **11.1.2 Digital Insighters**

To help us in this analysis, we worked with Digital Insighters, a company based out of Paris, France that offers services in Big Data analytics, Consumer Insights, Crisis Management and Reputation Management. Their experts handle a long range of business problems from tactical decisions to multinational strategies.

We defined with Digital Insighters<sup>107</sup> the security topic that we wanted to address and listed the social media sources the most relevant to be analysed. Digital Insighters consultants started to dive into the data beyond the usual simple social media metrics to connect them with our security of connected devices theme.

After collecting data, they gathered insights and created visualisation dashboards included in the following sections, allowing for a better understanding of trends and behaviours. They helped us on our analysis, exploring how customers behave in relation to secure connected devices, what are the main drivers that improve awareness, who influences the market and what are the market dynamics. They also provide us with country specific information to allow comparison.

---

<sup>103</sup> Gartner's IT Glossary: [Big data](#)

<sup>104</sup> The internet facilitated a massive data explosion. Massive volumes are generated daily by major websites. Google indexes 20 billion pages per day. Twitter has more than 500 million users and 400 million tweets per day. Facebook generates 2.7 million 'Likes' per day.

<sup>105</sup> Data can be stored in multiple traditional formats (For example database, excel, csv, txt) as well as untraditional formats (image, video, SMS, pdf...)

<sup>106</sup> Velocity deals with the pace at which data flows in from sources like business processes, machines, networks and human interaction with things like social media sites, mobile devices, etc. The flow of data is massive and continuous.

<sup>107</sup> [Digital Insighters](#)

### **11.1.3 Collected big data**

This study is based on one year of social data collected between July 1<sup>st</sup> 2014 and July 31<sup>st</sup> 2015 by Crimson Hexagon. Partner of Digital Insighters, this company is a social media analytics company based out of Boston, Massachusetts with a European division in London, England. The company's social media data library consists of over 500 billion posts, and includes documents from social networks such as Twitter and Facebook as well as blogs, forums, and news sites. Social media data is categorized by location using IP address or domain name, and language. To exploit its social media library, the company proposes a set of tools that monitors and explores consumers' conversations. Using a proprietary algorithm, the tool detects trends (keywords or phrases) over time (as granular as hourly) and performs sentiment analysis. A machine-learning algorithm allows categorization such as "intent to purchase" or "love the ad" and gives the ability to correlate those categories together.

### **11.1.4 Listening to Customer Analysis**

For our work, we decided to analyse the public web content (online conversations, product reviews, news articles etc....) on the subject of security in connected devices. Data came from the database of 500 billion public web documents (Blogs, Forums, Twitter, news websites, reviews...) managed by Crimson Hexagon. An analytical model has been set up to collect and crunch data relevant to this study. Its scope was defined in workshops between EURO-MILS and Digital Insighters.

In a first iteration (see 11.2), we limited the collection to English conversations related to our theme. We studied millions of online conversations to answer and understand the following questions:

- Are consumers realizing more and more objects are connected?
- Are consumers conscious these connected objects can pose security and safety risks?
- Are consumers looking for secure solutions?

An additional goal was to evaluate the amount of data available.

In a second iteration (see 11.3), we then focussed our analysis on a specific connected device, the smartphone, as being representative of a well-established market and susceptible to generate enough data to support the analysis. We analysed awareness and needs of European consumers regarding smartphones. As mentioned previously, a specific focus was given on conversions around purchase decisions. We also enlarged our data collection to include French and German conversations to be able to drive a comparison on three key markets (France, United Kingdom, and Germany), representative of European opinion.

The model was then implemented in social analytics tools, for: parsing, semantic analysis and trend discovery. We used the Crimpton Hexagon tool to identify more than 10 million relevant data and used the algorithms and machine learning to perform the first layer of analysis. The application produced a set of data-driven insights reports around questions, discussions, and interactions between European consumers on security and connected devices.

Human analysts then provided an understandable interpretation of the data. With the help of Digital Insighters experts, we exploited results to extract key insights and draw up this report.

## 11.2 First Iteration: Connected Device Online Conversations

In the first iteration, we extracted 14.7 millions of conversations about connected devices from the global social media database. To be selected, data should include keywords issued from a combined list of keywords characterising the domain. The list includes words such as device name (smartphone, television, connected watch, iPhone...), brands and categories (Apple, Samsung, Google, consumer, automotive...), technology types or concepts (operating system, network, access control...). This list was again filtered to select the 61K conversations about security and safety risks. Such conversations included security oriented words such as risk, secure, security, or damage. Finally, we added filters to select security solution conversations.

Of course, the relative size of the sets depends essentially on the filtering criteria. But nevertheless, it demonstrates the importance of the criteria in the domain.

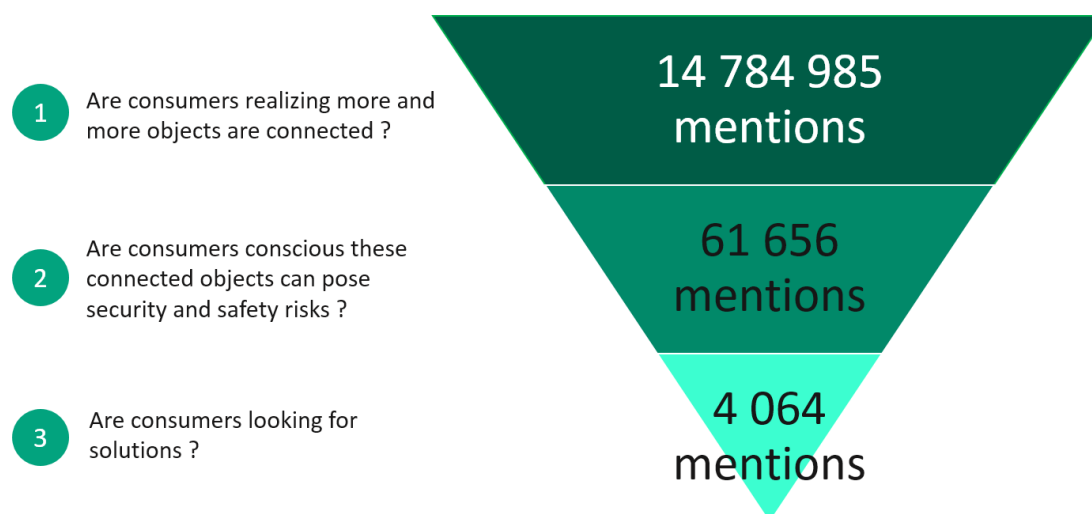


Figure 45: From Awareness to Protection

The same data set was then analyzed with a chronology viewpoint from 2014 to 2025. It shows that discussions on security and safety increase when an external event occurs (here, two announcement from Apple).

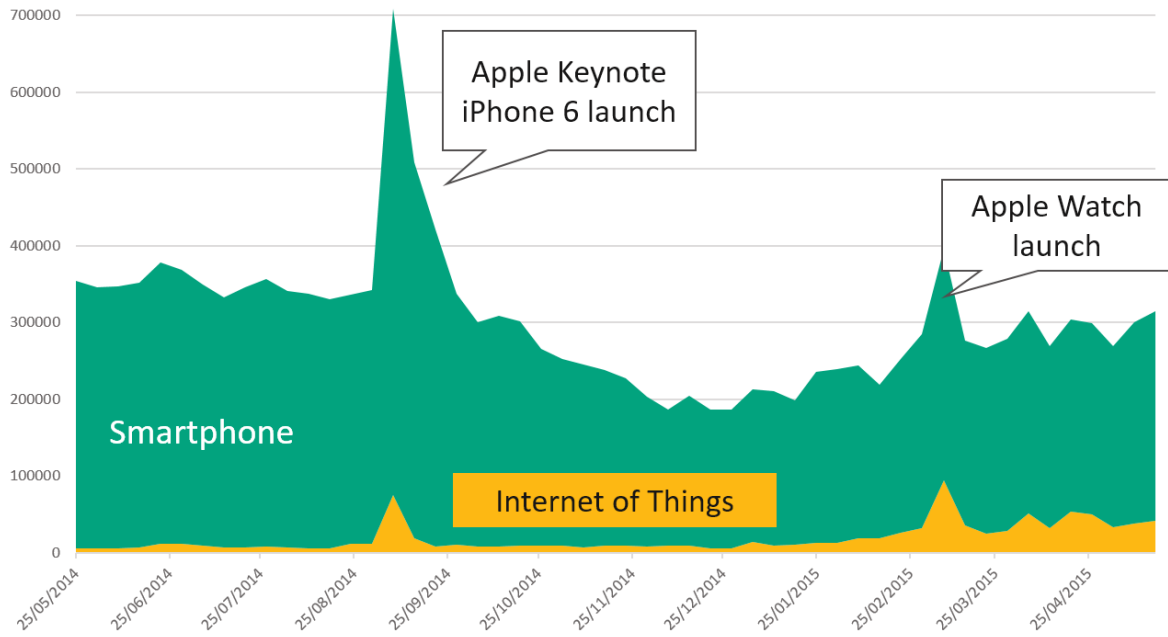


Figure 46: Conversation Chronology

Finally, if most of the conversations on connected devices deal with smartphones, wearables objects, mHealth, smart home and connected cars are also discussed. Their limited presence is also due to the fact that there is no common buzzword or generic name for their domain. For example, autonomous or driverless cars are all connected and can be mentioned as Google car, electric car, or even by naming the make and the brand (BMW 5 Series, 508 Peugeot).

### 11.3 Second Iteration: The Smartphone Customer Journey

In a security and safety context, there are four steps in the journey of a customer willing to buy a smartphone.

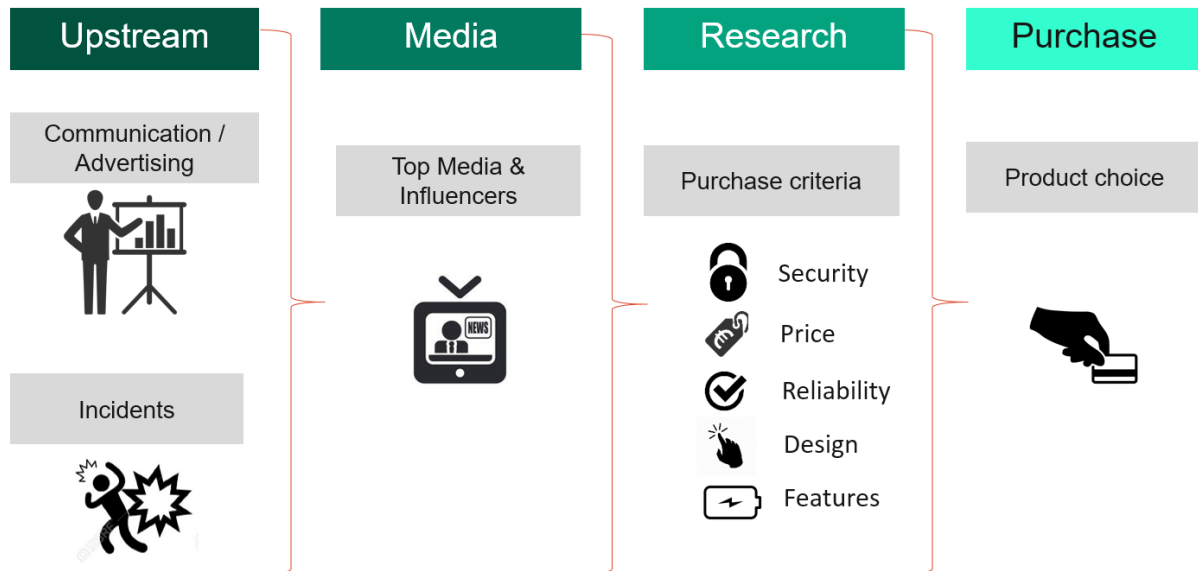


Figure 47: Smartphone Customer Journey

In the “Upstream” phase, consumers hear about smartphone security in their daily lives from two opposite sources. They are influenced by targeted communication and advertising. Enterprises involved on the smartphone market, i.e. vendors such as Apple or Samsung, operating system makers such as Google (Android) or Microsoft (Windows Phone) or telecommunications companies such as Orange or Vodafone regularly communicate on their product’s safety and security features. They communicate either directly to consumers through traditional advertising (TV, Radio, online ads...) or through public relations when their releases are mentioned in the news.

Security incidents, problems with smartphone security such as a hack or flaw, or more generally a security & safety issue with connected devices are frequently publicized in the news. Safety problems with the smartphones such as battery overheating and exploding are also reported on the web as well as in specialized and consumer newspapers. These articles influence consumers’ buying decision.

So it is important to characterize the different media outlets some have more authority than others when it comes to covering smartphone security and safety. There are also some important influencers: key opinion leaders which stand out in public debates about security and safety in connected devices.

Before the smartphone purchasing decision, consumers research the product and weight it along different criteria. The process varies in length and in topics:

- **Security:** How safe and secure the smartphone is
- **Price:** Price of the product compared to the competition and the consumer’s budget
- **Reliability:** Life span, resilience to bugs, or performance issues of the device.
- **Design :** Exterior look, friendliness of user interface, and user experience
- **Features :** Camera, battery life, performance, apps availability

And finally, in light of all his research and influences, the consumer make a product choice and buy a specific smartphone.

The following figures show the customer journey in three European countries: France, Germany, and UK.

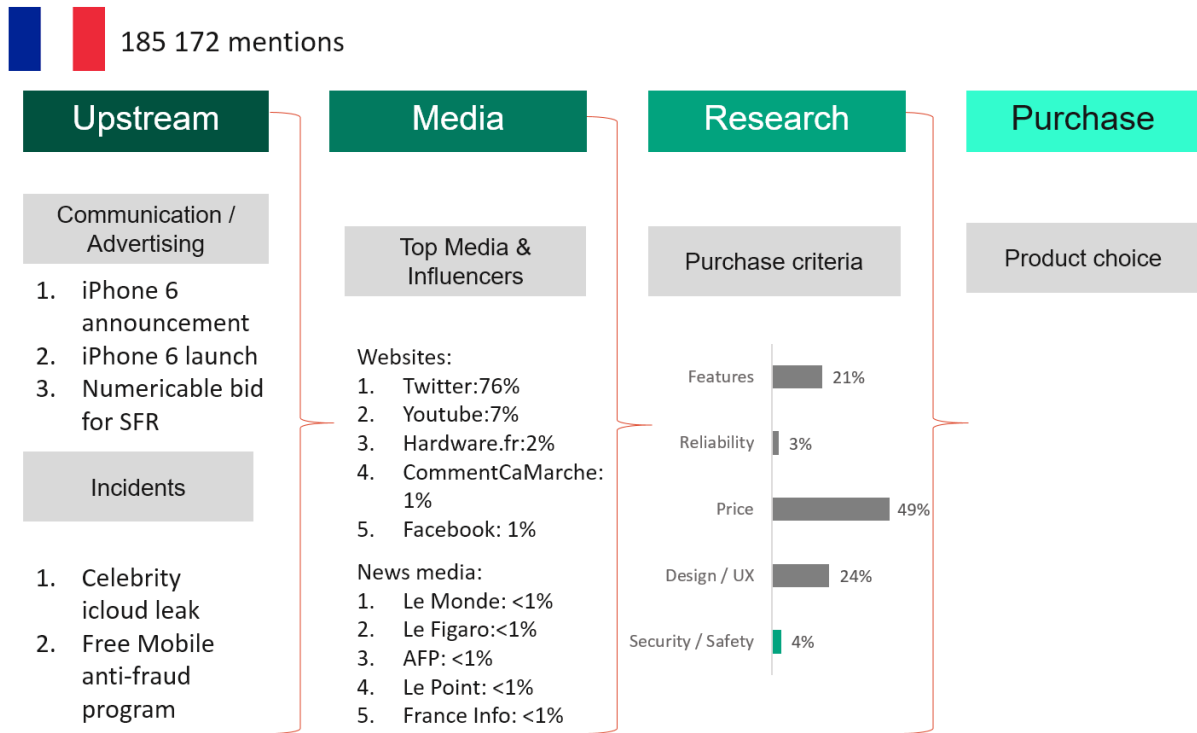


Figure 48: Smartphone Customer Journey in France

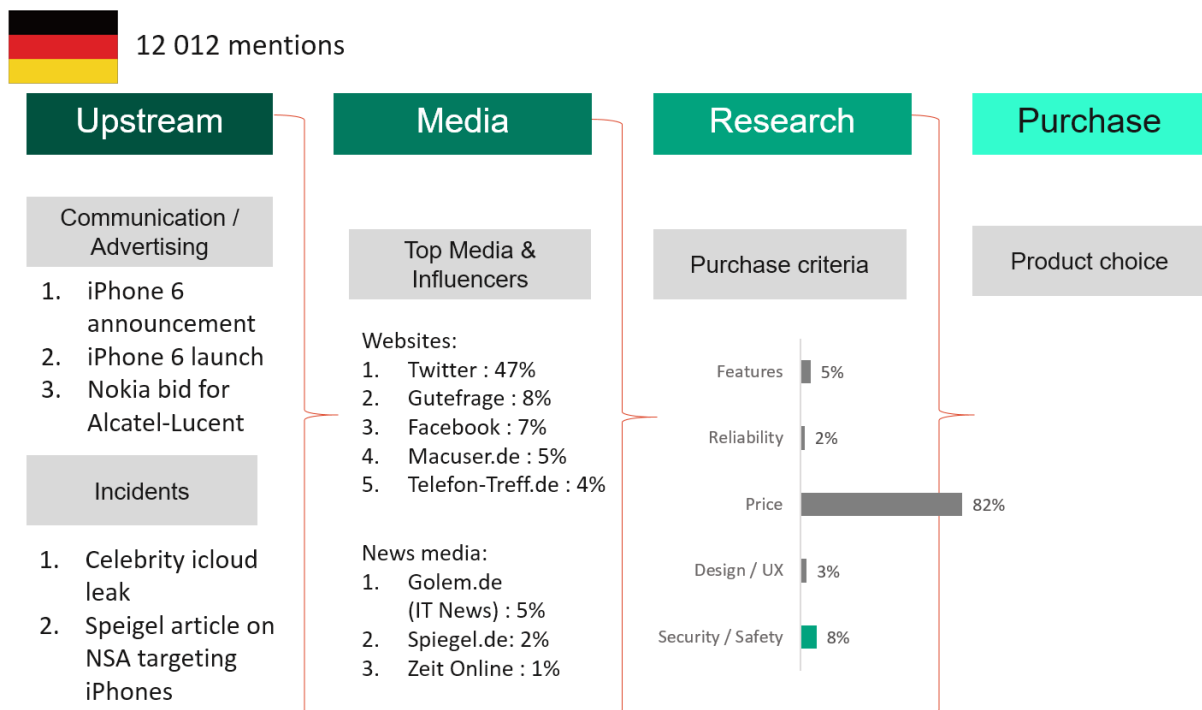


Figure 49: Smartphone Customer Journey in Germany



1 124 564 mentions

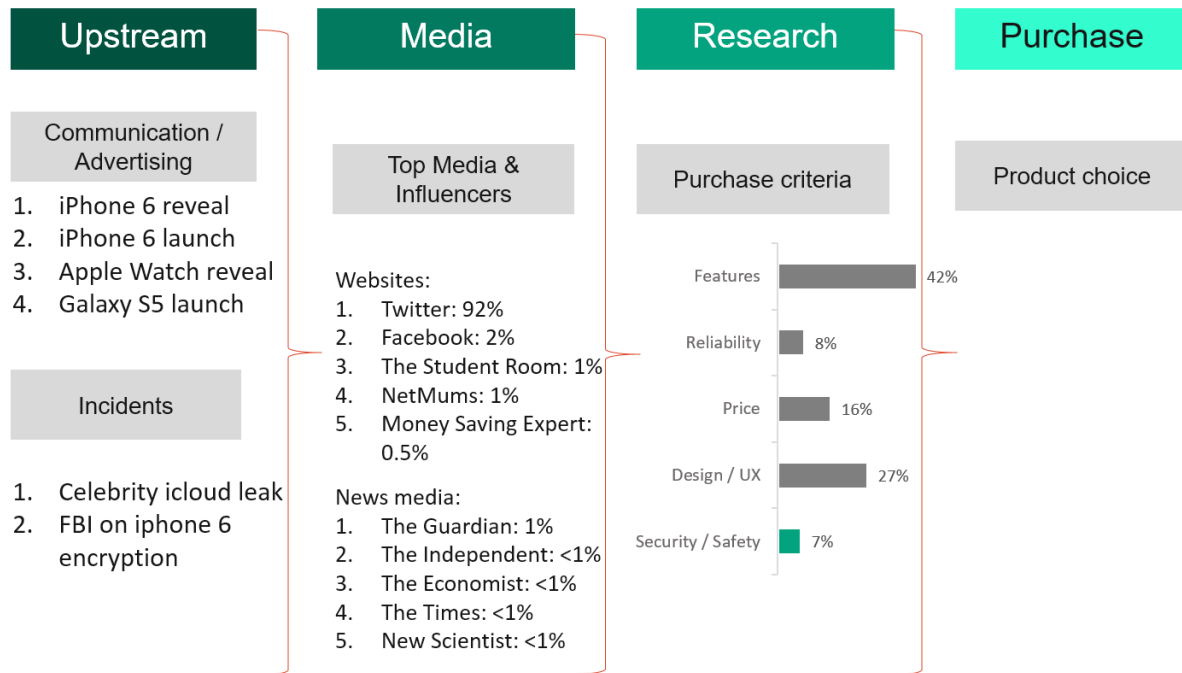


Figure 50: Smartphone Customer Journey in the UK

### 11.3.1 Mention, Upstream, and Media: Explaining the Results

All numbers of mentions about security and connected devices are statistically significant and can be exploited and analysed. However, they vary by country. Obviously, English is more common as it is the language of technology and people fluent in English have access to a large source of information from international web sites. Discussions in German are less frequent. It is probably due to the facts that technology geeks and consumers are likely to speak English and therefore discuss also on English websites where discussions between many participants can take place. Numbers of mentions in French on security and smartphones is aligned to the size of the population.

During the selected period, some important events created awareness globally in Europe. The iPhone 6 announcement and launch was covered in all countries and ads campaigns were launched in all geographies. Some events were specific in a given country: the cable company Numericable's bid for the telecom company SFR in France, the Nokia bid for Alcatel in Germany, and the Apple Watch launch in the UK. Incidents such as the celebrity iCloud leak<sup>108</sup> also were reported globally where local events had specific importance in the countries: the anti-Fraud program by the French telecom operator Free<sup>109</sup>, the FBI criticisms<sup>110</sup> for being unable to read iPhone 6 user messages in the UK or the article of the German newspaper Spiegel on NSA targeting iPhones<sup>111</sup>.

On the Top media and influencers, we don't need to introduce *Twitter*, *Facebook*, or *YouTube*. In France, *Hardware.fr* and *CommentCaMarche* are two influent websites where

<sup>108</sup> Wikipedia : [2014 celebrity photo hack](#)

<sup>109</sup> Univers Free : [Des contrôles aléatoires de sécurité pour éviter les fraudes](#)

<sup>110</sup> The Register : [FBI boss: Apple's iPhone, iPad encryption puts people 'ABOVE THE LAW'](#)

<sup>111</sup> The Spiegel : [iSpy: How the NSA Accesses Smartphone Data](#)

consumers discuss about products and technology with large forum oriented on technical problems. For the German market, *Gutefrage* is a very popular review website, *Macuser.de* is an influential Mac website where most Apple products are discussed and *Telefon-Treff.de* is a specialized news website about any smartphone related topics. In the UK, *The Student Room* is a media specialized in University student life, *NetMums* is the most influential website on motherhood and family related topics, and *Money Saving Expert* is a website that shares tips on saving money and relays promotions and deals.

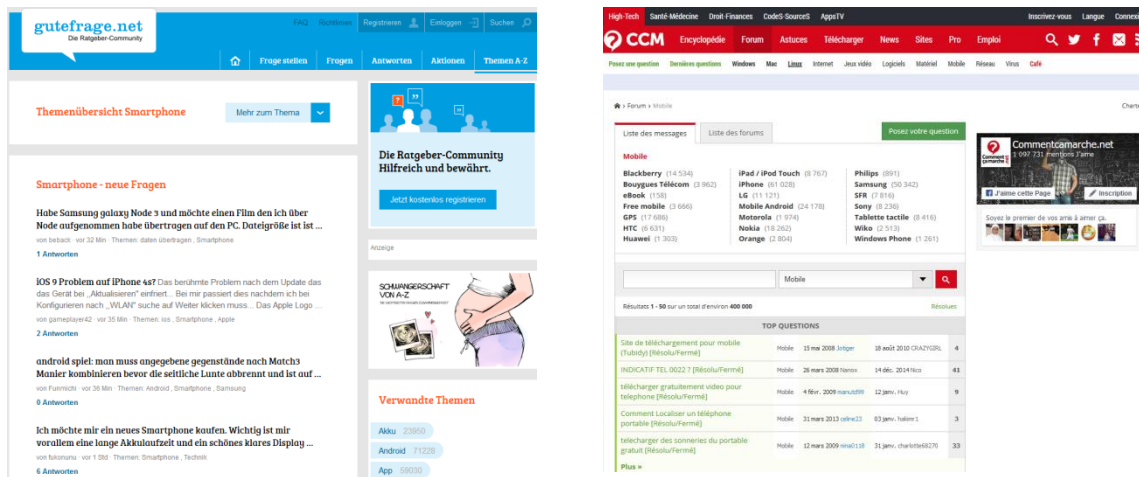


Figure 51: Influent Web Sites in Germany and France

### 11.3.2 Research: Exploring the Results

Figure 52 shows the relative importance of the five purchase criteria for a smartphone by country.

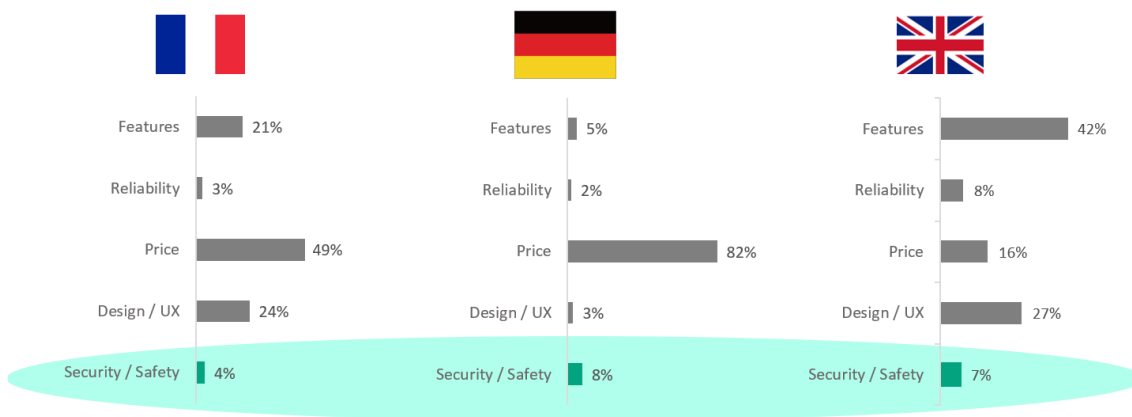


Figure 52: Purchase Criteria by Country

There are slight differences between countries. Consumers in the UK attach more importance to features (42%), design and user experience (27%) of the smartphone than price (16%). In France, price is the most important criteria (49%) but features (21%) and design (24%) are also considered. In Germany, price is the most and quite unique criteria of discussion (82%). This may be due to the market segment and the age of the consumers. Middle-aged consumers discuss more on forums than Twitter.



In general, security and safety capabilities of a smartphone are not that important. They are the 5<sup>th</sup> purchase criteria for France (4%) and the UK (7%), and in second position (8%) in Germany but far away from price<sup>112</sup>. This result confirms comments made by members of the Industry panel about the fact that customers do not care about security and safety (see 8.1.4, page 63) as well as results from our survey showing that consumers understands better what data protection means rather than what has to be done to secure devices than contain personal data (see 10.4.1, page 112).

Generally speaking, the subject of security and safety is a limited but slowly growing theme in conversations in Europe but not to the point where it becomes an important decision factor. As a purchase criteria, it is very volatile on the French market aligned to security incidents but more stable in the German market. Chatter spikes arise when a security incident is announced in the media. We also confirmed this increase in security discussions linked with security incidents when analyzing more recent data. After discovery of a significant flaw in Samsung devices that lets in hackers<sup>113</sup>, specific discussions about security increased to 13% of the total discussions about smartphones and becoming the third most important theme after price and features.

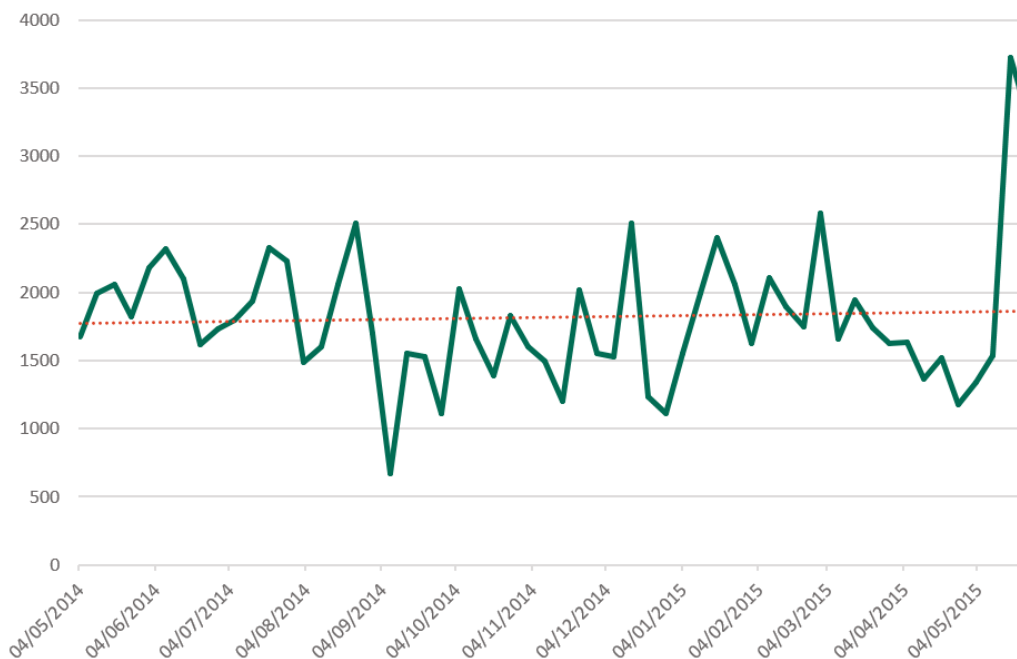


Figure 53: Total Mentions of Security in Conversations

## 11.4 Focus on Operating Systems

We investigated our results to understand the consumer's perception about security of smartphone's operating systems, mainly iOS and Android, Windows Phone mentions being limited and not relevant for statistical analysis.

<sup>112</sup> Price is often mentioned in pre-buy or post-buy conversations in Germany. Consumer review websites are also more popular in Germany than in other European countries.

<sup>113</sup> CNN : [600 million Samsung Galaxy phones exposed to hackers](#) – July 2015

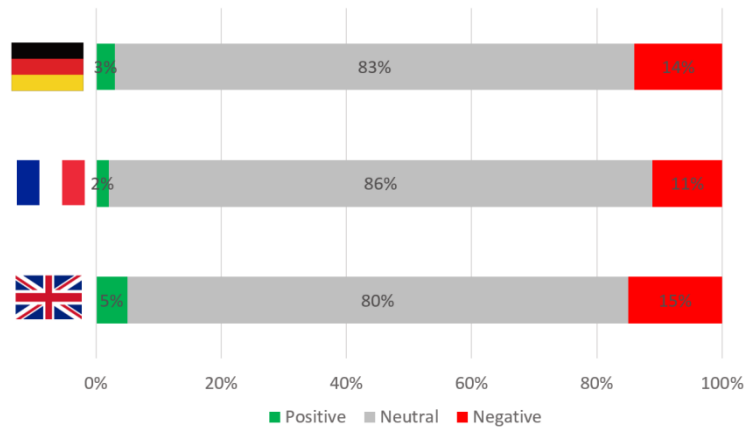


Figure 54: Security Perception of Operating Systems

As expected, discussions about security are almost neutral with a small percentage of negative sentiments and an even smaller percentage of positive ones. Consumers having a problem with their smartphone are more likely to react on the Web than satisfied ones. It is probably also due to the fact that media publish reports on potential security problems and how to prevent them.

Verbatim Media



Verbatim Consumers

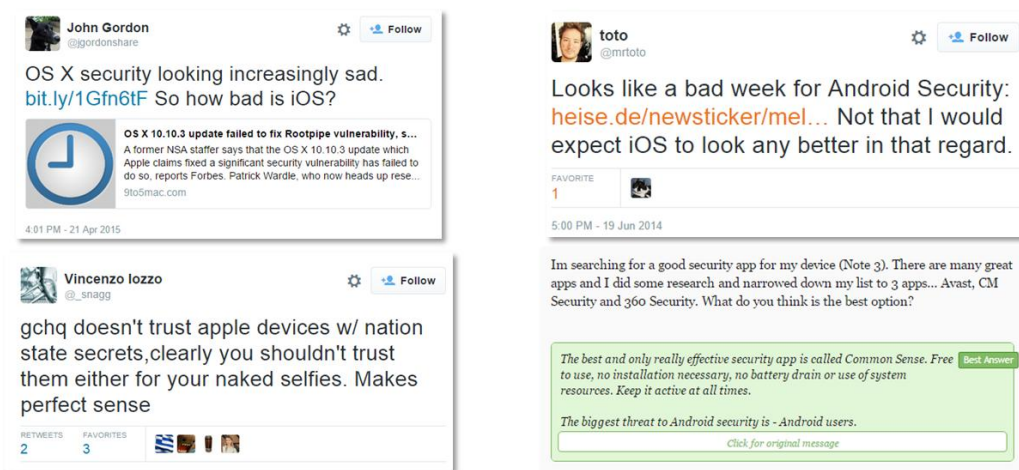


Figure 55: Security Perception of Operating Systems – Verbatim

## 11.5 Security Sensibilities in the Automotive Industry

To conclude on this Big Data analysis, we explored the segment of connected cars as more and more information are now available. Automobile makers are publicizing their researches in this domain, recognized companies such as Google or Apple are experimenting new connected software for the automotive industries. And last but not least, hackers and criminal gangs are targeting connected cars in all possible manners. And their exploits are reported in the news<sup>114</sup> and then discussed in the Web.

On the selected dataset, we compared the car and smartphone discussions. Figure 56 and Figure 57 shows the relative importance of the topics. Note that to overcome the problem of the small data amount collected during our first analysis (as mentioned in 1.2), we decided to cover the automotive segment with the overall discussions about cars by owners. The keyword of “connected car” was replaced by the keyword “security” instead.

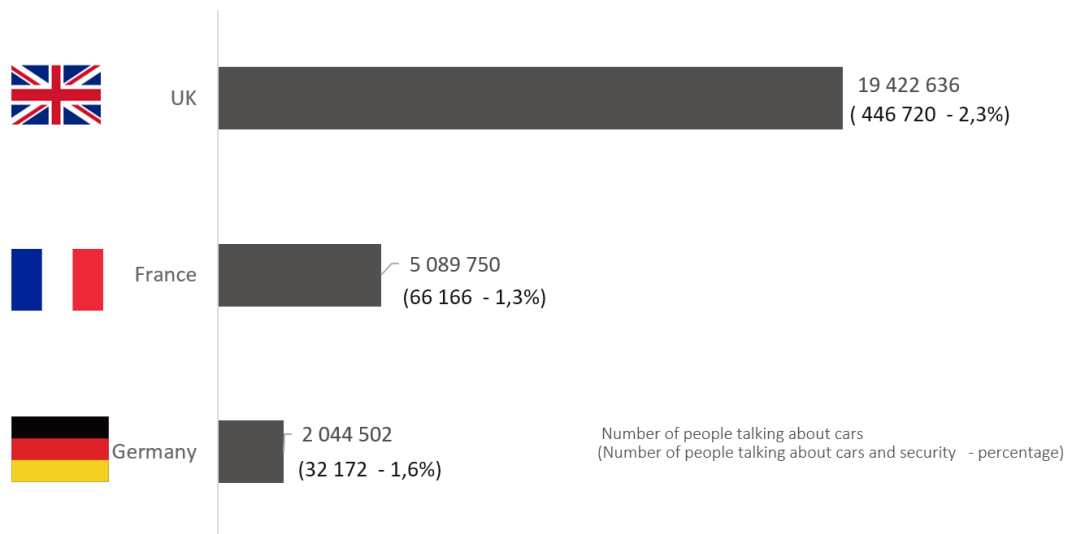


Figure 56: Conversations about Cars and Security

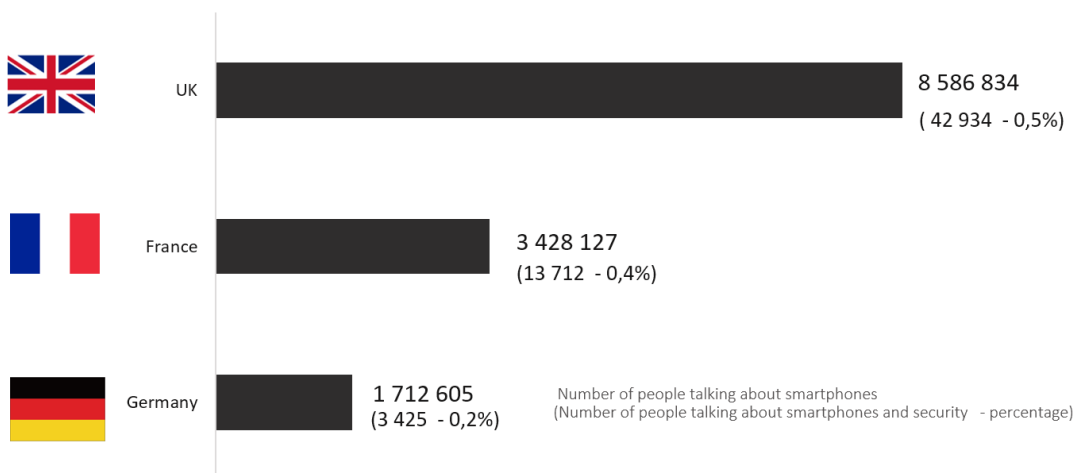


Figure 57: Conversations about Smartphone and Security

<sup>114</sup> Source BBC News : [Keyless cars 'increasingly targeted by thieves using computers'](#)

As expected people discuss more about their cars than their smartphone. Even car security discussions are more frequent by far. Security is the automotive market represents multiple aspects of dependability which combine safety and information security aspects (see 2.3, page 7). As the connected car market segment is nascent and not yet as established, we can hypothesize that it will follow the same trend that the smartphone business.

Also, the security ratio is higher in the car than in the smartphone conversations. The most obvious reason is that people are more concerned about their safety than about the confidentiality of their personal data.

Figure 58 and Figure 59 shows the evolution of security mentions in online conversations for cars and smartphones.

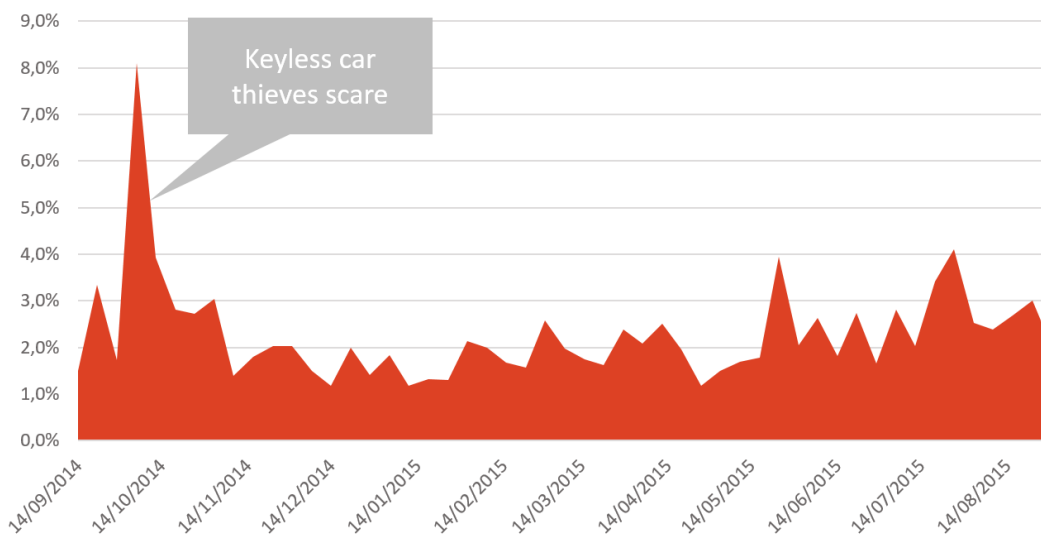


Figure 58: Weekly Evolution of Security Mentions in Online Car Conversations

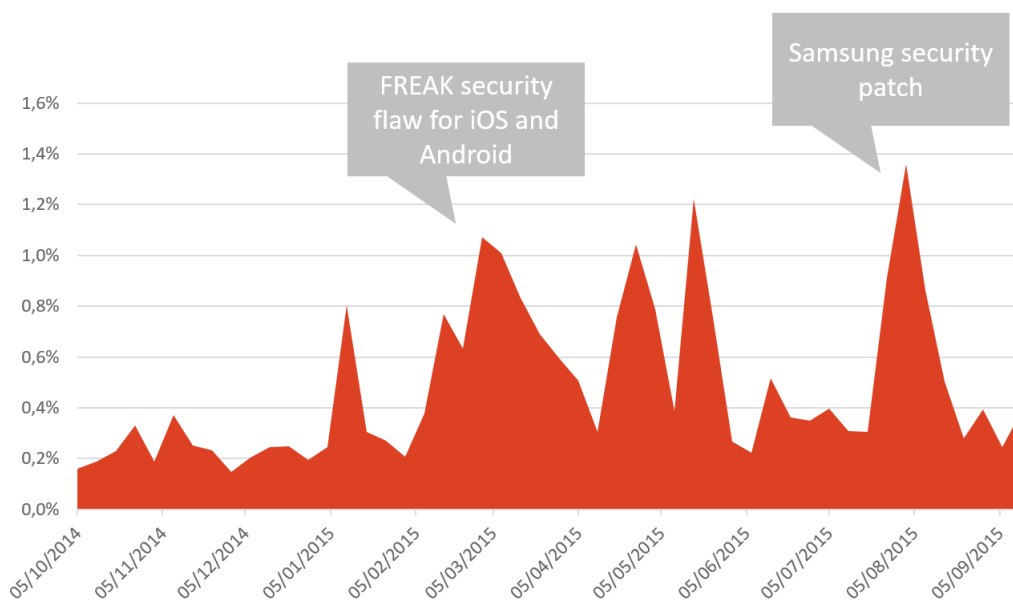


Figure 59: Weekly Evolution of Security Mentions in Online Smartphone Conversations

More precisely, looking at the security awareness in the connected cars, discussions are limited but slowly growing as well as very dependent on industry events such as product announcements or media reports about hacking or security flaws.

## Part IV: Legal Implications

Under the Internet of Things concept, everyday objects connect to the Internet and send and receive data. In 1999, for the first time, the number of “things” connected to the Internet surpassed the number of people. Yet we are still at the beginning of this technology trend. Experts estimate that, as of this year, there will be 25 billion connected devices, and by 2020, 50 billion.

We are entering a world where data is being collected all the time, bringing connected devices into our homes, into what used to be private spheres, and the data that is being generated is increasingly much more sensitive. And security — or the lack of it — will largely determine the success or failure of widespread adoption of internet-connected devices.

In a recent report<sup>115</sup> of the Federal Trade Commission of the United States, the overall recommendations of the FTC staff and industry experts have three prongs:

- Data security: companies should make devices physically secure from the outset),
- Data minimization: companies should not collect more data than they need), and
- Notice and choice: companies should let people choose what data to share, and tell them when a problem arise.

---

<sup>115</sup> [“Internet of Things : Privacy and Security in a connected world”](#) - FTC Staff report – January 2015

## Chapter 12 EURO-MILS and Internet of Things

In the IoT scenario, everything (objects, animals or people) has the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction (see 3.3.4 Internet of Things, page 21).

### 12.1 Internet of Things

Beyond direct consumer applications many businesses, we have seen that even “traditional” or business-to-business companies, are seeking to utilize IoT to improve their operations, capture multitudes of data to feed into “Big Data” analytical engines to gain new insights, and obtain competitive advantages:

- Financial Institutions: engage customers with experiential interactions based on consumption, health, travel and leisure, and transportation data.
- Energy: Providers monitor smart-meter energy usage, allowing them to recommend energy management applications for large buildings, and to pinpoint abnormal high-energy usage as a leading indicator of a forthcoming maintenance issue.
- Healthcare: Companies are leveraging proactive fulfilment by providing replenishing supplies of medicine and medical components before the patient runs out.
- E-Commerce: Retailers benefit from better inventory and fleet management, enjoy more information about warranty and functionality of products, and can offer targeted real-time promotions.
- Manufacturing: Manufacturers and customers alike benefit from new maintenance contracts, where inspections are reduced, and maintenance visits are targeted to specific components reporting problems.

### 12.2 IoT Risks

However, The IoT presents a variety of potential security risks that could be exploited to harm consumers by:

- enabling unauthorized access and misuse of personal information;
- facilitating attacks on other systems;
- creating risks to personal safety.

Security risks are of particular concern to information technology specialists. During the initial rollout of IoT, therefore, securing the devices, applications, and platforms that enable IoT may be an afterthought. IoT platforms are often equivalent in design, allowing hackers to exploit common vulnerabilities of one IoT device platform across different classes of devices. Even after vulnerabilities are discovered, the low cost of the devices may disincentivise IoT producers from issuing security patches.

Privacy risks may flow from the collection of personal information, habits, locations, and physical conditions over time. Companies might use this data to make credit, insurance, and employment decisions.

Safety risks are also important. The IoT, by definition resides in the physical world and is attached to physical objects. These objects, if something goes awry, could cause physical harm or bodily injury. The insulin pump that loses connectivity at night and fails to properly

monitor blood sugar levels and deliver insulin. The connected alarm system that fails to report an intruder because of a glitch. The car that is hacked, causing a fatal accident.

Perceived risks to privacy security, and safety, even if not realized, could undermine the consumer confidence necessary for the technologies to meet their full potential, and may result in less widespread adoption

## 12.3 Legal Issues

The risks posed to security and privacy by hackers being able to access and control devices are becoming increasingly apparent. For example, hacking into smart thermostats could reveal whether or not a family is at home. Web-linked security cameras could be used to spy on residential properties.

However, this is by no means the only issue that has arisen. As the IoT starts to play a greater role in our lives, other legal issues to be aware of will include:

- **Liability:** The more complex and articulated IoT devices and services become, the more parties will have to share liability in case of accidents, malfunctions, defects and related recalls. As people increasingly rely on machines to automate elements of their life, the question will arise as to what happens when the machines get it wrong? Who will be liable?
- **Patents:** The extent to which many parts of the technology required for the IoT are patentable could become an issue. UK and European case law is clear that software and methods of doing business are by and large not patentable. However, computer-implemented inventions that have a technical effect (and fulfil other certain requirements) are potentially patentable.
- **Ownership:** Who owns what when devices interact with each other and collect vast amounts of data?
- **User profiling:** the monitoring of data will increase the opportunity for businesses to profile individuals for various reasons. Under proposed EC law users are likely to be given the right to object to such profiling.

To tackle concerns, the manufacturers of products need to address legal issues at the design and production stages. With the growing number of connected things in people's lives, individuals will have the ability to become more in tune with their own data and interact further with brands and retailers. Businesses will need to establish a trust among consumers and prove that they have addressed these issues before going to market. The IoT has the huge potential for improving lives, saving resources, and lowering costs. However, only time will tell how much personal autonomy and privacy individuals are willing to risk in order to fully reap these benefits.

## 12.4 Potential Answers

So far, there is no dedicated legislation to the internet of things. In the absence of specific legislation, IoT is governed horizontally, by legislation concerning telecoms (the legal terminology refers to "electronic communications"), data privacy and security, intellectual property, safety and environmental, and competition, among others.

There is little doubt that legislation and regulation to support and facilitate the IoT will happen. IoT is a key influencer in the legislative proposals that are going through the European Parliamentary process at the moment for a single telecoms market.

For a long time cyber risk and cyber security were associated in many people's minds largely with the protection of personal data in the context of the hacking of multinationals, banks and



governments and the activities of high profile individuals such as Julian Assange and Edward Snowden.

Government and trade and professional associations have however, been aware for some time that in order to improve cyber security meaningfully, it is essential to engage individuals, SMEs and professional firms, broaden their perception of cyber risk and toughen sanctions for those that have, up until now, failed to address it.

This knowledge and concern is manifested in a number of relatively new and soon to be introduced laws, regulations and cyber standards that will inexorably change this common mindset.

There is more awareness of security issues in the world and more investment in cybersecurity than ever before, as companies and organization realize what is at stake. Some specific sectors expected to need to deal with cybersecurity more intensively are the banking and health sector, and IT as these attacks would have a significant impact on privacy and the protection of personal data.

### **From European Directives to National Laws**

A wide variety of Community measures in the field of safety and security have been adopted. European directives are legally binding and have to be transposed into national laws by Member States. They set out minimum requirements and fundamental principles, such as the principle of prevention and risk assessment.

Guidelines are non-binding documents that aim to facilitate the implementation of European directives. There are different types of guidelines, such as practical guidelines from the European Commission setting out best practice for the prevention of risks, Council Recommendations, European Commission Communications, EU social partners agreements, and others.

A 'harmonized standard' is a standard adopted by one of the European standardization organizations – European Committee for Standardization (CEN), European Committee for Electrotechnical Standardization (CENELEC) and European Telecommunications Standards Institute (ETSI) – following a request from the European Commission.

European directives set out the minimum standards for safety and health in the workplace. The EU directives are implemented through the national legislation of Member States. They may adopt stricter rules to protect people but their legislation must comply with the minimum standards. As a result, national safety and information security legislation varies across Europe.

### **European wide initiative**

The most well-known of these new measures are perhaps the draft EU Data Protection Regulations which are before the EU Parliament. The European Commission has published a cyber-security strategy together with proposed directive on network and information security through which it aims to force operators of critical infrastructures in some sectors (financial services, transport, energy, health), enablers of information society services (notably: app stores, e-commerce platforms, internet payment companies, cloud computing, search engines and social networks) and public administrations to adopt risk management practices and report major security incidents on their core services.

## **12.5 EURO-MILS Platform Ready for a Safe and Secure IoT**

There are many benefits of designing security into devices and systems using MILS technology.

MILS-based platforms provide applications from different domains, or at different security levels, to securely share the same hardware platform, enabling cost reductions through reduced size, weight, and power requirements. MILS architecture simplifies design of high assurance system

Using the EURO-MILS platform, customers can build security into their devices and systems, many of which will become part of the IoT. Some of these security-critical devices and systems will be used to secure national critical infrastructure.

The comprehensive, security evaluation evidence package of documentation and artifacts can be used by a manufacturer as their security-critical system undergoes a security evaluation. Once the system achieves its certification or authorization to operate, it can be deployed for the end users.

Official certification should also provide some new means for industrial manufacturers and service suppliers to protect themselves against suits or class actions from consumers. Having gone through the certification process means that the industrial manufacturer has based the development of its product using state of the art security techniques. For example, using the architecture framework as proposed by EURO-MILS project would be a definitive benefit for that matter.

Using a EURO-MILS-based platform implies also that the manufacturer or service provider implements best practices in its development organization in terms of security.

## Part V: Conclusion

This work package has been designed to analyse the business, social, and legal values of the EURO-MILS platform. The EURO-MILS platform has three principal value propositions:

- Virtualisation and Partitioning,  
The platform uses virtualization and partitioning to improve resources utilisation in the embedded device
- Security and Safety,  
The platform provides a high level of information security to protect its constituents from unauthorized access, use, disclosure, disruption, modification, or destruction
- Certification and User acceptance.  
The platform has been evaluated to provide confidence to industries, authorities and consumers that it can fulfil their security needs.

The EURO-MILS demonstrated its ability to be used in all type of markets from the most critical to the largest ones. Figure summarizes the EURO-MILS values as explained by our Industry panel and analysed with our consumer studies. It covers the whole spectrum from regulated or industrial (avionics, automotive, ICS, Healthcare...) markets to consumer (home automation, smart meter, mobile...) mass markets, from one year lifetime devices to systems that will be still in use in 50+ years.

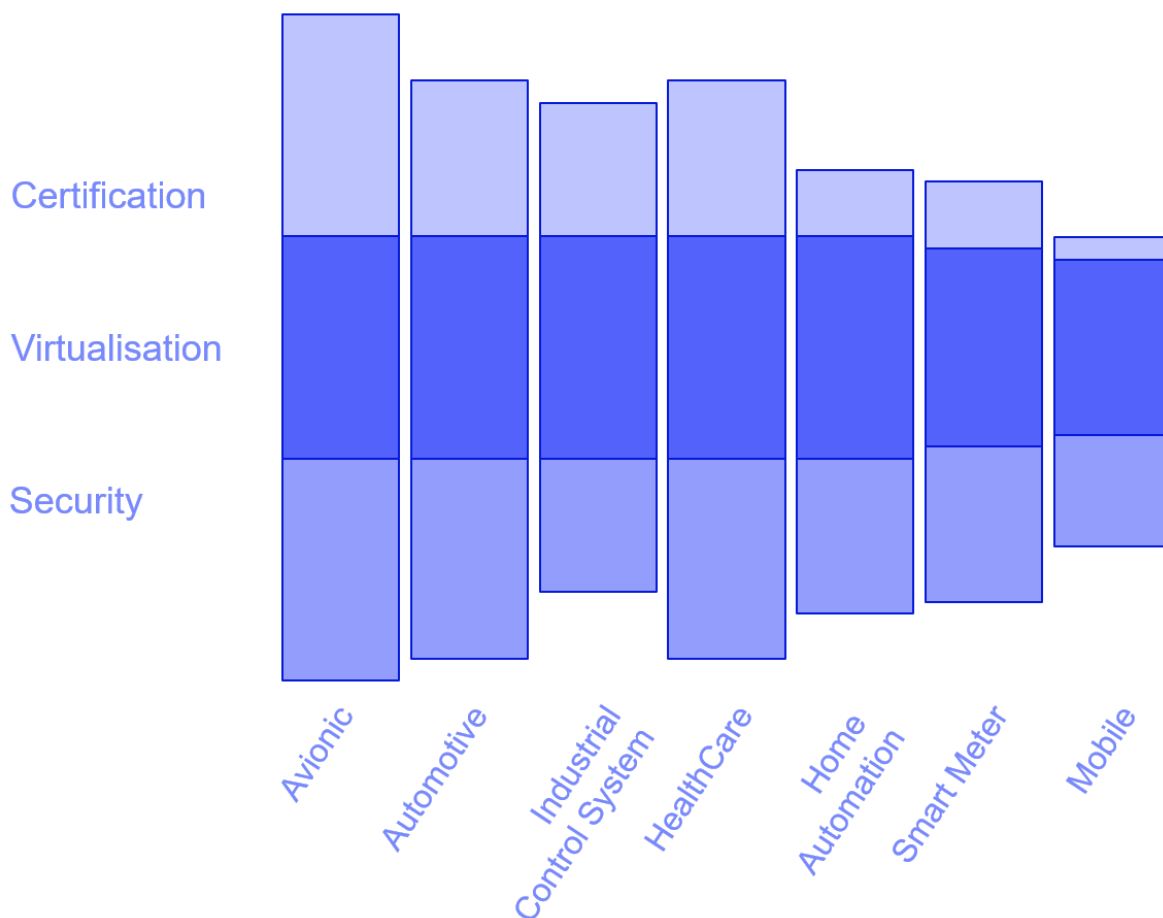


Figure 60: EURO-MILS Values by Market Segment

## **Business**

Avionics is our reference. The avionic industry requires EURO-MILS embedded platforms. Virtualization provides significant benefits to embedded systems with regard to enabling mixed real-time and guest operating system interoperability, legacy code migration, and hardware consolidation. The platform provides a high level of information security especially for a data integrity perspective to help improving the aircraft safety. Finally, security certification is mandatory as requested by the authorities.

The automotive industry benefits from avionic experiences. Automotive virtualization requirements are identical as the avionics ones. An average car is today shipped with 80+ ECUs connected via multiple networks and requires a multi-layered runtime environment. Security becomes mandatory because of open systems integrations (Infotainment and automotive applications) to segregate different vehicle domains. And there are meaningful use-cases that should be verified via a certification process.

At the other side of the markets, the mobile industry values virtualization and it becomes the norm for the newest smartphones. Virtualization is providing some interesting BYOD options for the enterprise. Security is key for enterprise and consumers but not as such requested by consumers which insist on personal data protection. Layered security components help to maintain the integrity of software components, strengthening system protection and safeguarding corporate data without compromising security or sacrificing performance. Official certification is not required by consumers but start to be a standard in a number of large enterprises and governmental organizations.

## **Social**

Our researches have prepared the Go-To-Market strategies when a EURO-MILS product will be launched. It revealed that most of the features are expected directly or indirectly by consumers. They don't understand information security but do care a lot about personal data, are aware and discuss about hackers, thieves, etc. Also, it has been a first-of-a-kind set of surveys and analysis performed in the context of a European research project preparing the move from a system prototype demonstration in operational environment to a manufactured system ready to be launched in the field.

## **Legal**

We worked on implications and issues of the new paradigm presented by the Internet of Things. In this context, the EURO-MILS platform and its security evaluation can have unique capacities in assuring users for its security and safety capabilities.