Safety and Security in a Smart Production Environment

Reinhard Kloibhofer[1], Erwin Kristen[1], Stefan Jakšić[1]

[1] AIT Austrian Institute of Technology GmbH, Giefinggasse 4, 1210 Vienna, Austria
reinhard.kloibhofer@ait.ac.at, erwin.kristen@ait.ac.at,
stefan.jaksic@ait.ac.at

Abstract.
Industry 4.0 is the term which designates an engineering philosophy of a modern, automated manufacturing technology. It includes tight cooperation of robots and humans and a seamless integration of the Information Technology (IT) and the Operation Technology (OT). Wired or wireless interconnection of devices and machinery across the existing manufacturing components plant borders. A data driven product life cycle starts with product concept ideas, and proceeds with the design, production and testing, commercialization and to end with the decommissioning of the product. Industry 4.0 also defines the smart factory where a smart product guides the production process and issues commands to the machinery about the necessary steps to take to produce the desired product. This paper contains the idea and a solution for a smart factory with a mobile robot, operating with secured product configuration and secured data communication. All production data is stored as a digital copy, named "digital twin".

Keywords: Industry 4.0, Industrial Automation Control Systems (IACS) Internet of Things (IoT), Cyber-Physical Systems (CPS), Safety & Security.

1 Introduction

A main focus of the ongoing international research project IoSense are safety and security (S&S) aspects of an industrial automation control system (IACS). Not only the requirements for today's modern manufacturing plants are under consideration, but also the challenges for S&S in future IACS. In the future, humans and robots will operate in the same working environment which raises new S&S concerns which must be analysed and assessed. The situation gets even more complex with each product becoming an intelligent product with a documented life cycle in form of a so called "digital twin", stored somewhere in the cloud. Security threats are critical more than ever in a strong interconnected world and both human health and production output are vulnerable in the same extent.

In Chapter 2 we provide a brief overview of modern production systems. We proceed with a definition of operation environment of a robot operated production field in Chapter 3. We build such environment as a demonstrator for Trustworthy Systems (TrustworSys) in the project IoSense, and document it in detail. Chapter 4 introduces the IEC

The final publication is available at Springer via
https://link.springer.com/book/10.1007%2F978-3-319-99229-7

62443 industrial security standard and deploys this standard to a part of the demonstrator. Chapter 5 gives an outlook of planned additional future work and a project assessment about safety in the industrial domain.

2 Modern Production State the Art

Industry 4.0 is the synonym for an engineering philosophy for a modern, automated manufacturing technology. The industrial production will be merged intensively with Information and Communication Technology. The base therefore are intelligent and digital networking systems. The production and process is more and more self-organizing, implying there is no engineer to plan each step in detail, but the plant is responsible for organizing the sequences of the production and consequently the use of the production machines and the production resources. Necessary ingredient for such a process is a highly automated facility with assistance from robots and gripper arms to transport the product. But more than only the production, the whole value-added chain should be optimized. All phases of the product circle are under consideration. This begins with the plan of raw material, development of products, production, utilization, service and at the end of the product circle, the decommission of the product.

The Number 4.0 is an expression of the 4th industrial revolution, which will come after the first (mechanization, water and steam power), the second (mass production, assembly lines, electrical current) and the third (computer support and automatization) revolution. The last generation include cyber-physical systems (CPS), Internet of things (IoT), cloud computing and cognitive systems.

Four design principles support the implementing of Industry 4.0:

- Interoperability: all components like machines, devices, sensors and people are connected and communicating with each other.
- Information transparency: a virtual (digital) copy of the plant is enlarged with sensor data. This means the raw sensor data must be integrated in high level systems.
- Technical assistance: the machines and the interfaces should be understandable to enable the technical support provided by humans.
- Decentralized decisions: most of the decisions should be done by the cyber physical systems itself. In case of exceptions, the decision is delegated to a higher level.

The components of a smart production environment will be more tightly connected one to the other. The complexity of such a system is increasing. A main goal is the communication and data exchange between these components. Many different wired and wireless communication channels are possible for communication. Today, these networks are typically placed in one factory, but in the future also more and more factories will be connected to form a world-wide production plant mesh. However, the data must be secured from malicious manipulation. Therefore, the security of such a network and the interfaces is crucial. Strengthening the system against cyber-attacks is still a very active research topic.

3 Demonstrator for Innovative Manufacturing

In the EU ECSEL (Electronic Components and Systems for European Leadership) project IoSense the focus of the project is to improve the Time-to-Market (TTM) period for sensor-based products and increase the market share with an early market launch. Several demonstrators are planned to demonstrate technologies to fulfill this goal. TrustworSys is one of the demonstrator developed in the project and shall be explained in more detail in this paper.

In the TrustworSys demonstrator we plan the demonstration of an innovative configuration of smart products and their production in a modern factory. A focus will be set to the safety and security process from a product being conceived until its being recycled for decommissioning.

There exist different approaches for configuration management of embedded systems. A direct approach is static configuration by using wire Jumpers or zero-ohm resistors directly on the Printed circuit board (PCB). A more flexible configuration can be done by deploying simple hardware elements (e.g. pluggable Jumpers, DIP-Switches), non-volatile memory (e.g. battery powered SRAM, EEPROM, Flash) contact based command line interfaces (e.g., RS232, USB), remote shells, or even web interfaces (HTTP). However, all these operations need a manual handling and are not simple to use in fully automated processes.

In this demonstrator we use contactless NFC (Near Field Communication) for the wireless configuration of the product in the production process. This technology is well applicable for an automated production line. In an automated factory the (raw) product will be transported by a conveyor belt or more flexible by (autonomous) robots. In our use case the factory layout is flexible, meaning that the production machines i.e. CNC (Computerized Numerical Control) can be replaced or the position of machines can be changed. We do not assume a fixed and inflexible floor plan of the factory. In other words, production process is not static in any aspect. In our approach the raw product is configured the first time and for the production the raw product guides the robot and the machines through the different production steps.

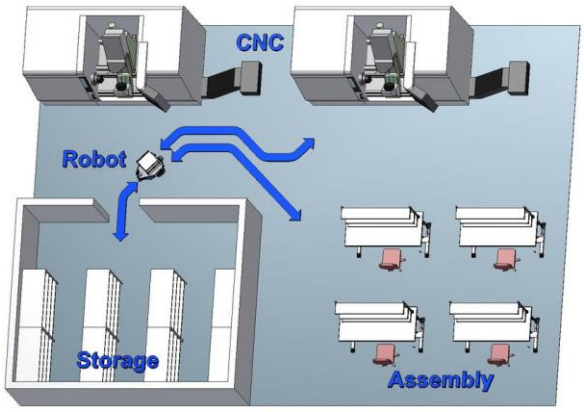

Fig. 1. Example of a Manufactory floor plan.

In Fig. 1 a typical floor plan for a manufactory area is show. A robot transports a product from storage to different production machines or to a manual production work benches for assembly. After the production phase, the product instructs the robot to bring it back to storage. The product is now ready to be sold to the consumer.

3.1 Demonstrator Setup for the Demonstration

To demonstrate this new configuration and production approach a set-up in the laboratory will be designed. One central component in this setup is a robot that can navigate autonomous through the factory.

We plan a demonstrator area of about 2 x 2 meters (which can be enlarged to a real-scale factory size) where all components are placed. For our demonstration we plan 3 different production machines (PM1, PM2 and PM3) and a storage (STO). These components are placed on the side of the area. In the whole area a mobile robot (ROB) transports a product (PROD) from the storage to the different machines and at the end of manufacturing back to the storage. The robot can navigate on the area and can also detect obstacles and drive around them.

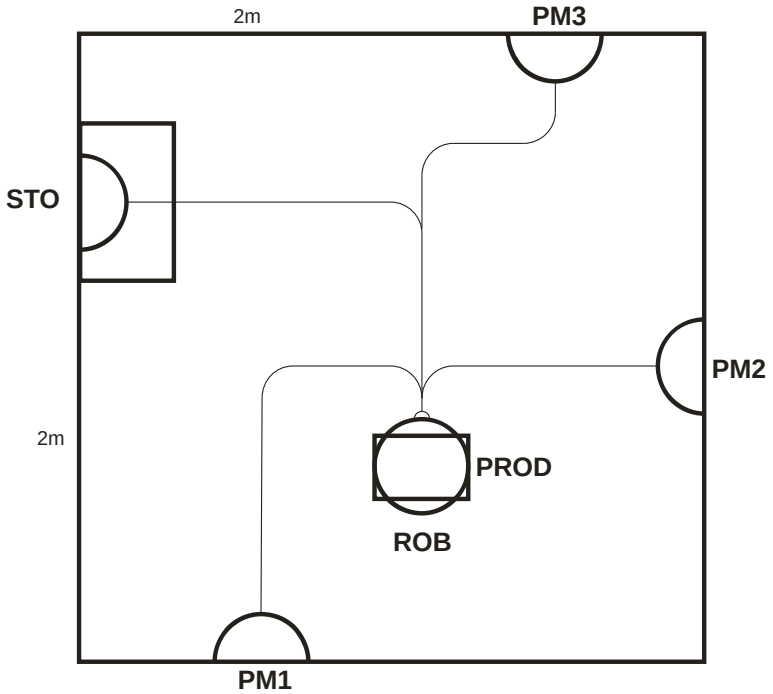

Fig. 2. Demonstrator floor plan:

- STO: Storage
- PMx: Production machinery
- ROB: Robot
- PROD: Product

3.2 Smart Product

Smart products are products that can communicate with the machines, equipment and other systems. They are equipped with embedded systems that can collect, communicate and elaborate data. Similar to configuring of microprocessors and embedded systems, it is possible to store configuration data on the component that speeds up the configuration steps.

Very common types of smart products are (electronic) sensors (e.g. Fig. 3) that communicate in a sensor network or with a high-level machine. In our view not only electronic components are considered as smart products, but also more or less complex mechanical components like a screw (Fig. 4) or an entire car gear box. Passive RFID components have a very low price in mass production.

Fig. 3. Smart temperature sensor
© Xiaomi Mi, Source: Amazon.

Fig. 4. Screw with RFID
© Source: Wikipedia.

3.3 Intelligent Robot Platform

The transport of components between different production machines is one of the most important action of a production cycle in a factory. In a simple and less flexible production sites conveyor belts are used. Other transport environments could be vehicles on rails. In modern factories more and more robots will be used for transportation. The first generation of robots in factories was navigating through the factory using dedicated tracks or lines on the floor. In later iterations, sensors positioned in the robot's environment or under the floor are used to guide the robots.

Modern transport robots are more intelligent than ever and can navigate with different sensors autonomously through the factory. Therefore, an accurate indoor navigation, obstacle recognition and collision avoidance systems are necessary.

In our demonstrator we use a generic robot platform with two motorized wheels. This generic platform can move in all directions and rotate left and right.

A de-facto standard, ROS (Robot Operation System) is used to program and control the robot platform. ROS is a robotic middleware, a software framework for robotic control software development. The programming language used is C++ or Python. A ROS application include a master coordination node and different other nodes, e.g. driving platform, sensor nodes, odometry nodes, navigation node. The nodes are communicating via topics. Nodes can publish to topics and they can subscribe to topics for receiving data. The structure is very flexible and allows simple adding more sensors or actuators.

For the TrustworSys demonstrator a new NFC node will be developed and added to the robot system.

3.4 NFC Communication

A key component in our configuration and production approach is a secure NFC wireless communication [1], [2], [3], [4], [5] which is developed by our partner Infineon Austria.

The block diagram for the NFC Enhancement is shown in Fig. 5.

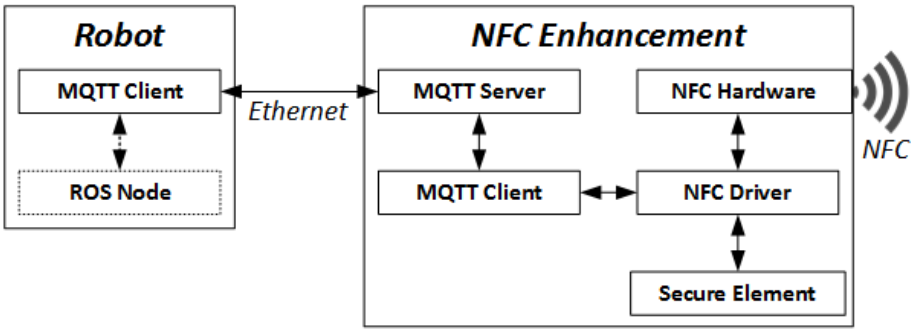

Fig. 5. NFC Enhancement block diagram

The NFC Enhancement is composed of different blocks. One is the NFC Hardware with the antenna for the wireless communication to another NFC device. It must be distinguished between an active and a passive NFC device. An active NFC device needs a power supply and generates an electromagnetic field with the antenna. If there is a passive NFC device in the communication range it will receive power from the electromagnetic field and powers a NFC electronic chip. This passive NFC component will modulate the electromagnetic field and this modulation will be detected from the active NFC device. Such communication with typical small antennas will only work for a few millimeters up to a few centimeters range. This is an important feature against malicious manipulation and therefore an important security aspect.

A second security aspect is the secure element on the NFC chip. This new developed secure element allows an encrypted communication between the passive NFC and the reader. As the secure element is on the same chip it cannot be manipulated without destroying the integrated circuit.

An additional feature is the Message Queue Telemetry Transport (MQTT) server-client approach. It is an ISO standard for a publish-subscribe-based messaging protocol. It works on top of the TCP/IP protocol. It is an extremely simple and lightweight messaging protocol, designed for constrained devices and low-bandwidth, high-latency or unreliable networks. The design principles are to minimize network bandwidth and device resource requirements whilst also attempting to ensure reliability and some degree of assurance of delivery. The publish-subscribe messaging pattern requires a message broker, which is a computer program module that translates the message format from a

device (e.g. sensor) to the message format to the receiver (e.g. computer). MQTT can be used for sending and receiving encrypted data and therefore it is very good solution.

The connection of the NFC Enhancement to the robot platform is established via Ethernet cable and it is integrated as a ROS software node with the robot.

In our demonstrator we are using several NFC components:

- Active NFC on the robot
- Passive (or active) NFC on the product
- Passive (or active) NFC on the production machines and storage
- Active NFC on a hand-held configuration device

3.5 Storyboard for Smart Manufacturing

The steps from a product idea to the final product has many production steps and each step takes time. A time and cost-optimal planning of the steps is a necessary condition to achieve a market success.

First Step: Product Definition

On a Backend Host or Product Server the definition and configuration for the new product is stored. This includes also the components, the production steps, the ID-numbers and the number of products which should be produced for the actual production batch.

We demonstrate this for a smart sensor with different alarm levels. The smart sensor is built with the following components:

- Analog to Digital Converter board, including a NFC
- The sensing element (e.g. temperature sensor or humidity sensor)
- Housing

Second Step: Raw Product Configuration

An Operator with a mobile configuration device which is connected to the Backend Server configures the raw product from the storage.

We distinguish between Trusted Operator and an Untrusted Operator:

- A Trusted Operator has access to the configuration device and can modify some parameter of the smart sensor (e.g. measurement range, resolution, color of the housing). The configuration data is programmed via NFC to the product. Serial Number or other ID numbers are generated automatically and all data which are transferred to the raw product are also stored on the Backend Server.
- An Untrusted Operator has no access to the configuration data. He can only transfer the configuration to the raw product without manipulation.

Third Step: Production Start

After the configuration of the raw product it will be set on the mobile robot by a robot arm (or in a simple form the operator puts the device on the robot). The raw product communicates now via NFC to the robot and instruct the robot for the first production action.

Product Processing Loop

In this phase several steps of the production loop are performed:

- The robot communicates with the Backend Host via WLAN to ask for the coordinates of the first production machine. The robot drives autonomous to the production machine.
- The robot communicates via NFC to the machine what action should be done on the product. The production machine acts according the configuration
- Production machine confirms that the work is done on the product
- Robot communicate with product for the next action

Production Finished

After all production steps are completed, the robot returns the product to the storage. The new smart Product is ready to be released for commercial use. The customer product life cycle can start.

3.6 Backend Host

The Backend Host is part of the factory IT-environment. It is assumed that the stored data is safe (periodic backup, …). This server keeps both the product data and the entire factory configuration. This means the Backend Host knows the status of all machines, storage and robots. Every step of the production is also stored. In other words, the Backend Host holds a so called "digital twin" of the products. The digital representation provides both the elements and the dynamics of how the product was produced. Furthermore, also the customization process can be stored on the Backend Host.

An additional important task of the Backend Host is the optimization of the factory. For example, the paths of the robot movements can be optimized by self-learning algorithms.

4 Security Considerations

4.1 IEC 62443 Security Standard

In the industrial sector for products and facilities the IEC 62433 security standard becomes the base for security requirements definitions and security recommendations. The standard series is divided in 14 sub-documents, which are sorted in four main groups,

- **General** – This group includes standard introduction, technical reports, glossary, life cycle definition, and other basic documents.
- **Policies and Procedures** – This group provides documents which focuses on the policies and procedures associated with industrial automation security
- **System Requirements** – This group lists requirements for the system level.
- **Components Requirements** – This group lists requirements for the components level.

The safety standard IEC 62443 postulate a workflow shown in Fig. 6.The workflow is combined of four ZCR's (Zone and Conduit Requirements) phases.

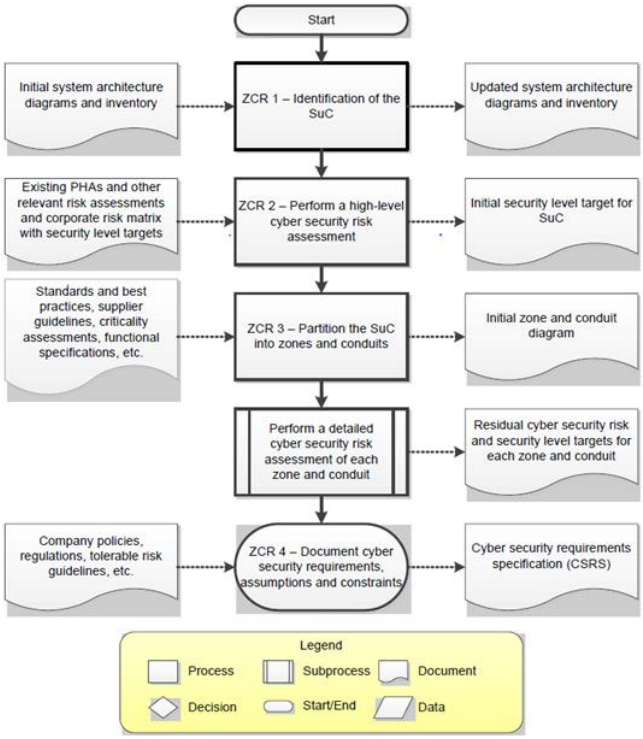

Fig. 6. IEC 62443 Workflow to establish zones and conduits and assess risk [5]

On the right-hand side the recommended documents and on the left-hand side the outputted documents are listed. First, in the ZCR1 phase, the System under Consideration (SuC) must be defined by a detailed description of the system architecture and the inventory. With the input of a Process hazard analysis (PHA) a high-level cyber security risk assessment deter-mines the target security level (ZCR2). The target security level (Security Level – Target SL-T) stated out the required estimated security level to operate the system in the documented environment.

In general, the security level defines the strength of the security measures, needed to safeguard the system for cyber-attacks.

The five levels are defined as:

SL 0	No protection
SL 1	Protection against casual or coincidental violation
SL 2	Protection against intentional violation using simple means with low resources, generic skills and low motivation
SL 3	Protection against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation
SL 4	Protection against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation

The standard provides methods and hints to estimate the suitable security level derived by zone security parameters.

The next step (ZCR 3) in the workflow is to split up the complex overall system in zones and conduits. See Fig. 7 as an example of a possible SuC partitioning in zones and conduits.

In final step (ZCR 4) a detailed cyber risk assessment for each zone and conduit is performed to estimate the individual target security levels.

The last step is the definition of necessary requirements for security countermeasures to harden the system against all analyzed and assessed cyber threats. The component supplier defines the feasible and cost-optimal archived Security Level (SL-A) for each components of a zone.

In the end of the integration and commissioning phase the system integrator must ensure that all the security measures implemented for the Archived Security Level (SL-A) are efficient, suitable and match the Target Security Levels (SL-T). This reports the final possible Capability Security Level (SL-C) of the system [6].

4.2 Zones and Conduits

The TrustworSys demonstrator has the following zones and conduits figured out in the following Fig. 7.

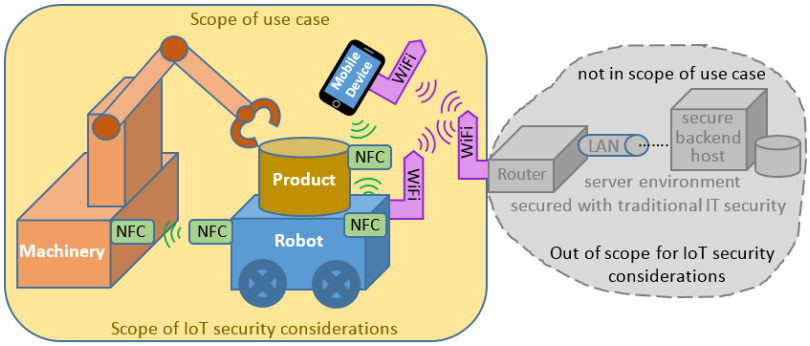

Fig. 7. Demonstrator zones and conduits definition overview

The zones of the system are:

- Robot
- Product
- Machinery
- Mobile configuration device

And the identified conduits are:

- NFC communication (between different devices)
- WiFi communication

A detailed cyber security risk analysis of the different zones and conduits was performed. The main result of this analysis is that by using the secure element in the NFC communication we have protection against attack to sensitive data and to the software. The robot never gets sensitive data from the product, but only encrypted data. The data communication between robot and Backend Host is also encrypted by the secure element of the NFC device. In this case the robot can be considered as an untrusted component. A malicious attacker who is manipulating the robot cannot read sensitive data from the product.

5 Outlook

The demonstrator allows to present smart production functionalities, like as setup different product variants on the same production environment. These operations are performed with considerable data security measures to prevent possible production flow manipulation from outside cyber-attacks. There also manipulations from inner-side attacks which are feasible. For such cases, risk analysis and countermeasures must be implemented. In future work a continuous monitoring of the robot operation parameters

shall be implemented, a further improvement for preventative maintenance (PM). Monitoring can be also used for anomaly detection and as additional security measure, to prevent manual manipulations of the robot platform.

Acknowledgment. This work has received funding from the IoSense project, under grant agreement No 692480. The project is co-funded by grants from Austria, Germany, Spain, Netherland, Belgium, Slovakia and ECSEL JU.

References

1. T. Ulz, T. Pieber, A. Höller, S. Haas and C. Steger, "Secured and Easy-to-Use NFC-Based Device Configuration for the Internet of Things," in IEEE Journal of Radio Frequency Identification, vol. 1, no. 1, pp. 75-84, March 2017.
2. T. Ulz, T. Pieber, C. Steger, C. Lesjak, H. Bock, R. Matischek, "SECURECONFIG: NFC and QR-Code based Hybrid Approach for Smart Sensor Configuration", 2017 IEEE International Conference on RFID (RFID), pp. 1-6.
3. S. Haas, A. Wallner, R. Toegl, T. Ulz and C. Steger, "A Secured Offline Authentication Approach for Industrial Mobile Robots", 13th IEEE Conference on Automation Science and Engineering (CASE) Xi'an, China, August 20-23, 2017.
4. T. Pieber, T. Ulz, C. Steger, and R. Matischek, „Hardware Secured, Password-based Authentication for Smart Sensors for the Industrial Internet of Things", International Conference on Network and System Security 2017, pp. 632-642.
5. ISA-62443-3-2 Security for industrial automation and control systems (IACS), Security Risk Assessment, System Partitioning and Security Levels, Draft 7, Edit 1, 2017 / page 13.
6. P.Kobes, "Protection Levels, an holistic approach based on IEC 62443", VDE Tagung Funktionale Sicherheit und IT-Sicherheit 2017.