
# IoT4CPS – Trustworthy IoT for CPS

**FFG - ICT of the Future**

**Project No. 863129**

# Deliverable D7.4
# Test-beds and guidelines for securing IoT products and for secure set-up production environments

**The IoT4CPS Consortium:**
AIT – Austrian Institute of Technology GmbH
AVL – AVL List GmbH
DUK – Donau-Universität Krems
IFAT – Infineon Technologies Austria AG
JKU – JK Universität Linz / Institute for Pervasive Computing
JR – Joanneum Research Forschungsgesellschaft mbH
NOKIA – Nokia Solutions and Networks Österreich GmbH
NXP – NXP Semiconductors Austria GmbH
SBA – SBA Research GmbH
SRFG – Salzburg Research Forschungsgesellschaft
SCCH – Software Competence Center Hagenberg GmbH
SAGÖ – Siemens AG Österreich
TTTech – TTTech Computertechnik AG
IAIK – TU Graz / Institute for Applied Information Processing and Communications
ITI – TU Graz / Institute for Technical Informatics
TUW – TU Wien / Institute of Computer Engineering
XNET – X-Net Services GmbH



*For more information on this document or the IoT4CPS project, please contact:*
Mario Drobics, AIT Austrian Institute of Technology, mario.drobics@ait.ac.at

**Document Control**

**Title:** Test-beds and guidelines for securing IoT products and for secure set-up production environments
**Type:** Public
**Editor(s):** Katharina Kloiber
**E-mail:** kk@x-net.at
**Author(s):** Katharina Kloiber, Nikolaus Dürk, Silvio Stern
**Reviewer(s):** Stephanie von Rüden, Violeta Damjanovic, Leo Happ-Botler
**Doc ID:** D7.4

## Amendment History

| Version | Date | Author | Description/Comments |
|---|---|---|---|
| V0.1 | 13.01.2020 | Silvio Stern | Technology Analysis |
| V0.2 | 10.03.2020 | Silvio Stern | Possible Research Fields for the SBI-System |
| V0.3 | 31.08.2020 | Katharina Kloiber | Initial version prepared |
| V0.4 | 08.09.2020 | Katharina Kloiber | State-of-the-Art |
| V0.5 | 22.09.2020 | Nikolaus Dürk, Katharina Kloiber | Test-beds |
| V0.6 | 07.10.2020 | Nikolaus Dürk, Katharina Kloiber | Guidelines and Structure |
| V0.7 | 15.10.2020 | Stephanie von Rüden, Katharina Kloiber | Internal review |
| V1.0 | 26.11.2020 | Katharina Kloiber | Correction and final Version |
| | | | |
| | | | |



The IoT4CPS project is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.

Federal Ministry
Republic of Austria
Transport, Innovation
and Technology

FFG
Forschung wirkt.

# Contents

## List of Figures

# List of Tables

## Abbreviations

| | |
|---|---|
| AES | **A**dvanced **E**ncryption **S**tandard |
| API | **A**pplication **P**rogramming **I**nterface |
| CLAT | **C**ustomer-side trans**LAT**or |
| CPS | **C**yber-**P**hysical-**S**ystems |
| CRM | **C**ustomer **R**elationship **M**anagement |
| DES | **D**ata **E**ncryption **S**tandard |
| DVI | **D**igital **V**isual **I**nterface |
| ERP | **E**nterprise **R**esource **P**lanning |
| FPGA | **F**ield **P**rogrammable **G**ate **A**rray |
| GDPR | **G**eneral **D**ata **P**rotection **R**egulation |
| GUI | **G**raphical **U**ser **I**nterface |
| GW | **G**ate**w**ay |
| ICMP | **I**nternet **C**ontrol **M**essage **P**rotocol |
| IDS | **I**ntrusion **D**etection **S**ystem |
| IEC | **I**nternational **E**lectrotechnical **C**ommission |
| IoT | **I**nternet **o**f **T**hings |
| IPv4 | **I**nternet **P**rotocol **v**ersion **4** |
| IPv6 | **I**nternet **P**rotocol **v**ersion **6** |
| IPS | **I**ntrusion **P**revention **S**ystem |
| JSON | **J**ava**S**cript **O**bject **N**otation |
| LAN | **L**ocal **A**rea **N**etwork |
| LED | **L**ight-**E**mitting **D**iode |
| LTS | **L**ong **T**erm **S**upport |
| M2M | **M**achine-**to**-**M**achine |
| MQTT | **M**essage **Q**ueuing **T**elemetry **T**ransport |
| NAT | **N**etwork **A**ddress **T**ranslation |
| NFS | **N**etwork **F**ile **S**ystem |
| OSPF | **O**pen **S**hortest **P**ath **F**irst |
| PCI | **P**eripheral **C**omponent **I**nterconnect |
| RDP | **R**emote **D**esktop **P**rotocol |
| REST | **RE**presentational **S**tate **T**ransfer |
| RFC | **R**equests **F**or **C**omments |
| SBI | **S**ecurity **B**y **I**solation |
| SFTP | **S**ecure **F**ile **T**ransfer **P**rotocol |
| SME | **S**mall and **M**edium-sized **E**nterprise |
| SIIT | **S**tateless **I**P/**I**CMP **T**ranslation |
| SSD | **S**olid **S**tate **D**isk |
| SSH | **S**ecure **SH**ell |
| TCP | **T**ransmission **C**ontrol **P**rotocol |
| UDP | **U**ser **D**atagram **P**rotocol |
| USB | **U**niversal **S**erial **B**us |
| VGA | **V**ideo **G**raphics **A**rray |
| VNC | **V**irtual **N**etwork **C**omputing |
| VPN | **V**irtual **P**rivate **N**etwork |

**Executive Summary**

Digitalization is confronting companies and especially small and medium enterprises (SME) with an ongoing change in their environment. The use of digital technologies has a direct impact on business processes, products and services and customer behaviour. But it also changes business models, employment and forms of employment, shifts value chains, increases the use of flexible working conditions, facilitates flatter corporate structures and intensifies global competition.

The challenge is that digitalization over the entire product life cycle accelerates the development, validation, instrumentation and deployment of complex industrial products while increasing product quality. The digitalization and increasing connectivity of (critical) cyber-physical objects enables the development of new applications but also leads to new safety and security related requirements in design, testing, production and operation of these systems as IoT devices are always in focus of attacks.

Production companies cannot only invest in security once, they have to consider security continuously in production environments, in development of new products and during all life cycle processes. They have to define internal resources and structures as well as (external) experts to constantly work on their security strategies.

This deliverable presents approaches and solutions for secure set-up production environments and to secure IoT products. It provides the results of the research done in work package 7, task 7.4 and especially the results which were received within the development and validation of test-beds to demonstrate Industry 4.0 use cases.

# 1. Introduction

## 1.1. Motivation

Our motivation in the project IoT4CPS is to research some of the major challenges and business cases for future industry to taking place in Europe. Here, our particular interests relate to Cybersecurity and safety conditions of the Internet of Things (IoT) for Cyber Physical Systems (CPS). The focus of our research was to develop the basis for continuous processes in form of tools that reach a high degree of reuse between different environments (e.g. in-vehicle instrumentation, test-beds) while taking into account physical and energy constraints, heterogeneity of data sources and throughputs, computing power and targeted user groups. The decision for open source as basis for security was obvious as the sharing and exchange of knowledge and methods to reach customized security solutions is the most promising way into a secure future. Details for this decision are explained in section 5.

Production companies are currently facing enormous challenges in the area of IT security. Manufacturers are forced to protect themselves from external attacks towards their production operations. At the same time they have to open their environment and closely work together with suppliers and customers. Further on their products require remote maintenance, updates and upgrades until end of life (life cycle management). Sub-suppliers of production systems and/or of components need secure access to their products in order to maintain their services and uphold quality standards. Data transfers are necessary as data source and the place of production and assembling differ.

The increasing globalization of production and external conditions (e.g. Covid-19 restrictions, climate protection measures) complicate on-site service. The worldwide shut-downs in 2020 taught us to decentrally communicate in new dimension but also that new structures and strategies for globally distributed (production) networks are needed. Our aim is to give European SME a guideline for a secure set-up of production environments, to secure IoT products. It is important to raise the awareness of IT security risks and to visualize available solutions. IoT4CPS targets ways and solutions that help SME with their IT-security and provides tools, methods and guidelines to enable safe and secure IoT-based applications for smart production.

### 1.2. Market figures

SMEx cover a wide range of activities and are a decisive factor for the economy. Over 99% of European companies were SMEs in 2019 and about two-thirds of employees currently work in SME[1]. Although the 2019 European Union survey on 'ICT usage and e-commerce in enterprises' points out an high awareness towards IT security and necessary measures (in 2019, 93% of EU enterprises with 10 or more persons employed used at least one ICT security measure, control or procedure in order to ensure integrity, authenticity, availability and confidentiality of data and ICT systems), one in eight enterprises (12%) at least once experienced problems due to ICT related security incidents. Overall, large enterprises were more likely to experience problems due to ICT related security incidents, as almost a quarter (23%) experienced at least once problems due to such incidents in 2018, compared with one in six medium enterprises (17%) and one in ten small enterprises (11%) [2].

Digitalization is still in growing and further challenges arise continuously. In 2020, the number of connected devices is predicted to hit 50 billion. This number includes all devices, machines and sensors all over the world[3] and will further increase, which also contributes to an increase of security incidents most likely. Further on, digitalization in industrial manufacturers makes massive strides. In Germany, nearly 6 out of 10 industrial companies with more than 100 employees (59%) use special applications of Industry 4.0 in 2020. This means an increase of 10% compared to 2018. 51% actually develop new products or services in the course of Industry 4.0 or will do this in the near future and 26% change existing products[4]. On average, each fourth machine of German manufacturers was connected to the Internet in 2019[5]. These developments clearly show that the importance of IT security in the surroundings of Industry 4.0 and CPS will increase. Tools, methods and solutions for the use in industrial production areas as well as to accompany IoT products from their fabrication and the first start of operation through the whole life cycle until the final shut down are needed. As digitalization in all its aspects is changing, the used technologies need to be able to be updated and adapted also during running operations to meet future needs and to be able to increase security when attack vectors change with the change of the markets.

# 2. Current State of Technology Play

Depending on their size, companies have different preconditions and frameworks that have to be considered. This allows a great bandwidth in the analysis of the state-of-the-art. Geographical conditions, existing corporate structures, used hardware and IT infrastructure have to be included. This section, therefore, just gives an overview and reflects only a very limited picture. However, this serves to illustrate the different interests and needs of the individual company groups.

The first challenges to realize secure set-up production environments are usually found when a company is located at different regional sites or even international countries. But not only large companies have different locations and production sites. More and more SMEs are internationally networked today. Such companies can especially be found in special machinery, but also companies that own (secret) processes, compositions, software or other content have a high need in IT security solutions. The value of these companies is immaterial, but necessary to finalize an IoT product. Companies that do not produce (hardware) products themselves but outsource the manufacturing have to transfer the data to the production line in a secure way. They need to build secure, isolated routes to their manufacturing facilities and they need security standards on-site at the manufacturer so that this third party is not able to read out any transferred data without permission. Further on, maintaining and communicating with customer-installed machinery and robots must also be ensured through secure channels.

The following chapters describe environments, hardware, software, remote diagnostics and maintaining, data integration into IoT products and relevant regulatories. Further state of the art analysis regarding IoT and CPS can be found in the publicly available deliverable D2.1 “Consolidated state-of-the-art report”.

## 2.1. Environment

The following table gives an overview about the environment of small, medium sized and large companies and their structures. Whereas small companies usually have one site, one network and a small number of machines, medium sized companies are likely to have several (national) sites and several production lines. They have a small number of machines / robots of different manufacturers. Their net-

work is divided into office and production and they have an internal development department. Large companies have several international sites and a large number of machines /robots of different manufacturers. Unlike smaller companies, they have their own IT department and their network is highly subdivided. Nevertheless, they are depending on remote maintenance for their machines and do not have separated networks for each machine.

**Table 1: Environment and enterprise structure**

| Small | Medium sized | Large |
|---|---|---|
| One site | Several national networked sites | Several international networked sites |
| | Several production lines | Several production lines |
| Small number of machines | Small number of machines / robots | Large number of machines / robots |
| | Machines/Robots of different manufactures | Machines/Robots of different manufactures |
| Small number of machines | Small number of machines / robots | Large number of machines / robots |
| External IT support | External IT support | Own IT department |
| | Development department | Development department |
| Remote maintenance | Remote maintenance | Remote maintenance |
| One network | Office-Network | Office-Network |
| | Production-Network | Production-Network |
| | | Development-Network |

### 2.2. Hardware

There are big differences between the individual companies in terms of hardware. Not only is the size of the companies to be distinguished, but also whether they themselves provide hardware built by them or if they are pure users of this IT hardware.

Smaller companies usually use standard hardware as individual solutions would be too expensive. They (have to) accept that standard solutions do not always fulfil

their actual requirements and adjust their processes and products to standards. Innovations are disabled.

The situation is quite different for companies that they themselves have to provide a maintenance solution for products manufactured by them. It is in the foreground that their technology is secure and at the same time a remote maintenance is possible without undermining the security concepts of their customers.

Especially larger companies have their own internal solutions and the know-how to implement these solutions. They have enough specialists in their own ranks to ensure security in their own IT network and yet they also have to check their own concept with the installation of each new component so that the security of their devices and networks is guaranteed. So it is already planned ahead. The connections to the gateways are individually modifiable with modern techniques such as FPGAs and can be adapted to new devices, without having to replace the gateway itself. Thus, the security system remains intact.

**Table 2: Hardware for remote access used in small, medium sized and large companies**

| Small | Medium sized | Large |
|---|---|---|
| One network | Separated networks / VLans | Separated networks / VLans |
| Remote maintenance | Remote maintenance | Remote maintenance |
| No cloud | External cloud / container | Own cloud / container |
| Standard gateways | Individual gateways | Flexible gateways |
| | | Flexible / replaceable connectors |
| Small number of gateways | Middle number of gateways | Large number of gateways |
| Gateways of different manufacturers | Gateways of different manufacturers | Clustered gateways have the same manufacturers |

In the case of hardware and especially gateways which connect to the used IoT devices, very different solutions are preferred, above all for cost reasons. Startups and smaller SMEs often rely on favourable solutions from their point of view. They

have no budget for own developments, which is why they still prefer such solutions, ignoring their specific conditions and potential needs. They use complete solutions that they would not need at all, since they will never take advantage of these devices and their functions, but also have to pay for this functionality.

| |
|---|
| Individual and local hardware solutions with appropriate support would be desirable, but they also need to be affordable for small and medium sized companies. |

### 2.3. Software

The investments in certain software products are also very different from company sizes. The use of virus scanners, firewalls and office products is standard in every company, but small businesses and start-ups, in addition to office software, rely almost exclusively on standard software and systems that are not individually tailored to their (security) needs.

Since it is almost normal for large companies to use intrusion detection or even intrusion prevention software (IDS / IPS), this is still relatively new territory for medium-sized or small companies. IDS and IPS are often installed along with the firewall on gateways, increasing the minimum hardware requirements of the gateways and thus the cost. If there is another digital twin, which can be another layer on the gateway, then the requirements are even higher. In addition, special attention should be given to the devices and stored data at the end of their lifecycle.

The collection of operating and expiration data gets more and more important. The so-called Digital Twin is increasingly coming to the fore. Collected data is already used in the planning of new machines and processes in order to improve the development in advance. In use, the current operating data are then stored and analysed in order to make further improvements. There are several interested parties in the data, namely the company itself, as well as the manufacturers of the machines or their individual components. For this reason, it must be precisely defined here, who may have access to which data at all and the whole must take place in compliance with the GDPR.

Especially in small companies, messenger software which includes e.g. Facebook, WhatsApp, Telegram etc., is used extensively for internal communication. In

larger companies, however, this software is often strictly prohibited and may not even be installed on corporate mobile phones.

Besides software that is relevant for security reasons, other software like enterprise resource planning, manufacturing execution systems, customer relation management or data management systems, is used in different constellations. Interfaces and exchange of data not only varies from company to company, each solution and software differs from another. Solutions for securing IoT products and for secure set-up of production environments have to deal with different interfaces and software. Further on, IoT products have to be connected until their end of life (which is in case of an machine after 25 years or more), even though software and interfaces of the maintenance provider, the customer or other involved parties have changed in the meantime.

### 2.4. Remote Diagnostics and Maintaining

Within increasing digitalization, smart manufacturing gets more and more important. Not only that operational efficiency and reliability can be increased when digital control systems are used, machines that are connected to the Internet can also be maintained remotely. Technicians are more efficient and there are no unnecessary costs for travel and other charges. Additionally, response times are minimized which also reduces system downtime. Remote diagnostics and maintenance usually identify and fix problems with machines before the downtime reaches expensive dimensions. Especially for smaller companies that do not have their own IT department and their own technicians this is a very economical option to have access to experts.

In order to be able to manage remote access different methods are used. This variety of methods is a blessing and a curse at the same time, because machine manufacturers in particular nowadays still have to be very attuned to the customer's infrastructure, which often causes problems. In addition, customers want to have a guarantee that secret data and processes can not be viewed by anyone. Maintaining from the outside should only be possible if the customer allows it actively for a certain time slot. At the moment an external access is to take place, the complete session at the key position must be recorded by an audit log so that each

step can be followed later. This log must be unchangeable by appropriate mechanisms, but also be stored for a limited time to meet the condition of the GDPR.

**Table 3: Tools for Remote Maintaining**

| Small | Medium sized | Large |
|---|---|---|
| Teamviewer | Teamviewer | Teamviewer |
| RDP | RDP | RDP |
| | VNC | VNC |
| | Cisco WebEx | Cisco WebEx |
| | VPN | VPN |
| Putty | Putty | Putty |
| SSH | SSH | SSH |
| Individual Solution | Individual Solution | Individual Solution |

The remote IT maintenance methods listed in table 3 are typical standard practices used by many organizations, both customers and supporters. The problem with support is that operations often only require very specific methods, and thus they have to provide customer-specific procedures.

The belief of being able to solve everything via VPN and remote maintenance turned actually out to be very complicated and time-consuming in practice, sometimes even unsolvable for simplest problems. Concrete issues that need to be addressed are:

- connectivity (lack of bandwidth and Internet connection)
- too strong security mechanism are likely to lead to work flows that bypass existing security structures
- lack of awareness and knowledge of security needs
- inadvertent loss of metadata due to the used systems
- lack of monitoring for external connections

Remote maintenance is standard in IT, but now it is important to identify new and safe methods and to offer companies more effective solutions.

### 2.5. Data integration into IoT products

There are two possibilities to integrate data into an IoT product:

- firmware or flash device is recorded and verified directly on-site at the production location (in-line)
- the recording and verification of flash media is outsourced to external service provider. The media are delivered to the production location afterwards and then integrated into IoT products.

In both cases, one image is used for the whole product family. Individualization only takes place at the initial operation. Due to the amount of data (operating system, configurations, process data) and missing work flows for the recording and correlation of individual media, outsourcing is often preferred. The mass production of one and the same image through service provider seems to save costs and reduce production time, as recording and verification processes take place previously, before the IoT product is even in production. The tremendous security risks when using one and the same image for a mass of IoT products and the resulting costs are neglected: once attackers have hacked themselves into the primary image, they have access to the whole system.

Many industrial companies have realized these risks and start recording on-site at their production locations themselves again. Increasing digitalization of production processes allow the recording of individual data and unique encryption of each data carrier. The challenge in most cases is to install the necessary processes and work flows.

### 2.6. Relevant Regulatories

The following regulations and initiatives are relevant for IoT and Industry 4.0:

- GDPR General Data Protection Regulation (DSGVO [6]): It’s a regulation in EU law on data protection and privacy for all citizens of the European Union.
- TKG Telecommunication Act [7]: Law on the creation of modern electronic infrastructures, prevention of restrictions of competition and promotion of the interests of the population.
- Commission Implementing Regulation (EU) 2018/151 [8]: Defining the elements to be taken into account by providers of digital services in relation to

the security of network and information systems and the parameters for determining the significant impact of a security incident
- IEC 61508 is an international standard for the “functional safety” of electrical, electronic, and programmable electronic equipment [9]
- IEC 62890 Life-cycle management for systems and products used in industrial-process measurement, control and automation
- IEC 62264 Enterprise-control system integration
- IEC 61512 domain specific models for design and control of batch production processes
- RFC 2473 Generic Packet Tunneling in IPv6 Specification [10]
- RFC 6147 DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers [11]

## 2.7. Technology Analysis

This chapter give some details about existing technology for firewalls and remote maintaining. This information is important as their application is a must-have for companies. Please be aware that the the analysis only considers open source technology and might be incomplete.

### 2.7.1. Firewall

#### Iptables

This is a strong tool to set rules for the firewall. It runs directly at the shell level. However, there are some GUI that make the whole thing visually simpler. Iptables is considered widespread, which is why many system administrators are very familiar with it, but it is increasingly being replaced by Nftables, especially under Linux. The integration of an IDS / IPS in Iptables is not without problems and is rather complicated to carry out. IDS / IPS uses Netfilter and there are several points to note:

- IPS receives the bundle coming from kernel via rules using the NFQUEUE target
- The IPS must receive all bundles of a given flow to be able to handle detection cleanly

- The NFQUEUE target is a terminal target: when the IPS verdicts a bundle, it is or accepted (and leave current chain)

#### IPFire

Successor (actually splitting) of IPCop, which is very easy to use. IPFire can also be used in very simple systems and does not require many resources. The modular design makes it possible to determine what you install and use yourself.

#### Nftables

The nftables kernel engine adds a simple virtual machine into the Linux kernel which is able to execute bytecode to inspect a network bundle and make decisions on how that bundle should be handled. The operations implemented by this virtual machine are intentionally made basic. It can get data from the bundle itself, have a look at the associated metadata (inbound interface, for example) and manage connection tracking data. Arithmetic, bitwise and comparison operators can be used for making decisions based on that data. The virtual machine is also capable of manipulating sets of data (typically IP addresses), allowing multiple comparison operations to be replaced with a single set lookup.

The above-described organization is contrary to the iptables firewalling code, which has protocol awareness built-in so deeply into the logic that the code has had to be replicated four times—for IPv4, IPv6, ARP, and Ethernet bridging—as the firewall engines are too protocol-specific to be used in a generic manner.

The main advantages of nftables over iptables are the simplification of the Linux kernel ABI, reduction of code duplication, improved error reporting, and more efficient execution, storage and incremental changes of filtering rules. Traditionally used iptables, ip6tables, arptables and ebtables (for IPv4, IPv6, ARP and Ethernet bridging, respectively) are intended to be replaced with nft as a single unified implementation, providing firewall configuration on top of the in-kernel virtual machine.

Nftables also offers an improved user space API that allows atomic replacements of one or more firewall rules within a single Netlink transaction. That speeds up firewall configuration changes for setups having large rule sets; it can also help in avoiding race conditions while the rule changes are being executed. nftables also

includes compatibility features to ease transition from previous firewalls, command line utilities to convert rules in the iptables format, and syntax compatible versions of iptables commands that use the nftables backend.

In addition, IDS / IPS systems such as Suricata can be integrated into NFtables relatively easily. The best thing to do is to filter the bundles first, whether they could even get through the firewall and then add the IPS system as a further filter in the chain, which is then checked next.

### PfSense

PfSense is moving more and more towards commercial solutions. Therefore, the project OPNSense split off from it.

### OPNSense

OPNSense has best performance as firewall and also in the cooperation with the IDS/IPS Suricata. With the open source firewall OPNsense, there is the digital platform ET Open Rules[13] that offers many additional features such as intrusion detection & prevention, VPN two-factor authentication or high availability. Very easy to extend with own modules.

**Table 4: OPNSense Hardware Recommendations**

| | Mbps | User | CPU | RAM | Disk |
|---|---|---|---|---|---|
| Minimum | 11-150 | 10-30 | 500 MHz Single-Core | 512 MB | 4 GB SD/CF |
| Reasonable | 150-350 | 30-50 | 1 GHz Dual-Core | 1 GB | 40 GB SSD |
| Recommended | 350-750+ | 50-150+ | 1,5 GHz Multi-Core | 4 GB | 120 GB SSD |

As a firewall with stateful bundle inspection, OPNsense logs the status of all active network connections (connections / sessions) that run through the firewall. This information is stored in a state table. Two entries are saved for each individual connection (one for the outgoing connection and one for the incoming connection).

Each entry in this table occupies approximately 1 KB of RAM. Depending on the number of simultaneous sessions, the following RAM requirements arise:

**Table 5: OPNSense Stateful bundle inspection requirements**

| Parallel Network Connections | Entries | Needed RAM |
|---|---|---|
| 10.000 | 20.000 | 20 MB |
| 50.000 | 100.000 | 100 MB |
| 100.000 | 200.000 | 200 MB |
| 1.000.000 | 2.000.000 | 2 GB |
| 1.500.000 | 3.000.000 | 3 GB |
| 5.000.000 | 10.000.000 | 10 GB |

### Untangle NG Firewall

Untangle NG Firewall is a commercial version of a firewall, configured via a web based user interface. From content filtering to advanced threat protection, VPN connectivity to application-based shaping for bandwidth optimization, NG Firewall delivers a comprehensive, enterprise-grade network security platform for organizations in any industry.

### UFW – Uncomplicated Firewall

Uncomplicated Firewall (UFW) is a program for managing a netfilter firewall designed to be easy to use. It uses a command-line interface consisting of a small number of simple commands, and uses iptables for configuration. There is also a graphical called gufw interface available. UFW is part of the Ubuntu Linux installation but it is also available in Debian-based distributions and in Arch Linux.

### Smoothwall Express

Linux-based network firewall installed on a computer via CD and configured via web frontend; Internet connection can be made via ISDN, DSL or Ethernet; Firewall features such as a web proxy (Squid), virtual private networking (FreeS / WAN), IDS (Snort), bundle filtering and accounting (ipchaines) are preconfigured.

### VyOS

VyOS is a Linux-based network operating system based on Debian GNU/Linux that provides software-based network routing, firewall, and VPN functionality.

The VyOS project was started in late 2013 as a community fork of the GPL portions of Vyatta Core 6.6R1 with the goal of maintaining a free and open source network operating system in response to the decision to discontinue the community edition of Vyatta. VyOS is primarily based on Debian GNU/Linux and the Quagga routing engine. Its configuration syntax and CLI are loosely derived from Juniper JUNOS as modeled by the XORP project, which was the original routing engine for Vyatta.

In the 4.0 release of Vyatta, the routing engine was changed to Quagga. As of VyOS version 1.2, VyOS now uses FRRouting as the routing engine.

- It's more than just a firewall and VPN, VyOS includes extended routing capabilities like OSPFv2, OSPFv3, BGP, VRRP, and extensive route policy mapping and filtering
- Unified command line interface in the style of hardware routers.
- Scriptable CLI
- Stateful configuration system: prepare changes and commit at once or discard, view previous revisions or rollback to them, archive revisions to remote server and execute hooks at commit time
- Image-based upgrade: keep multiple versions on the same system and revert to previous image if a problem arises
- Multiple VPN capabilities: OpenVPN, IPSec, Wireguard, DPMVPN, IKEv2 and more
- DHCP, TFTP, mDNS repeater, broadcast relay and DNS forwarding support
- Both IPv4 and IPv6 support
- Runs on physical and virtual platforms alike: small x86 boards, big servers, KVM, Xen, VMWare, Hyper-V, and more
- Completely free and open source, with documented internal APIs and build procedures
- Community driven. Patches are welcome and all code, bugs, and nightly builds are publicly accessible

The recommended system requirements are 512 MiB RAM and 2 GiB storage. Depending on your use you might need additional RAM and CPU resources e.g. when having multiple BGP full tables in your system.

**Vuurmuur**

Vuurmuur is a iptables GUI that works very well with Snort and Suricata, but it hardly has any maintenance and accordingly IPv6 is not fully supported. So it is easier to set up zones for DMZ, WLAN, LAN suitable for these interfaces.

The setup of the zones goes from "trusted" (everything is forwarded) to "drop" (incoming bundles are only forwarded if they refer to outgoing bundles). The setup is done via command line, but there is a graphical tool ("firewall") for Gnome, which always has to be installed separately.

### 2.7.2. Remote Maintaining

Remote access from one computer to another is indispensable in today's private or business world. On the one hand, an employee on the move or in the home office can use the necessary programs and resources of the corporate network via remote access. On the other hand, it happens that within the framework of order data processing, a service provider has to carry out remote maintenance via the Internet. The possibilities for the connection between two computers and their security level are explained in the following article.

Protocols:

- Telnet: Terminal level, unencrypted data flow, connection only to one computer
- SSH: Terminal level, encrypted (SSH1 has security vulnerabilities, SSH2 should only be in use); Connection only to a computer
- VPN: connection via encrypted tunnel to the network, not just to a single computer (thus also direct use of printers etc. possible) Pros: Easier to troubleshoot, problems easier to solve, more secure; Cons: large bandwidth requirements, may have slower speeds, can cause system errors if not configured properly; For VPN, PPTP (outdated, TCP port 1723), SSTP (TCP port 443, proprietary), OpenVPN (TCP port 443), L2TP + IPsec (maybe NSA compromised) and IKEv2 (uses IPSec for encryption, developed by Mircrosoft

and Cisco); OpenVPN is generally recommended for its tranparency and safety (open source); Crucial is the encryption, because it is on the latest standard AES-256.

- VNC: Screen content of the remote computer is transferred to the own monitor. He has the complete desktop access. Disadvantage is the large amounts of data that is transmitted, which can be reduced by compression. Additional software required in the form of a web browser or special viewer. Encryption is not available in all VNCs!
- RDP: similar to VNC, proprietary network protocol. Data is automatically encrypted. Pros: easier to use, can use screen share; Cons: harder to diagnose, can be hard to configure
- X11: Use the possibilities to connect directly to an X11 server and open a new session there.

**UltraVNC/RealVNC/ThinVNC**

When it comes to the remote control of computers, VNC is mainly used. The tool is available in different versions. Above all, VNC is popular for remote maintenance in networks when no connection via the Internet is necessary. VNC variants use the VNC protocol, which means that the programs are compatible with each other.

UltraVNC is especially suitable for experienced administrators. UltraVNC also lets you transfer data, create encrypted connections, and enable users to communicate with each other. In order for administrators to be able to access a computer through the viewer, the UltraVNC server component must first be installed.

To build a remote maintenance session, the Viewer tool from the UltraVNC installation is used. An alternative is RealVNC. The password and authentication for access are configured on the client to be accessed.

The third known variant of VNC is ThinVNC. ThinVNC does not require software on the computer for client access, but can be accessed via a web browser. To do this, you must start the server part of ThinVNC. An installation is not necessary. To work over the network, a rule must be created in the firewall to allow access. To connect to ThinVNC, enter the IP address and port of the destination computer.

### Teamviewer

The TeamViewer software also offers the possibility of establishing a connection via the Internet. The software is for private use. Anyone who uses TeamViewer commercially must license the software.

The advantage of TeamViewer is that no software has to be installed on the remote-controlled computer, but the user simply starts the tool and passes on the access code to the remote-controlled user. This can then quickly and easily establish a connection. TeamViewer also provides its software for macOS X, Linux and other operating systems. There are also apps for iOS and Android.

TeamViewer is one of the best-known tools for remote maintenance because it provides an infinite amount of features that does not need to be installed, even for beginners to use, and is available for home users free of charge.

### Anydesk

AnyDesk provides the ability to efficiently access the desktop of Windows computers. The solution is generally available for private use free of charge.

The tool focuses on remote maintenance of workstations. As with TeamViewer, an installation is not required. After the start of the client, an address is generated via which the administrators are allowed to access the computer. However, the connection does not take place with the RDP protocol but proprietary.

### Chrome Remote Desktop

If you work with Google Chrome, you can opt for the free Chrome Remote Desktop extension. You can also access your PC at home with Chrome Remote Desktop, while Chrome does not need to be running.

In addition to Chrome Remote Desktop, you can also access Android smartphones / tablets on their home PC. All you need to do is install and set up the Chrome Remote Desktop app.

### Datemware

Dameware is a remote control for computers, but offers much more than a simple remote maintenance. The solution also lets you manage and remotely control Mac and Linux machines. Dameware can also remotely manage system services

and also provides an overview of the respective computers. Users looking for remote maintenance should see the solution for 14 days. During this period, the product will be available as a trial version almost unrestricted. Then you have to buy Dameware, but until then the software can be used for free.

**Ammyy Admin**

Ammyy Admin provides remote control and can exchange data between two computers, even over the Internet. An installation of the software is not necessary, Ammyy admin only needs to be started. When the tool is started, an ID is generated and displayed. These can be used to establish a connection with the client.

Using Ammyy Admin is similar to using Teamviewer. It has the functions of displaying the screen, remote control, file manager, voice chat and RDP connection. After connecting, the accessing user sees the desktop of the other computer. The toolbar can be used to perform various tasks.

**Cisco WebEx**

WebEx offers a variety of online collaboration solutions for companies and colleagues. These include, for example, video conferencing solutions or screen sharing features. For larger companies, remote support solutions or various large, virtual meeting rooms are available to collaborate internationally. The individual products have a modular structure and can be adapted and expanded according to their own needs. In addition, there is platform independence, which enables the use of mobile devices for remote collaboration.

Cisco WebEx is considered the standard in the virtual meeting market. According to Cisco data the chrome extension is used by approximating 20 million users is world-wide. In total, according to Cisco, up to three billion minutes of meetings are scheduled each month, with a total of 52 million users.

The software of WebEx and in particular the various browser extensions were heavily criticized, as more security holes had occurred. The use of the plug-in for the web browser Firefox was temporarily blocked by Mozilla on January 23, 2017 in the meantime even global, so the access for WebEx users had to be done via the desktop software. Certain domains could directly execute code on any Windows system through the browser extension. You could even use cross-site scripting (XSS) on one of these legitimate WebEx sites to inject code around.

### Guacamole

Apache Guacamole is a clientless remote desktop gateway. It supports standard protocols like VNC, RDP, and SSH. It's called clientless because no plugins or client software are required. Guacamole is installed on a server (or a Hub, SBI-Hub) and thanks to HTML5 the only thing needed is access to a web browser.

Apache Guacamole is free and open source software. It is licensed under the Apache License, Version 2.0, and is actively maintained by a community of developers that use Guacamole to access their own development environments.

For enterprises, dedicated commercial support is also available through third party companies.

Guacamole masters many currently used authentication methods:

- Database authentication
- LDAP authentication
- Duo two-factor authentication
- TOTP two-factor authentication
- HTTP header authentication
- CAS Authentication
- OpenID Connect Authentication
- RADIUS Authentication

# 3. Risks of Security Leaks in IoT Products and Production Environments

The quality of hacker attacks has increased dramatically in the recent years. Attacks on the IT infrastructure of companies are carried out by professionals with a high level of technical knowledge. Not only the Darknet has to be mentioned here as potential source of attacks, these attacks can also be carried out by competitors (e.g. to prepare an unfriendly takeover) or even by foreign state institutions.

In many companies, IT systems are the backbone of business models and responsible for their performance. Problems with IT systems can cause enormous damage to a company, ranging from loss of production through loss of revenue to the existential threats. Though the expenses on IT security are still rather low until companies suffer from attacks themselves. Once they are confronted with the impact of hacking attacks, they invest significantly more in their IT security.

Potential risks include e.g. hardware failure, software failure, data theft, data loss, data misuse or espionage. To avoid security leaks in IoT products and production environments, both hardware and software and their potential attack vectors have to be considered, as well as different communication channels.

## 3.1. Hardware Attacks

There is a distinction between three variants of physical attacks: non-invasive, semi-invasive and invasive attacks.

### 3.1.1. Non-Invasive

For non-invasive attacks, the examined hardware chip remains completely unchanged. In order to get conclusions from the behaviour of the chip, two methods can be used. First the method of time measurement, in which one tries to perform a password decryption and at the same time logs the time each time. Especially with poorly programmed decoding, the routine is aborted immediately if a character does not match. Such routines should only return the result after a complete pass, so there are no time differences. The second method analyses the power in two ways: consumption during an operation and fault injection. With the help of an oscilloscope the attacker visualizes the power consumption on the side-channel. It is

important to know that an addition in an encryption has a lower power consumption than a multiplication.

The remedy is masking, random dummy operations or the use of secure components that have been tested for side-channel attacks. While using fault injection, the attacker either influences the clock (clock glitching) or the applied voltage (voltage glitching).

In the semi-invasive method, the actual chip is exposed through mechanical and chemical measures to reach the top layer and all contacts. Care is taken to ensure that the chip remains fully functional. Thanks to the optical refraction, optical microscopy identifies the individual layers with an electron microscope. One can analyse the uppermost layer accurately and identify potential targets to which an oscilloscope can be connected in order to obtain information during the operation of the chip.

### 3.1.2. Invasive

The most extreme method is invasive. Here, all layers are exposed by either wet chemical methods or polishing and analysed. When analysing the layers between the layers, additional information is obtained about the connections between the layers, since they can be seen very well under the microscope there. Most interesting, however, is the lowest layer of flash memory. Here you can possibly read the information about the firmware and then analyse again. Probably the most expensive process at the moment is the use of a Focused Ion Beam, where the chip is only drilled through the beam at very specific locations. This process is unlikely to be used by individuals and is a process normally used to analyse defective chips.

Obtaining information about the installed hardware is associated with high costs, but takes place and offers a completely different dimension when attackers obtain information about the device or the components used.

## 3.2. Software Attacks

Attackers use gaps in IoT products and in production networks. It is in their interest to enter IoT equipment as unnoticed as possible in order to generate botnets (e.g. like Mirai) or they try to infiltrate higher-quality IoT hardware in companies to

penetrate the corporate networks for various reasons (e.g. unfriendly takeover, to damage competitors). The following listing points out the most important security leaks. Another good summary is provided by the Open Web Application Security Project (OWASP), a non-profit organization dedicated to improving the security of applications and services on the World Wide Web[12].

### 3.2.1. Weak, Guessable or Hard-Coded Passwords

Sometimes hurdles are not even put in the way of hackers. The default password has not been changed or the password is very weak. Often it is only enough to know the firmware of an IoT device. Nothing easier than that, because not infrequently hackers will find the latest firmware of a device on the homepage of the manufacturer as a download to provide the devices with updates. So the attacker only needs to load these files, then extract them and he'll be able to get in-depth with them to find potential attack points.

### 3.2.2. Check of Service

The second important point of attack is a check of service, in which the ports of an IoT device are tried out. If you look at network traffic on the Internet and analyse it, you can see that this is happening permanently. As soon as a device goes into operation, it receives requests for specific ports. Very popular are the ports 80 and 443, as these show whether a web interface is present and if so, further penetration tests are performed here to find gaps in the system.

### 3.2.3. Web Interfaces

There is a high risk that parameters will be taken over unchecked in the web interface, e.g. additional arguments. Program calls can be hooked up, which are then executed automatically, allowing the attacker to infiltrate the system.

### 3.2.4. Updates

They are extremely important for IT and IoT systems today. The more incomprehensible it is how reckless it is handled. Together with the updates often obsolete

libraries are used, which no longer comply with the current standard and are therefore not at the security level they should actually be. Obsolete devices with old technology deployed in the production or in the network infrastructure are used according to the motto "never touch a running system" or simply nobody looks at these components, which means that they do not experience any renewal. A good update management is necessary to react quickly to new forms of attack.

#### 3.2.5. Default configuration

Sometimes the problem is not the user but the delivery of devices. The default configuration of network components does not take strict security settings into account. The components are pre-configured so that once everything works, it is not maintained any more.

### 3.3. Communication Channels

There are two main communication channels in the context of securing IoT products and secure set-up of production environments that are current status: communication between manufacturer and suppliers and communication between manufacturers and their products.

#### 3.3.1. Communication between Manufacturer and Suppliers

A manufacturer has one or more suppliers with sub-suppliers who e.g. provide parts of the product or a machine of the production process. A production machine at the same time consists of different components (e.g. manipulators, sensors, servers). The manufacturer must now provide the supplier with secure access to this production machine. The production machine is usually not separated from the entire production network in terms of safety. In this case the supplier has access to the entire production network. The problem increases if the supplier has to forward the access to sub-suppliers.

In most cases, VPN and remote maintenance tools (e.g. Teamviewer) are used and a transparent audit log (what was actually done during remote maintenance, what was changed and which data was transferred to and from the machine) is usu-

ally not possible. At the moment, the manufacturer in most cases simply trusts the supplier. Contracts are used to compensate the security gap.

### 3.3.2. Communication between Manufacturer and Suppliers

During the life cycle of a product, updates or upgrades of the delivered systems will be necessary. In some cases, remote analysis of unknown errors have to be carried out. The importance of the transmission of different product meta data to the manufacturer increases and above all, the establishment of artificial intelligence requires the data of the individual IoT devices. Anonymization of data and protection of privacy are of enormous importance in this context.

# 4. Requirements

Although manufacturing environments, production sites and IoT products differ in many dimensions, they all have to satisfy special requirements and require a secure set-up of production environments (see the public available deliverable D2.2. “Consolidated business needs” for further details). It is necessary to protect sensitive data at any process step and any stage of their life cycle: machines, data transfers, machine-to-machine communication, remote maintenance of machines and of IoT products, updates and upgrades, authorization and rights management, access logs and so on have to be considered when an IT security strategy is implemented. It is important to involve all participants in security concerns, as this affects production and technicians as well as sales, after-sales and marketing, document management, development and back-office. Further on, different participants along the value chain have to be considered: this begins with the manufacturer of individual components that will later be installed in IoT devices, continues with the manufacturer of devices that use IoT and goes on to the user of these IoT products.

The firmware of IoT devices has to be specially protected today, since experienced technicians and attackers can use information from the firmware to draw conclusions about the methods and techniques used. This is all the more critical when it comes to portable media, since it could easily be read out on another device or even duplicated. A first step is to encrypt such media using currently recommended methods. There are several methods to enable decryption. One method would be to have a user enter the key on the device, but this would simply not be practical with the quantities of IoT devices. So the decryption must be done by the device itself. Here it would have to be determined which media already exist that offer methods for this and, alternatively, how one could automatically encrypt media that do not offer any built-in methodology for this. The question then arises, where are the encryption algorithms stored, because this should not take place in a normally accessible area if possible. Another point to pay attention to in this context is what should happen to the medium if it is not connected to the assigned IoT device.

According to the number of involved parties and to the environment, there are a number of requirements that have impact on IT security strategies and solutions:

1. secure and trustworthy service connection to the installed machine in the simplest possible way that allows remote control, logging and service for defined authorities
2. methods and tools to easily install and integrate new equipment or machines
3. support of elderly machines (possibly upgraded)
4. clear authentication for the individual service technicians in case of maintenance (remote or on-site) and logging of all activities (preferred in form of audit logs) during service operation to provide traceable security about all actions on all sites
5. a rights management that does not grant access to every component (e.g. access to sub-units of the machine for sub-suppliers) is necessary to ensure that a hack or leak does not affect the whole machinery or all IoT devices at once
6. availability of remote provisioning, configuration and maintaining of all components and machines, including historically grown networks; relationship of trust between machine manufacturer and machine operator as the operator wants to collect and evaluate data about the manufacturing process, whereas the machine manufacturer or the external technician should have no or only limited access to this data
7. support of machine-to-machine communication and monitoring of data streams
8. mechanism to securely transfer data form the data sources (which may be decentrally located) to the production site and to ensure that workers in the production have no possibility for data misuse (e.g. access to data, unauthorized copies of flash media, unintended data loss)
9. data encryption and mechanism that only allow decryption in combination of different parameters (e.g. product serial number and unique flash device)
10. secure data recording of (flash) media devices directly before assembling the IoT production to ensure error-free correlation; quality assurance and work flows that accompany the recording are necessary for the traceability of data transfers, correlations and access
11. safe processes are needed to securely communicate with IoT devices in _CPSas they are favoured targets of attacks from the network to either infiltrate the network they are in or to use them as tools for mass attacks (e.g. DdoS) with so-called botnets (e.g. Mirai)

12. secure communication between IoT devices in the CPS is a necessary process in the age of digitization
13. appropriate secure communication (privacy, confidentiality) to support deployment, maintenance and updates/upgrades at customer side
14. implementation of security testing along the whole life cycle of a machine but also of an IoT device, including product quality assurance, component and system maintenance, update/upgrade processes; security concepts, tests and validation methods as well as appropriate documentation and traceability are needed

IoT products are not only hardware products anymore. Their digital content (software, configurations, meta data etc.) is likely to be more important than hardware parts. In modern manufacturing settings, content owners are not manufacturing the products any more. They deliver their content to third parties where the manufacturing of the IoT product takes place. Not only the delivering process has to be secure, it is furthermore important that the content is secure during the whole production process.

Data can be recorded to encrypted flash media and shipped all over the world to the production site. Besides the fact that this would mean having a lot of media on stock, there are a lot of risks in this strategy. The correlation of individually encrypted media to the corresponding IoT product is nearly impossible then. Software changes or new releases are not available immediately, as flash media has to be produced in advance. And what happens when a container full of flash media gets damaged or lost on the way? How to manage access and identification processes to the IoT device? What about access during the production when the data to be recorded is decentralized stored? Secure boot, unique and personalized encryption considering product-specific indicators and explicit identification are only some parameters that have to be considered already during the recording process of flash media.

#### 4.1.1. General Data Protection Regulation (GDPR)

This point is all the more important as companies need to store sensitive, security-relevant data and keep that data in line with current European regulations. In addition, regulations stipulate the highest security levels for these data centres.

## 5. Guidelines

An analysis of the IT infrastructure and the needed IT security components should be done with the support of IT security experts, which is generally desirable and recommended. Back office, development department, production department, guest network and existing IoT devices (e.g. heating, lamps, printer) should be taken into consideration, as well as different CPS architecture layers (see the public available deliverable D3.2 “Guidelines, processes and recommendations for the design of dependable IoT Systems” for further details).

Systems that isolate individual networks within the enterprise (security by isolation) use virtual networks and allow secure remote maintenance, while at the same time providing security for the machine manufacturer and the machine user through audit logs. It is important to ensure that all networks and devices are regularly maintained and receive security updates. Further on, all accesses have to be logged to get an overview about anomalies.

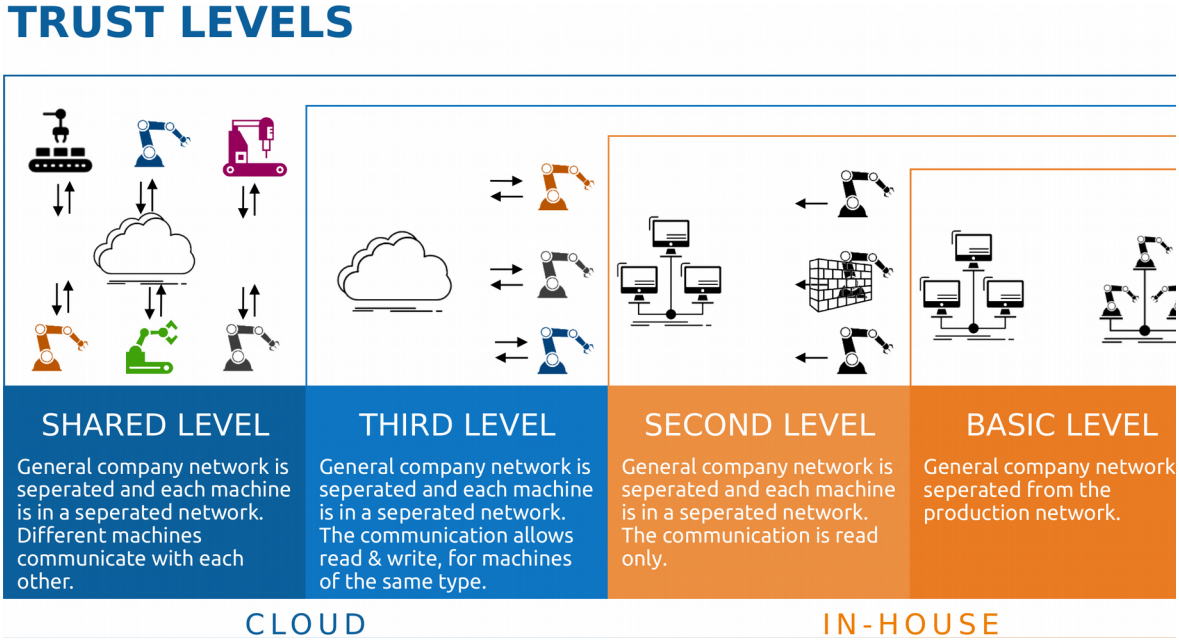


*Figure 1: Trust Levels*

To reach a high level security standard, the company structure has to be divided into individual zones. Depending on the number of individual zones and the intensity of separation, different trust levels can be defined (see figure Figure 1: Trust Levels). With regard of these trust levels, the following guideline gives hints what to consider.

The **basic level** describes a simple separation between the general company network and the production network. This is the first step to enhance security, as different end devices (e.g. mobile phones, tablet PCs, notebooks), which are a fundamental weak point in a network, are separated from the production machines. Companies have to ensure that occurring incidences (e.g. single devices which are hacked or historically grown networks which have some misconfigurations) do not affect production, production areas and machine configurations.

The **second level** describes the separation between general company network and production network, in which every machine of a production environment is separated in its unique network. User, service technician or even hacker are working only in one network and on one machine. Changes of configurations and other settings do not affect other machines. The communication is read only. Similar to the basic level, all data and communication is in house and there is only one location.

If production takes place on several production sites and locations and it is necessary to allow read and write, it is necessary to consider cloud solutions including their risks and opportunities. If machines of the same type have to be considered only, companies should reach the **third level** of security. This means that the general company network is separated and additionally each machine is in a separated network. The communication allows read and write, but additional security measures have to be taken into account (e.g. logging of all activities, analysis of anomalies). A test-bed to demonstrate how third level security can be integrated into production environments is developed during the project and is described in detail in chapter 6.1.

The highest possible security level is the **shared level**. In this level, different machines can communicate with each other, while each machine is separated in its own network. A secure cloud is available that handles the communication and all security relevant elements.

The aim of our research in IoT4CPS is to reach “third level” and to demonstrate high security levels for IoT and Industry 4.0 that are affordable for SME.

### 5.1. Open Source

The characteristics of open source are basis to develop and reach high trustworthy security solutions:

- the entire source code and the sources are available
- sources are provided in standards that can easily be implemented into projects
- large communities support, adapt and improve developments continuously
- codes and knowledge are shared which enables rapid location and elimination of errors
- open source solutions are long-term available and cannot be stopped by individual stakeholders

Open source enables transparency. Each manufacturer can understand and control which components were installed, what these components are doing and how things were set up. The attention to security is clearly visible and there are no hidden gaps.

Commonly, open source describes software tools, programming languages and libraries, but also hardware parts are developed under open source. Developers share the layouts of circuit and wiring diagrams. They build up low cost systems that start to overtake industrial standards and offer long-term available systems.

Open source software and open source hardware enable SME to build their independent cloud solution and to offer trustworthy systems.

### 5.2. Regular Maintenance

Commercial systems that are easy to use (e.g. VNC, Teamviewer, Anydesk) are the state of the art for regular remote maintenance. These tools have been settled as standards, but the relay systems behind these concepts and the potential security risks are disregarded. These third party products have access to the most sensible areas and data of companies.

It is necessary for companies to choose or develop secure maintenance systems that do not work over public brokers giving unknown third parties access. Further on, logging and monitoring of each session have to be available and provide all in-

formation in case of an accident or breakdown. It has to be impossible that a remotely maintained machine endangers human health because of misconfiguration, malfunction or intervention through third parties. It has to be defined what a system is allowed and able to do in the background to protect human health in front of machines. This is one of the main guidelines when remote maintenance systems are designed, with a view on human safety conditions.

### 5.3. Security Updates

It is essential that security updates are available for the IT components of each single product. Therefore, remote access and connectivity has to be available throughout the whole product life-cycle. Security updates must not only be installed as soon as possible after new scenarios become known, it is further on reasonable to update IT components periodically. Environments and protocols change during the life-cycle of a product and insecure components may have to be replaced by newer versions if remote updates are not possible.

Secure connections from manufacturer to their products will get more and more important in the next decades. Manufacturers will have to pay increased attention to security until the end of the life-cycles of products. Missing life-cycle management leads to security vulnerabilities and outdated functionalities, which will further on lead to a loss of market share and economic damage.

Manufacturer further on have to consider security updates for hardware as well. Even hardware updates can be done remotely, e.g. using field-programmable gate array (FPGA) chips.

### 5.4. Cloud Computing

Cloud computing has significantly gained in importance as high speed internet access from any location worldwide, hardware virtualization, low-cost computers and high-capacity networks have become standard. Cloud server can be used for internal storage, for the exchange and collaboration of data or for the whole communication infrastructure.

The advantages of cloud systems are obvious (e.g. independence of device and location, improved agility for organizations, cost reductions, availability, scalability), but security concerns may not be disregarded. In the past, a lot of different platforms and standards were developed and settled on the market as security component manufacturers, cloud providers or industrial control system developers try to build up their own cloud systems. Movements in the sectors of Industry 4.0 and IoT even push these developments further. Though these cloud systems differ from each other, the problem for externals to identify their trust levels is all the same. Manufacturers and customers of a machine have to trust the security of the cloud systems. System architecture, implemented standards and location of data storages commonly are the secret of the cloud providers.

Considerations for cloud services have to include a lot of different concerns, among them:

- check of the physical location of the server: where the data is stored makes a difference to the legislation that applies. The European General Data Protection Regulation (GDPR) e.g. has different requirements on the protection of personal data than American law.
- check of backups: it is necessary to check if backups of the cloud services and the data exist and how data can be recovered if it comes to data loss.
- access to sensitive data: it is important to check the privacy policies of the cloud provider to learn how data is protected and who may have access to this data. Please be aware that some countries have laws that allow governmental organizations unrestricted access to the data.
- type of data stored in the cloud: which information should be processed in the cloud? Is it used for the exchange of documents or for the whole mailing? How sensitive is the meta data (e.g. who communicates with whom how often)?
- meta data: an institution has to be aware that even if data is protected (e.g. through contracts, encryption), agreements can be bypassed or meta data can be collected, independent of the encryption method or the type of contract. Meta data like which file was opened several times through different persons, frequency of communications, destinations of links etc. can give revealing information about internal company processes or customer structures.

The ideal system would be transparent and based on open source components. Manufacturer who need a cloud system for secure remote maintenance, life cycle management and data exchange would be able to build up such a system by themselves. The security by isolation (SBI) cloud concept demonstrates this opportunity for the SME manufacturers as well as for global acting enterprises (see chapter 6.1 for further information on the SBI-Cloud).

### 5.4.1. Private vs. public cloud

Provider all over the world offer public cloud services as a paid subscription or free of charge. Besides these very well visible providers (in most cases large companies that are registered in the US), many regional provider run server infrastructure in their regional periphery and offer tailor-made cloud solutions. It is worth the effort for companies to search for these regional provider and to check their cloud services in relation to availability, security and data protection. If some aspects are unclear, they usually have one contacts person that can explain strategies and structures of their clouds. These contacts person are also available if there are technical problems, data gets lost or hacked or in any other cases.

Alternatively, companies should aim to run their own private clouds. Open source tools are available for free and can be installed and configured on any server. Companies who have their own IT department can run these private clouds themselves, but also external IT experts can install and service the infrastructure. The main advantage of private clouds is the knowledge about access to data and meta data. A company that runs its own private cloud can decide itself at any time who gains access to data. Meta data are not extracted unnoticed and analysis through third parties do not happen.

## 5.5. Encryption

Various methods should be examined for encrypting the transmitted data taking into account the results researched in work package 3 deliverables 3.4 “System architecture patterns for enabling multi-stakeholder trust provisioning during production and maintenance” and 3.5 “Guidelines and recommendations for the use of cryptography to build trustworthy IoT applications”. In particular, the performance of alternatives to AES256 should also be considered. Development continues in the

area of encryption. New methods should be tested again and again in the system for the usability and improvement of protection, but also completely different possibilities, e.g. Quantum encryption should be checked for its general applicability.

Even if it is not possible to analyse the content of encrypted data, it does contain meta data that provides important information. In particular, the accumulation of data that travels between certain nodes can provide important conclusions. These facts have to be considered when setting up communication environments.

### 5.6. Firewalls

Firewalls are standard in every company network these days. However, when dividing a network by security by isolation, it is necessary to install a firewall at each intersection in order to secure the respective area separately so that malware from the adjacent clusters cannot penetrate or unauthorized persons do not get access to systems they are not allowed to access.

Firewalls have been a standard in IT for many years, but their tasks are becoming increasingly complex, making configuring firewalls no easier. In addition, the approaches of firewalls are very different and, accordingly, the combination with additional filters such as IDS or even IPS systems on the same system is not always easy or sometimes even impossible.

For this reason, it is necessary to clarify exactly which systems could be considered and which are suitable for future-oriented tasks.

### 5.7. Afterlife of devices

IoT products are continuously in use (7/24) and repeatedly collect and store data. It is important that companies have a strategy defining what should happen if devices are replaced or sorted out. Each device has to be restored to its original state so that no sensitive data remains stored at this device. If third parties come into possession of such a device, it may be functional, but it must not contain any information about the previous owner’s processes. If a device has a defect and therefore has to be replaced, existing data can no longer be removed from the memory easily, though it may still be possible to read out sensitive data. Companies

have to take care about what happens with this IoT device to avoid unintended data access.

It is important to involve all participants in these processes. This begins with the manufacturer of individual components that will later be installed in IoT devices, continues with the manufacturer of devices that us IoT, the user of these IoT products.

# 6. Test-Beds

The objectives of the research and development activities in IoT4CPS pursue a holistic approach that combines operational aspects as well as technology. The test-beds therefore integrate security levels across all dimensions in order to a) ensure trusted interaction across devices, machines and networks; b) maintain integrity, authenticity and confidentiality of information; and c) sufficiently protect production data and intellectual property.

Splitting networks within an industrial environment becomes more and more important with a growing number of IoT devices. For security reasons, it is necessary to create distinct network areas that restrict the capability of IoT devices to communicate otherwise attack vectors will be opened. On the other hand, a smart production architecture must allow for easy handling of attaching, provisioning and remote maintenance of new equipment or machines, as well as data analytics for process optimization.

## 6.1. SBI Virtual Factory Demonstrator

Security-by-Isolation (SBI), which is based on the virtualization of the network and the virtual separation of the connected components, is basis for the realized test-beds. This concept requires only a few hardware components, which do not necessarily have to be on-site (except for the actual SBI-Box as shown in our demonstrator). SBI architecture can provide the appropriate tools for achieving the necessary trade-off for that purposes. Security can be created by cryptographically protecting the complete communication (e.g. by using a secure VPN) of the individual components and using modern authentication and authorization methods (Active Directory, two-compon-

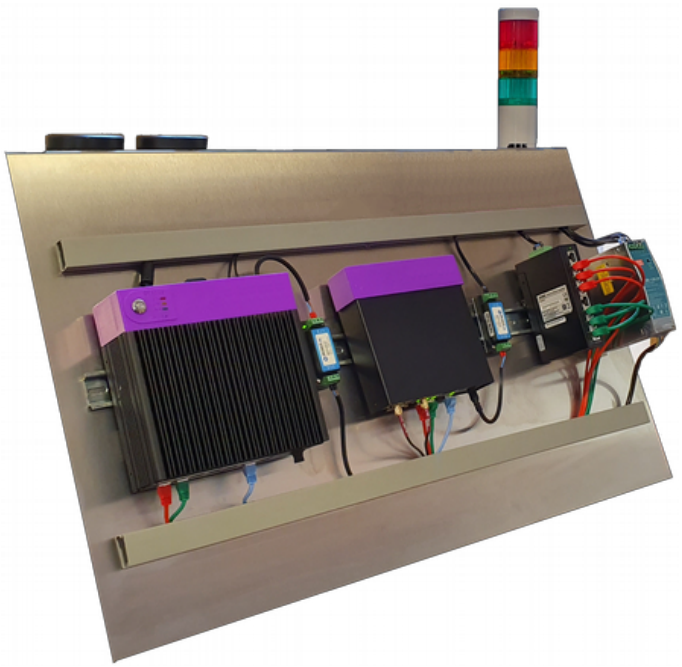

*Figure 2: SBI virtual factory test-bed*

ent authentication). To facilitate users' trust into the system, its components are made available to users as open source. Thus, its processes are transparent, the product itself can be further developed and there are no hidden surprises like backdoors in the software. Reliability is also ensured since operations can be guaranteed at any time with appropriate measures, in this case by redundant systems.

The results of work package 3, especially deliverable 3.2 "guidelines, processes and recommendations for the design of dependable IoT systems", deliverable 3.3 "Guidelines and recommendations for resilient system architecture pattern concepts and HW-based solutions for safe & secure IoT", deliverable 3.4 "System architecture patterns for enabling multi-stakeholder trust provisioning during production and maintenance" and deliverable 3.5 "Guidelines and recommendations for the use of cryptography to build trustworthy IoT applications" were used to design the solution.

To facilitate users' trust into the system, its individual components are made available to users as open source. Thus, its processes are transparent, the product itself can be further developed and there are no hidden surprises like backdoors in the software.

### 6.1.1. System architecture

The SBI-connected virtual factory consists of a database (SBI-Core) at the mechanical engineer, several VPN hubs (SBI-HUB) and the gateways (SBI-Box) for the machine user. It is in the machine operator's sense that there is no down time of the hardware, so the systems should be redundant. In particular, the SBI-Box set up and used in the enterprise should either be redundant or at least have a fail-over solution. In case of any failure in the systems, the SBI-Box with fail-over solution recognizes these fails and takes over the most important functionalities of the SBI-Box (see figure 3).

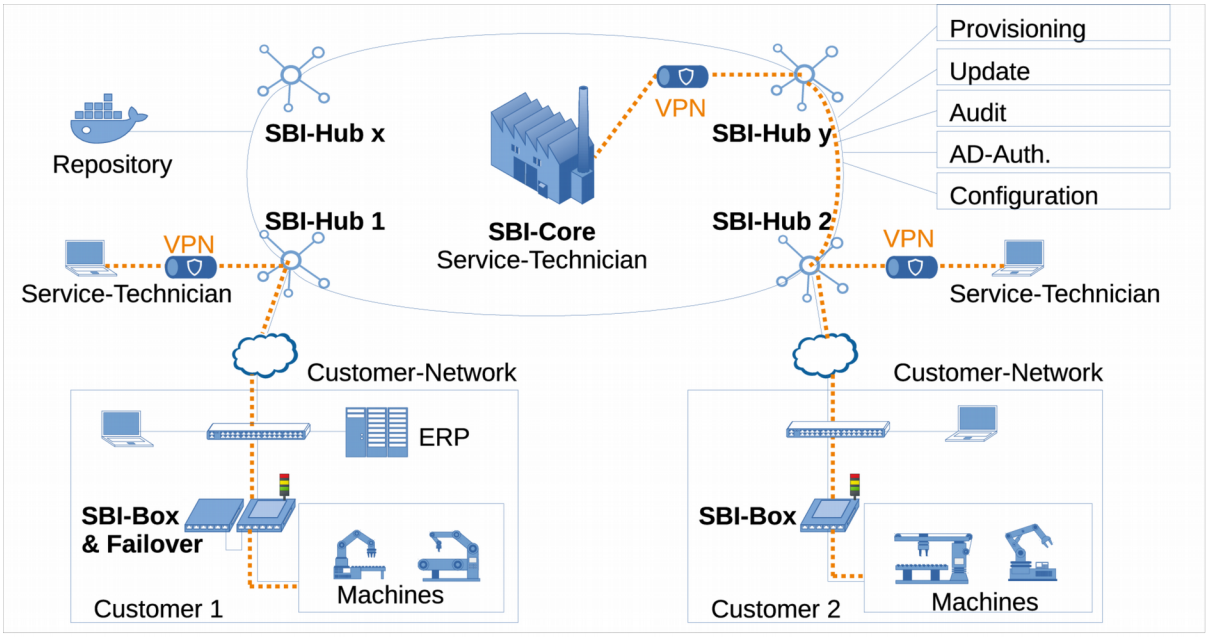


*Figure 3: Overview SBI-Concept*

The **SBI-Core** is the central database management system. It manages the SBI-System. Among other things, it manages and provides the SBI-Hubs, SBI-Boxes, connected machines, technicians, audit logs, firewall templates and rules for the SBI-Boxes. Individual certificates and configurations of the SBI-Boxes and technicians who are supposed to have access to the machines are managed here. In addition, the connection of ERP, CRM or other internal company system is possible at any time.

The task of the **SBI-Hubs** is to coordinate the operation of a connection between the service technician, the machine manufacturer or the manufacturer of machine components and the machine. They are the nodes in the system and the global interfaces for the components defined in the SBI-Core. The SBI-Hub is the interface that establishes a secure connection between the SBI-Box, e.g. the machine(s) and the service technician through state-of-the-art encryption technology. It enables remote service and support. The connection can only be authorized via the SBI-Box. This ensures that no running processes are disturbed or even interrupted. In addition, logging of actions on the SBI-Hubs are performed both as an audit log and a video log. The logs are labelled and invariably stored in the SBI-Core.

For SMEs, it may be interesting to install multiple SBI-Hubs. There should be at least two independent hubs in different locations so that even if a hub or network

connection to that hub fails, it will still be able to reach the SBI-Box to service it. Depending on the distribution of its machines, it may make sense to install additional hubs in the countries where a large number of machines of the machine manufacturer are used.

The **SBI-Boxes** set up at the end user take over several functions. They are primarily used as a gateway to the connected machines. In addition, they can act as a firewall with additional functions and tasks. The goal is to unify corporate networks through unified ports (RJ45).

The SBI boxes are provided with IoT layers to enable IoT data collection and analysis. Another feature of the SBI boxes is a secure and fast initial installation as well as remote provisioning and maintaining. Even if the locally existing LAN or WLAN is out of service, this can be ensured by using mobile connections.

The SBI-Boxes can be configured redundantly. This can be done either through a second SBI-Box or through a slightly less expensive box that only acts as firewall and gateway. In the event of a defect, this emergency box takes over the connections of the SBI-Box within just a few seconds and thus enables maintenance of the ongoing operation.

The complete configuration of the SBI-Boxes will be done in the SBI-Core. The SBI-Boxes itselves are delivered only with a unique certificate and will receive the provisioning remotely while the SBI-Box will be switched on at the customers side. No configuration has to be done anywhere else.

The technician is the last component in the SBI concept and the one who works in this system and can carry out remote maintenance on the machines. This is only possible if he is certified and the permissions have been defined in the SBI core. This also ensures that a third party technician only gains access to the components a technician is allowed to and does not gain access to the entire machine network. The connection of a technician to the customer network must be explicitly authorized at the customer by activating the VPN connection to the SBI box or via a user interface. For security reasons, the access of the technician is also displayed via an USB traffic light.

### 6.1.2. Components

- Overview

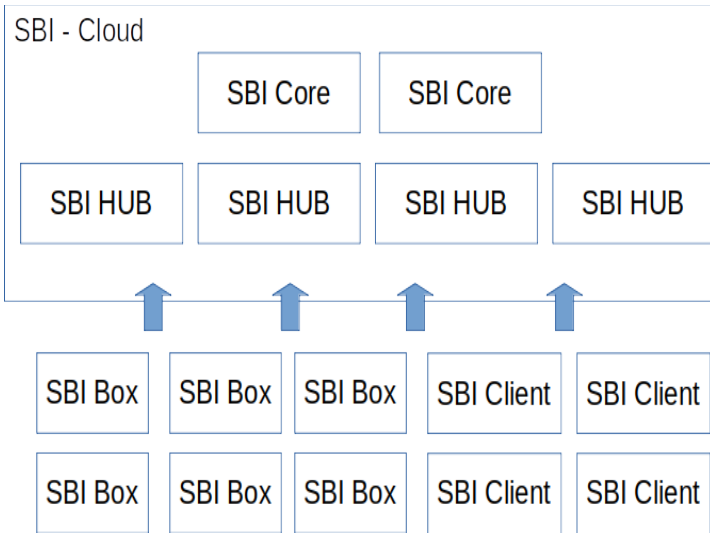


*Figure 4: Components of the SBI-connected virtual factory*

- SBI-Core Server

The SBI-Core system bases on a virtual Linux machine and is designed to be hosted in customers data centres. It can be implemented redundantly and is the central configuration and update unit for all clients. Also the remote client will be managed by the SBI-Core system and supports different APIs to connect additional company services e.g. user and group management over existent AD or LDAP services.

**Table 6: SBI-Core Requirements**

| SBI-Core Requirements | |
|---|---|
| virtual machine | yes |
| cores | 1-2 |
| RAM | 4-8 GB |
| line speed | min. 100Mbit |
| redundancy | yes; minimum two systems |
| operating system | any Linux distribution |
| license costs | €0 |
| monthly costs | €50-€80 |

- SBI-HUB Server

The SBI-Cloud consists of several SBI-HUB systems. The systems can be deployed on virtual environments in company internal or external structures. At minimum two HUBs must be implemented, controlled and managed by the SBI-Cloud system. The SBI-HUBs can be scaled up and down during running operation. The management of the HUBs is controlled by the SBI-Core system. Pending on the available line speed and the required transfer rate per remote session, the system can handle 100 to 1000 concurrent systems. One single HUB can handle 1000 to 5000 concurrent VPN connections to transfer minimum process data. RAM and line speed influence the amount of concurrent sessions significantly.

**Table 7: SBI-Hub Requirements**

| SBI-HUB Requirements | |
|---|---|
| virtual machine | yes |
| cores | 2 |
| RAM | 8 GB |
| line speed | min. 100Mbit – 1Gbit (depends on the amount of concurrent connections) |
| concurrent connections | 100-1000 |
| redundancy | mandatory (minimum three systems) |
| operating system | any Linux distribution |
| license costs | €0 |
| monthly costs | €80-€120 worldwide |

- SBI-Clients

The SBI-Cloud can be entered by the SBI-Box and the SBI-Client. The SBI-Remote Client is based on OpenVPN connections and requires an OpenVPN client on the operating system. OpenVPN is implemented in open source on any standard operating system. The installation and rollout is simple and can be managed central. The required update-system and version control cannot be managed from the SBI-Cloud system. Insecure client versions can be managed and locked out by the SBI-Cloud system.

**Table 8: SBI Remote Clients**

| SBI-Remote Clients | |
|---|---|
| operating system | Linux, BSD, Android, iOS, Windows |
| line speed | 3G-4G, ADSL |
| installation requirements | administration rights (depending on the operating system) |
| required software | secure web browser, Firefox recommended |
| license costs | €0 |
| monthly costs | €0 |

- SBI-Box

The SBI-Box is the connection between the machine network, the company network and the SBI-Cloud system. The SBI-Box system can operate in two modes. In the remote control mode a redundancy is not required. In case of the firewall/gateway mode, the box system should be implemented highly available. In both modes the system connects to the next and fastest SBI-HUB using different connection methods. By default the systems use the LAN connection of the customers network. To support first installation, remote configuration and life-cycle-management, all systems are configured with 4G/5G modems with global SIM cards.

The SBI-Box is available as a fat gateway system with the possibility of hosting virtual machines as well as a small reduced redundant system to keep alive highly available functions (e.g. firewall, remote connection, logging).

The fat SBI-Box system has integrated VPN functionalities and a physical switch to enable external connectivity. An industrial USB traffic light displays different modes in three colors. A virtualization layer is available on this system with different standards. It can be configured from a low level security virtualization host (e.g. Docker or simple change root environments) up to high security open source hypervisors (e.g. KVM and XEN).

The combination between the small SBI-Box as redundant system with the fat SBI-Box system with more system resources for a virtualization layer or the small

SBI-Box as a simple remote service box give the user full freedom to operate and to build up their own customized solutions.

The SBI-Box is construed with the following connectors

- machine connection: minimum 3x RJ45 (gateway function to the machine, heartbeat connection between SBI Box and failover GW), additional RJ45 for more machines are reasonable
- USB port for service connections (only connection of authorized USB media for security reasons enabled)
- SBI-Box connector: for communication directly with other SBI-Boxes (disconnection could lead to significant disruptions during operation and should be avoided)

SBI-Boxes provide the necessary mechanism to make it impossible to connect unauthorized USB media with third-party software or malware. The connectors can be used to connect a screen and input devices for maintenance on site.

**Table 9: SBI-Box Requirements (Fat Box)**

| SBI-Box Requirements (Fat Box) | |
|---|---|
| system as virtual machine | no |
| CPU | Intel Core i5-6300U, 2-Core 2,4 GHz |
| LAN | 6 x 1Gbit |
| RAM | 8-32GB |
| modem | 4G / 5G |
| case | DIN rail mounting, passive cooling |
| redundancy | In combination with small SBI-Box |
| operating system | Debian |
| hardware costs | €1.700 |
| monthly costs | €0 |

**Table 10: Fail-over SBI-Box Requirements (Small Box)**

| Fail over SBI-Box Requirements (Small Box) | |
|---|---|
| system as virtual machine | yes |
| CPU | Intel Celeron J3160 |
| LAN | 4 x 1Gbit |
| RAM | 8-16GB |
| modem | 4G / 5G |
| case | DIN rail mounting, passive cooling |
| redundancy | In combination with fat SBI-Box |
| operating system | Debian |

- Software

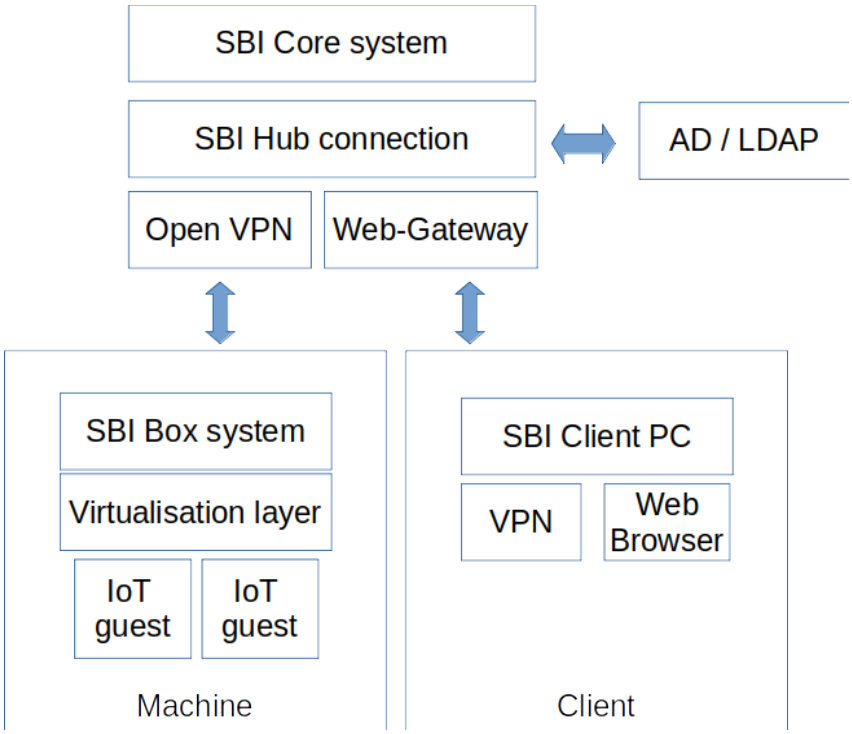


*Figure 5: SBI connected virtual factory – software overview*

The SBI-Cloud is fully based on open source components and provides in its concept trust and transparency. All components are based on Linux Debian and can be ported on different distributions. Following components are used for integration of the SBI modules:

- **SBI-Core:** The core of the system is based on Debian 10, which hosts a PostgreSQL database and a python/django based framework as back end and a web-based front end. The web services are distributed by apache2. The PostgreSQL can optionally be expanded to an database cluster spread to several data centers. The network stack of the core system is based on OpenVPN server and nftables. The log system is based on rsyslog services and extended with several extensions.
- **SBI-Hub:** The SBI Hub system is also based on Debian 10 Linux distribution. OpenVPN is used for the connection between the core system and the client SBI boxes. It is used in the server mode as well as in the client mode. For simple and easy to use connections (e.g. read only connections, visual monitoring and logging) Guacamole server is used for X11, RDP, VNC and SSH sessions. All programs are developed in python. The network stack is based on nftables, The log system is based on rsyslog services and extended with several extensions.
- **SBI-Box:** The SBI-Box is based on Debian 10 Linux. The main logic of the SBI system is in the core and the hub system. The SBI-Box itself is operating with a view subsystems. OpenVPN clients are used for the different tunnel systems to the SBI-Hubs. They are able to handle tunnel in tunnel solutions. A python/django system provides local web services hosted by an apachew server. Nftables are used as firewall in the network stack. On top the SBI-Box provides XEN, KVM and Docker for different types of subsystems.
- **SBI-Box with fail-over solution:** The small SBI-Box is similar to the fat box and based on Debian 10 Linux. The main logic of the SBI system is in the core and the hub system. The SBI box itself is operating with a view subsystems. OpenVPN clients are used for the different tunnel systems to the SBI hubs. They are able to handle tunnel in tunnel solutions. A python/django system provides local web services hosted by a apachew server. Nftables are used as firewall in the network stack. On top the SBI-Box provides XEN, KVM and Docker for the different types of subsystems.
- **Machine to machine communication through tunnel in tunnel solution:** To realise the connection of two machines over the SBI-Cloud, each SBI-Box is connected via OpenVPN to the next SBI-Hub. To connect the machines to each other, a second VPN tunnel is build up between two boxes. Both systems try to reach each other and both are working in server and client mode.

The following open source tools and distributions were evaluated and used within the project:

**Table 11: Used Open Source components**

| | Components | Description |
|---|---|---|
| virtualization | XEN<br>KVM | used for SBI-Core and -Hubs as well as virtualization stack on the SBI-Boxes |
| container | Docker | IoT layer for data collection and data analysis |
| firewall | Nftables<br>OPNSense | both can be combined with IDS/IPS Suricata<br>OPNSense is intended only for security purposes without remote maintaining |
| encryption | OpenSSL<br>3DES<br>AES<br>RC5<br>Blowfish | OpenVPN in combination with various encryption variants, all of which offer 256-bit encryption |
| remote maintaining | Guacamole | Provides the most common protocols (X11, VNC, RDP, SSH) to establish connections to a client and the recording and storage of video logs. The system provides read only and full connection mode. |
| digital twin/broker | Kafka (Apache) | Allows communication between multiple machines without the machines having direct contact. The broker collects data from so called sensors, so-called subscribers retrieve the data. The broker is only the mediator (collects the information and makes it available), there is no direct access to the sensor (e.g. a machine) |
| logging | Guacamole | All external connections are recorded in an audit log so that every action of the SBI-Boxes, of the technicians and of the connected devices or of the machines can be traced. Video logs are created on the SBI-Hubs because they represent the interface between the technicians and the SBI-Boxes. |

The basic costs for the cloud servers starts at monthly cost of Euro 300-500 plus internal or external service costs. Also the scaling factor is manageable and affordable. Through the additional features (remote services and access) and a high level of additional security, the customers are willing to pay for these additional services. To offer an own cloud will be an additional business model.

| |
|---|
| The SBI system demonstrates that every SME can build up own IoT cloud system. Even at a small amount of customers (10-20), the configuration is reasonable. |

- Network

For the implementation of the SBI concept, it must first be determined in which network type the SBI-Boxes should be used later. It is therefore necessary to clarify whether one operates a pure IPv4 or IPv6 network, or whether a dual operation of the two network types must be performed. Within a pure IPv4 network, there should be no major problems, as software used in the enterprise basically masters this.

The situation is quite different if the SBI-Boxes are to be operated within an IPv6 network. Here it must be analysed very precisely how the existing network is structured, which machines and devices are installed and ultimately which software has to communicate over the network.

**IPv4**

With IPv4, there should be no technical problems with the implementation. It should be noted, however, that the address space used by the interfaces of the SBI-Boxes is available within the company. Depending on the size and structure of the companies, problems can arise here that should actually be remedied by a sensible subdivision of the address space. The solution is provided by the address spaces listed in Table 12.

**Table 12: Possible IPv4 adress ranges for the use in a SBI-system**

| Adress Range | Specification | Largest CIDR-Block | Number of IP addresses |
|---|---|---|---|
| 10.0.0.0-10.255.255.255 | private, 1 8-Bit | 10.0.0.0/8 | $2^{24}$=16.777.216 |
| 172.16.0.0-172.31.255.255 | private, 16 16-Bit | 172.16.0.0/12 | $2^{20}$=1.048.576 |
| 192.168.0.0-192.168.255.255 | private, 256 24-Bit | 192.168.0.0/16 | $2^{16}$=65.536 |

### IPv6

The main problem with the "transition" is that the change from IPv4 to IPv6 takes place over decades with the effect that Internet users all around the world are affected in different degrees.

There are different mechanisms for each scenario, some of which are only needed to be activated and partially manually configured. Transitional procedures play an important role. As more and more Internet service providers and companies switch to real IPv6 in the future, the transitional procedures should not disappear altogether, but at least decrease. In general, all transitional procedures should be seen as a temporary solution on the way to IPv6-only. It will be several years before IPv6 is fully used.

Another problem is the lack of IT experts who are already familiar with the configuration of an IPv6 network. Most companies still use IPv4 internally and shy away from switching to IPv6, mainly because they also use some software that may not be IPv6-compliant. Devices and machines may also only be compatible with IPv4. Before a complete switch to IPv6, companies have to do a lot of considerations.

The basic idea of IPv6 is that it works across all transmission systems. For example, also over IPv4. In general, two routers are the endpoints for the tunnel. The latency of the infrastructure must be added to the round-trip time of tunnelled IPv6 bundles. This can be a problem for some applications.

### Dual Stack

With dual stack, each public or private IPv4 address network node runs in parallel with a global IPv6 prefix. Dual Stack is not to be confused with Dual Stack Lite, the latter is just a special operating mode for a broadband connection.

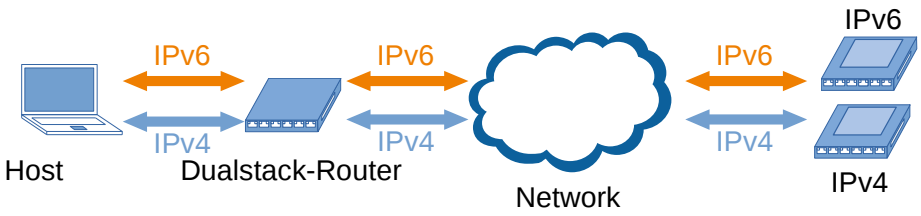


*Figure 6: Dual Stack*

Basically, "dual stack" means that IPv4 and IPv6 can be used in parallel on the same connection. Whether NAT takes place in the end customer router (typically in the DSL connection) or whether the NAT is carried out by the mobile service provider is completely irrelevant. Because IPv4 is always NATed, Dual Stack makes no distinction as to whether a port has a private or public IPv4 address.

### Dual Stack Lite

"Dual Stack" is the term for IPv4 / IPv6 parallel operation whereas "Dual Stack Lite" is a tunneling technique that describes an Internet connection where a global IPv6 address exists and IPv4 bundles are tunnelled in IPv6.

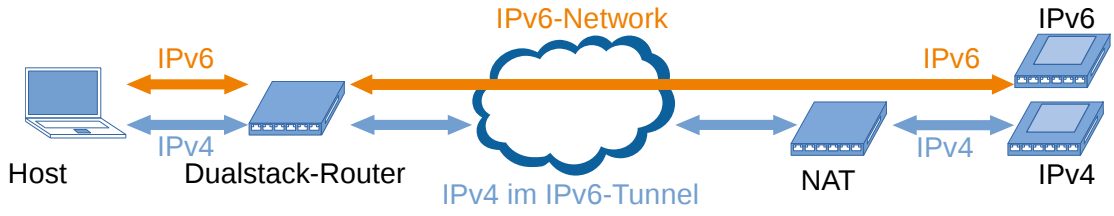


*Figure 7: Dual Stack Lite*

The distinguishing feature of Dual Stack Lite is that provider have no IPv4 networks, but only IPv6 networks. Each participant receives a global IPv6 prefix. In order to also be able to transmit IPv4 traffic, the outgoing IPv4 bundles in the end customer router are provided with a private IPv4 address and tunnelled via a 4in6 tunnel into the public IPv4 network. Each IPv4 bundle receives a new IPv6 header. Between the private provider network and the public IPv4 network provides carrier-grade NAT (CG-NAT). The responsible NAT server is at the provider and takes

care of the address translation between the private and public IPv4 addresses and then passes the bundles on the public IPv4 network.

Another feature of Dual Stack Lite is a B4 component in the end-user router (CPE) that transports IPv4 traffic over IPv6 to an Address Family Transition Router (AFTR) device that routes traffic to the IPv4 Internet. If the provider assigns private IPv4 addresses to its end customers, then the provider's tunnel endpoint is routed via carrier-grade NAT to the IPv4 Internet.

With DS-Lite, the customer's network access router does not get a public IPv4 address, but a private IPv4 address. This means that the customer first receives a public IPv4 address via Carrier Grade NAT. This has significant disadvantages. Some network and Internet services do not work on Dual-Stack Lite if no public IPv4 address has been assigned. A real problem is when IPv6 is not yet supported by this service.

### 6in4 Tunnelling

When tunnelling with "6in4", the clients in the local network must have IPv6 addresses and also the servers in the Internet must be reachable at an IPv6 address. In addition, two routers or gateways must be in dual-stack operation between the client and the server. So dominate both IPv4 and IPv6. The first dual-stack router generates IPv4 bundles containing the IPv6 bundles. Via the IPv4 network, the IPv4 bundle arrives at the last dual-stack router, which retrieves the IPv6 bundle from the IPv4 bundle and forwards it to the IPv6-capable server.


*Figure 8: 6in4 Tunnelling*

Specifically, this means finding someone who has IPv6 connectivity. For example, a tunnel provider or tunnel broker. With this one agrees on how the tunnel should come about (protocol) and can then assign a prefix (address assignment).

### 6to4 Tunnelling

"6to4" is a tunnelling method that is only interesting to reach IPv6-only services. And 6to4 only makes sense if a public IPv4 address is available. In general, companies need to enable "6to4" if they want to address services that can only handle IPv6.

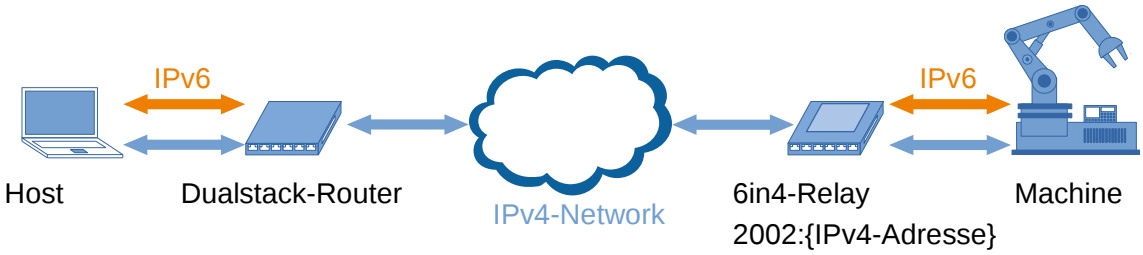


*Figure 9: 6to4 Tunnelling*

For "6to4" the entire IPv6 address space "2002 :: / 16" is reserved. This makes it possible to convert all public IPv4 addresses into a globally valid IPv6 address if required. The IPv6 address is returned in the form "2002: {IPv4-Address}". The IPv4 address is converted to hexadecimal notation. Then the bundle content can be transmitted in an IPv6 bundle.

This means that anyone who has a public IPv4 address automatically also has an IPv6 address. If the IPv4 address changes, the IPv6 address will automatically change too. The question is, where are the IPv6 bundles tunnelled? What is the IPv4 destination address? The router tunnels to the IPv4 anycast address "192.88.99.1". This means that somewhere there is a gateway that unpacks the IPv6 bundle from the IPv4 bundle and forwards it into the IPv6 network. The way back just works in the opposite direction. The IPv6 bundle goes to any gateway that packs the IPv6 bundle into an IPv4 bundle and forwards it to the specified IPv4 address in the IPv6 address.

### 6over4 Tunnelling

"6over4" works much like "6to4". At "6over4" an IPv6 address is formed in the form "fe80 :: {IPv4-Address}". The IPv4 address is used in hexadecimal notation. The IPv6 bundle with the link-local address is then embedded in IPv4 and transmitted over an IPv4 multicast network.

However, this tunnelling process is less frequently used because of throughput and security issues. The simpler and more practical tunnelling methods "6in4" and "6to4" are much more common than "6over4".

### 4in6 Tunnelling

With "4in6" the principle of "6in4" is reversed. It is necessary if you want to transport IPv4 bundles in an IPv6 network. For this one needs an IPv4 client and IPv4 server and two routers in dual-stack mode. In the client-side dual-stack router, the IPv4 bundle is packed into an IPv6 bundle, transmitted over the IPv6 network, and unpacked at the last dual-stack router. From there, the IPv4 bundle is forwarded to the IPv4 server.


*Figure 10: 4in6 Tunnelling*

### Protocol translation DNS64 and NAT64

DNS64 ([11]) and NAT64 are about accessing an IPv4 server with an IPv6 client. There is practically a translation between internal IPv6 addresses and external IPv4 addresses. The IPv6 client queries a DNS64 server for the IPv6 address of the IPv4 server. Because the server does not yet have an IPv6 address, the DNS64 server converts the server's IPv4 address to an IPv6 address, much like 6over4 and 6to4. Then the DNS64 server tells the client the IPv6 address that sends the IPv6 bundles to the NAT64 gateway. The NAT64 gateway, in dual-stack operation, detects the IPv4 address in the IPv6 address, generates a new IPv4 bundle and forwards it to the IPv4 server. The answer bundles take the opposite route.

The advantage of protocol translation with DNS64 and NAT64 is that the IPv6 client does not need to know that it is connecting to an IPv4 server.

The downside is that you need public IPv4 addresses that may not be available. As is typical for NAT, the individual internal IPv6 clients are distinguished by port numbers. In this way you can then save IPv4 addresses again.

### Protocol translation 464xlat

464XLAT is an IPV4-IPv6-IPv4 translation method for use on pure IPv6 networks. This method is mainly used by mobile service providers and has proven itself there. 464XLAT, described in RFC 6877, allows computers in IPv6 networks to access Internet services that are only accessible via IPv4. The client (the application) uses a client-side translator (Stateless IP / ICMP Translation) to convert IPv4 bundles to IPv6. These bundles are sent to a NAT64 translator on provider side (PLAT: provider-side translator) and translated back. There they can then reach an IPv4 device.

The SIIT translation (CLAT) can be done directly on the client itself using special software or on an IPv4-enabled (W) LAN in front of it, such as a smartphone in hotspot or tethering mode. However, if the LAN itself is connected via IPv4, 464XLAT is not necessary. The NAT64 translator must be able to reach server and client (through CLAT). The use of NAT64 limits the connections to the client-server model with the protocols UDP, TCP and ICMP. Since 464XLAT is a supplement to NAT64 with DNS64, their advantages and disadvantages are essentially also applicable to 464XLAT. Unlike NAT64, 464XLAT also supports services that are restricted to IPv4 addresses (for example, URIs with numeric IPv4 addresses instead of names or software with outdated IPv4-limited programming interfaces).

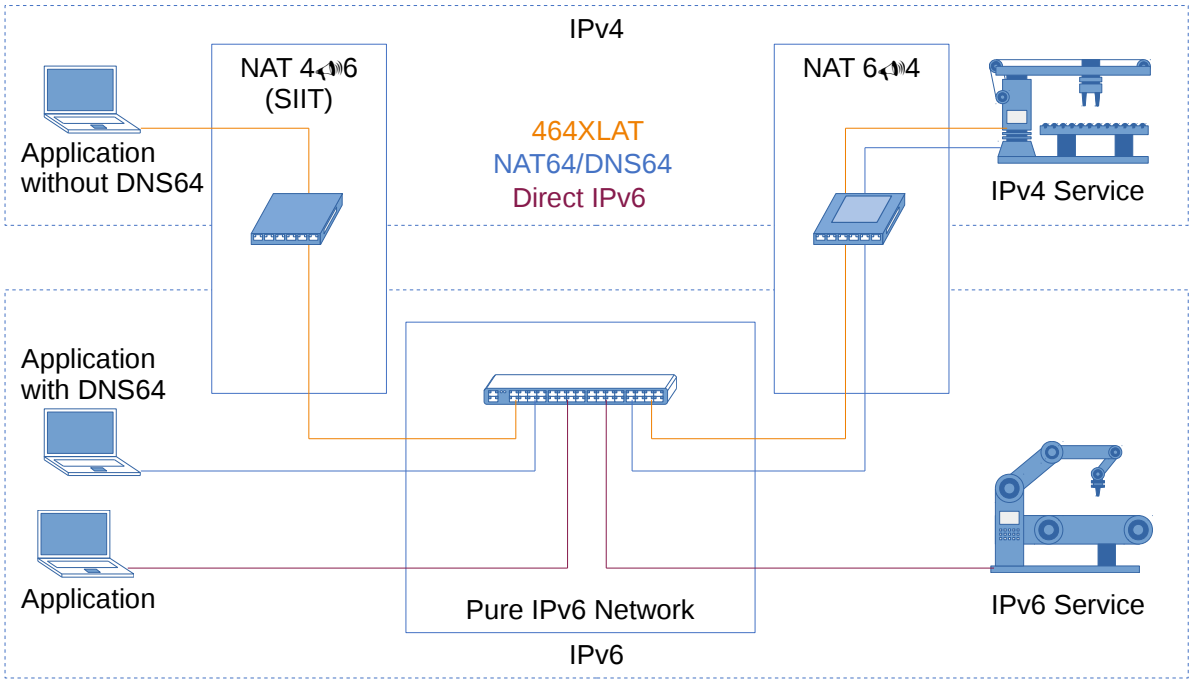


*Figure 11: I464 XLAT Configuration to use IPv4 in a IPv6 network*

An additional disadvantage to NAT64 with DNS64 is the need for an additional service on the client or on the immediate network before (for example on the router). In addition, problems arise from replacing the typically 20-byte IPv4 header of a data bundle with a 40-byte IPv6 header. As a result, a data bundle grows by 20 bytes, which may result in the maximum transmission unit being exceeded. Solutions such as Path MTU Discovery, IP fragmentation or MSS Clamping become necessary.

464XLAT can fix problems ([11]) that DNS64 / NAT64 can cause by violating DNSSEC by using synthetic unsigned AAAA records by using the signed A-record, which is the IPv4 address. This case only occurs when a server only supports DNSSEC but not IPv6 and the client wants to validate. If validated in the DNS64 resolver / cache, the problem is solved without 464XLAT.

### 6.1.3. Demonstrator remote 3D-printing

It was planned to install the demonstrator in a real industrial environment within the end of Q1/2020. Because of the international lock down caused by COVID-19, it was not possible to implement the demonstrator. Salzburg Research and X-Net build up an machine-2-machine communication instead using two 3D printers. They were connected to each other over the SBI cloud. Two SBI-Boxes opened a separated VPN tunnel which connected both subsystems. A Raspberri-Pi system and a camera module control the two 3D printers. If the print on one printer fails (automated detection by the camera), the printing job is copied to the fail over machine and started there.

Both systems were connected to each other, but the administrator of each network was able to access only the own environment. The administrator was further on enabled to connect remotely to his production site.

In another use case the administrator A got access to restricted areas of of the opposite site (e.g. the status of the printer or access to the camera). This was controlled and monitored by the SBI cloud system and not by the application itself.

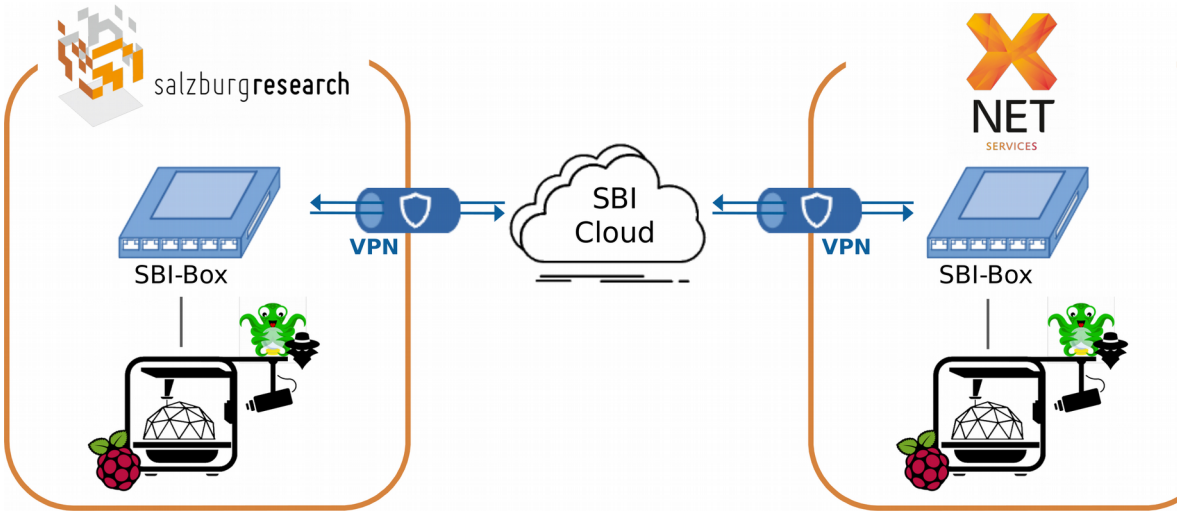


*Figure 12: Digital Twin demonstrator*

Within the SBI demonstrator, several functionalities were tested and demonstrated. The following table gives an overview about the functionalities.

**Table 13: Demonstration of SBI 3D-printing**

| Demonstration of SBI 3D-printing | Tested | Successful |
|---|---|---|
| remote implementing | yes | yes |
| 4G and LAN connectivity by remote provisioning | yes | yes |
| 5G connectivity | no | - |
| VPN connection to SBI-Cloud | yes | yes |
| remote service connection to SBI-Box | yes | yes |
| tunnel in tunnel connection between the SBI-Boxes | yes | yes |
| machine2machine communication | yes | yes |
| remote access to partial environments | yes | yes |
| test in real environment of an industrial partner with partial access to specific environments | no | no |

### 6.1.4. Twins

Many variants of a twin in the SBI system are conceivable. The most common twin is certainly the real twin, i.e. a complete replica of the SBI-Box, which takes over the complete tasks in the event of a failure of the main device so that there is no downtime in the network.

The second variant, which is related to the general digitalization of the industry and its products, is the digital twin, whose task is to collect data in order to analyse it for the optimization of processes and products, and later products based on the known data to test and optimize in the planning phase.

The third twin in the system would be a security twin, more commonly known as Honeypot, a virtual machine as a dead end for potential attackers to analyse their attacks without realizing that their attack has already been noticed.

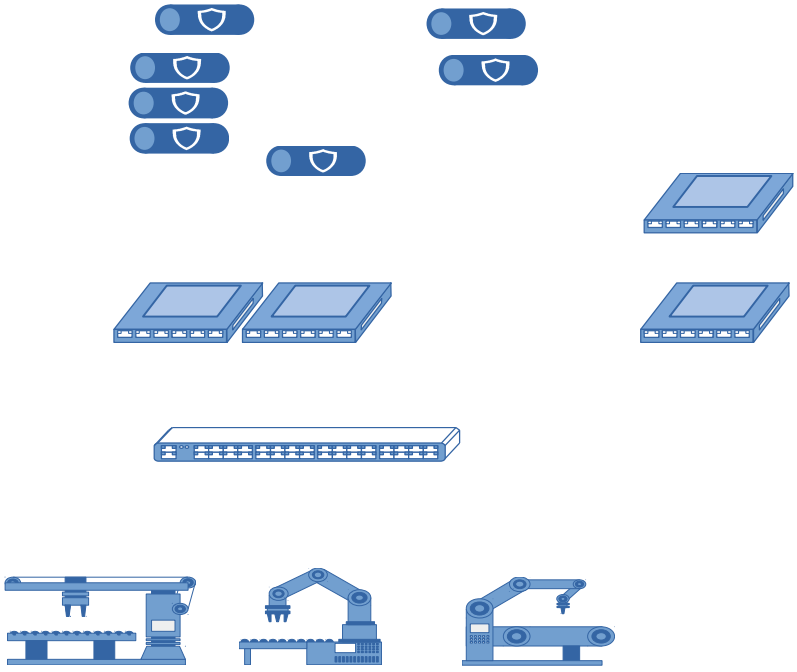

*Figure 13: SBI-Box - Twins*

- Redundant Twin

The company where the SBI-Boxes are used and the redundancy of the other SBI components of the IoT device manufacturer are important for a smooth process. Downtimes can put companies at risk here because they may have major financial losses during this time, but the company's reputation and therefore its value are certainly suffering.

It is therefore extremely important to avoid or at least minimize such downtimes. In most cases, it will not be necessary to install a complete redundant twin of the SBI-Box in the network, but only the most important functions in an emergency box, i.e. the components relevant to security and the network functions will have to

be available. Systems that are only required for data analysis do not necessarily have to be installed for the emergency box.

- Digital Twin (Virtual Copy)

An IoT layer is required for the digital twin. Currently the Digital Twin is only used on the SBI-Boxes in order to digitize the attached industrial devices. But it would also be of interest to generate a Digital Twin of the SBI-Boxes in order to be able to simulate and improve the system in a long term.

A separate virtual server should be configured for data analysis in the sense of security by isolation, which also collects its information from the SBI boxes via encrypted channels and then evaluates the data. This ensures that the digital twin does not come into contact with other relevant systems and has no direct access to sensitive data.

- Security Twin (Honeypot)

Since the system should be expandable by an intrusion detection or even an intrusion prevention system, it is of course necessary to think about how to deal with possible attacks. The easiest way is to lock out a potential and recognized attacker, but this does not prevent them from possibly carrying out further attacks on the system. Especially the SBI-Box, with additional devices and modifications have to be detected again.

Another conceivable option would be to redirect the attacker to a security twin (Honeypot) in the SBI-Box and thus lead it into a controlled cul-de-sac. This security twin could be a virtual twin that enables simulation to capture and analyze the attacker's methods.

From the analysed data, new rules could then be obtained for the IDS / IPS software used, which could then be distributed to all SBI boxes in order to make the entire system even more secure and to prevent future attacks that use the same methods to be able to fight back faster.

### 6.2. SBI Flash Media Recording Demonstrator

Solutions have to consider the protection of each single IoT device, not only now but also in the future. The highest level of security available is the complete individualization of security mechanism, which also includes unique encryption and unique keys. This is the only logical and effective method to secure products against hacking and fraud.

Unique encryption means that each software distribution has its own key and is connected to a specific product. It prevents that this software is used in another product (even in a product of the same batch) or ensures that no other IoT product is affected.

Within IoT4CPS, the 'SBI flash recording demonstrator' was developed to record flash devices directly at the place they are needed: at the manufacturing environment. It can easily be integrated in work flows and processes on-site and supports the error-free correlation of individual content (e.g. software, keys, configurations, metadata) and IoT products.


*Figure 14: SBI flash recording demonstrator*

To be able to assemble each product with unique software (e.g. BIOS, operating system, data, key, certificates) and explicit identifications, it is not enough to only focus on the hardware system that allows individual mass recordings. Also the structures before (content collection, time of delivery of content, matching of data to semi-finished IoT products etc.) and after (validation of data, logging of recording but also of removal, matching during assembling, additional print material, distribution etc.) recording have to be taken into consid-

eration. It is not about copying data to media (USB flash device etc.) any more when the output has to be individual.

These processes are considered in the advanced SBI flash recording demonstrator which allows flexible connection of several systems like manufacturing execution systems, document management systems or others and at the same time the automation of processes. The demonstrator is designed to transfer digital content from de-centrally located data sources into IoT products in a secure and customized way. It makes use of secure communication protocols, single encryption and quality control mechanism to take the recording of data carrier to a completely new level. Quality control mechanism avoid errors during production or in the matching of data to the products (e.g. using barcodes).

With the combination of different tools and methods like authentication, encryption, access control, remote access, validation and matching processes, high level security is ensured:

- production of the SBI-Box and secure recording of the flash media
- mechanism to enable secure boot of the SBI-Box
- personalized unique encryption by the means of product-specific indicators
- personalized and secure token preparation for commercially available flash devices which enables secure access to the SBI VPN
- explicit identification of user
- recording of USB flash drives for service technicians that can connect to the SBI-Hub with the corresponding certificate
- mechanism to match the media to the corresponding products
- validation of data using MD5 or SHA methodology
- asynchronous recording mechanism and status overview (finished media, faults, logs)
- data protection mechanism (for the whole life cycle of an IoT product)
- secure remote management during and after recording processes

To secure data and keys not only on the USB flash device but as well during production, the SBI flash recording demonstrator supports secure data transfer and communication and provides authentication mechanism. Access during production is controlled and logging provides all relevant information to reconstruct recording

processes. Product reliability and quality control mechanism are integrated and ensure error-free recording and assembling/distribution.

The SBI flash recording demonstrator consists of hardware, software and interfaces. By using open source components, functionality and processes are transparent and offer high security. A modular system architecture allows individual customization of hardware and software components and the integration in different environments. It is therefore ensured that the solution is flexibly adaptable to the individual needs of factory and supports each level of digitization.

The SBI flash recording demonstrator shows a way how to produce decentralized and keep the secret of the software in the hand of the product owner. The system is based on an individual encryption for each product. Under these circumstances the sources of the software part must be transferred to secure areas (the SBI flash copying systems). The transfer and versioning system is controlled by an SBI cloud system.

SBI flash copying systems are positioned on each production site and provide a secured storage of data. During the production, individual data sets are generated for each product. The SBI flash recording demonstrator encrypts every data set with a unique key that is generated out of the product itself. The flash media will only run on the unique product it is produced for. Due to logging mechanism and access control, the content owner has an exact overview about who produced which media at what time.

Individual encryption for each produced gives the product owner the possibility to outsource production sites even if the situation in these countries are not save or not trustable.

To visualize the functionalities, an example application is described in the following: An European sewing machine producer is forced to expand the production to US and China to be able to serve the local market there. As in other areas, the know how and USP of the sewing machines moved from the hardware parts to the software. Software, firmware and IoT functionalities must be protected on a high level to prevent from reverse engineering.

A very effective method to protect all software parts is individual encryption, but the credentials of a machine, on-site production and assembling and the data

sources have to be considered. In the example, the unprotected binaries for the firmware and IoT connectivity are stored at the headquarter of the sewing machine producer. In a synchronization process, the data is copied to a protected storage of the SBI flash recording system. The SBI flash recording system is located at the external production site (e.g. in China), but the local staff of this production site has no direct access to the unencrypted stored data.

Checkpoints during the manufacturing of a sewing machine are defined. When they are reached, the credentials of a machine are transferred to the local SBI flash recording system. The system connects to the headquarter to go ahead for production, as key and certificates for each single sewing machine are generated in the headquarter. As soon as the outsourced SBI flash recording system and the local manufacturing process is ready for recording, key and certificate are transferred to the local SBI flash recording system. The system copies the certificate to the firmware image and encrypts it individually. Afterwards, the image is recorded on a flash media and verified. Only in case of positive verification, the X5 system prints the required label and informs the worker in which slot the corresponding flash media is placed. The worker takes the flash media, labels it and assembles it into the sewing machines. All single steps are protocolled and sent to the master system in the headquarter.

During the initial operation of the sewing machine, the boot loader collects the individual credentials from the machine, builds the key and encrypts the flash controller for booting. To connect the sewing machine as an IoT device, a product specific certificate is used to e.g. enable secure https connections or remote VPN tunnels to an SBI-Coud. In case of a security hack, single sewing machines can be blacklisted and easily excluded.

### 6.2.1. Components

- Hardware

The setup of the hardware allows individual configurations. Especially the number of modules, the type of slots and additional systems like touch screens, printer or scanner can be assembled individually depending on the needs of a factory. The following hardware components give an overview about the configuration of the test-bed, which was developed in the project and represents a common use case:

- Chassis including fan: 500 x 405 x 45mm
- 2 copy modules with 10 USB slots each and 3 colored LEDs at each slot to display the status of each slot optically (no need for a screen)
- adapter circuit board: each slot is equipped with an adapter circuit board that allows the connection of any possible media type (SD, USB3.0) to USB-C
- controlling circuit board: controls the LEDs and each adapter circuit board
- USB-C card PCI-E x8: the industrial card is used to reach high speed
- 1x Intel Core i7-9700, 8-Core, 3,00GHz 12 MB
- CPU cooling NH-L9i
- 1x 16 GB DDR4-2400 SO-DIMM 2 Rank Crucial (1x 16384 MB)
- 1x 1 TB Samsung SSD 970 PRO (M.2 PCI-E x4 2280)
- 1x Delock MiniPCIe I/O PCIe full size 1 x 19 Pin USB 3.0 Pin Header
- 17" rackmount display: full HD, LED Screen, DVI & VGA inputs, resistive touchscreen
- slot to plug in a label printer
- network connection

- Software

The software was fully developed using open source tools. The programming language is Python3, the most important libraries are

- python-bottle: provides the REST-API
- django: provides the connection of the database
- pillow
- reportlab: supports the label generation

The operating system is Ubuntu 18.04 LTS 64bit.

The free and open source relational database management system postgreSQL is used for the database in the back-end and provides the traceability of any produced media. It stores all relevant information about a job, data, date and time, success, faults, etc.

The following figures give an overview about the structure and architecture of the software:

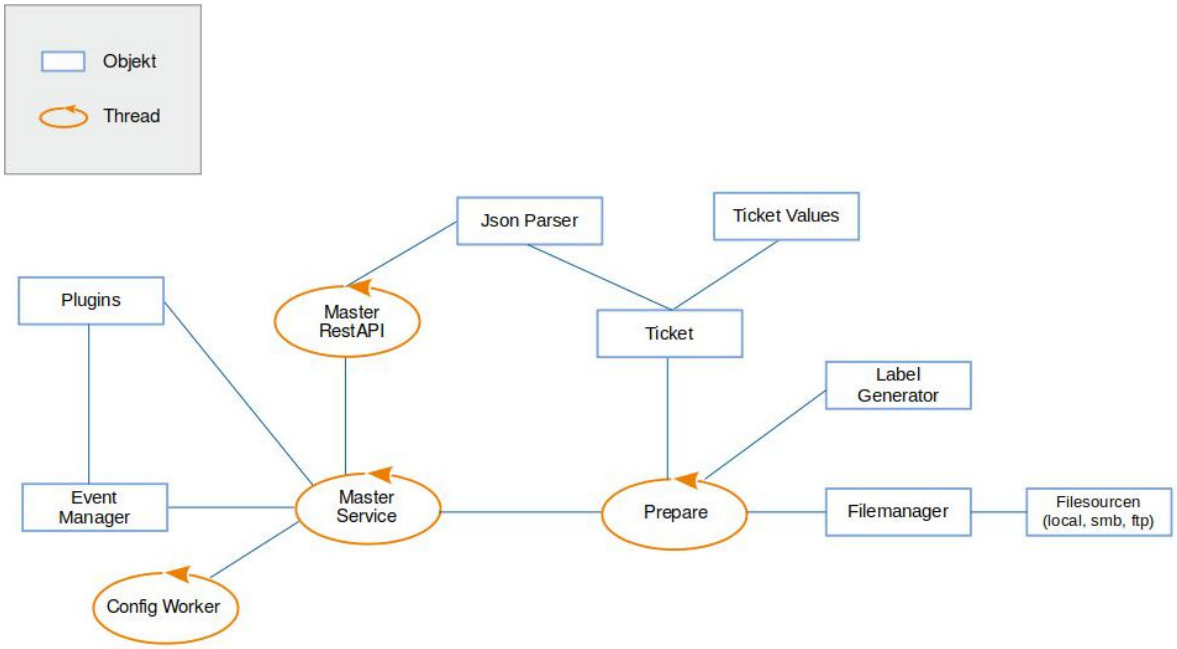


*Figure 15: SBI flash recording demonstrator master system*

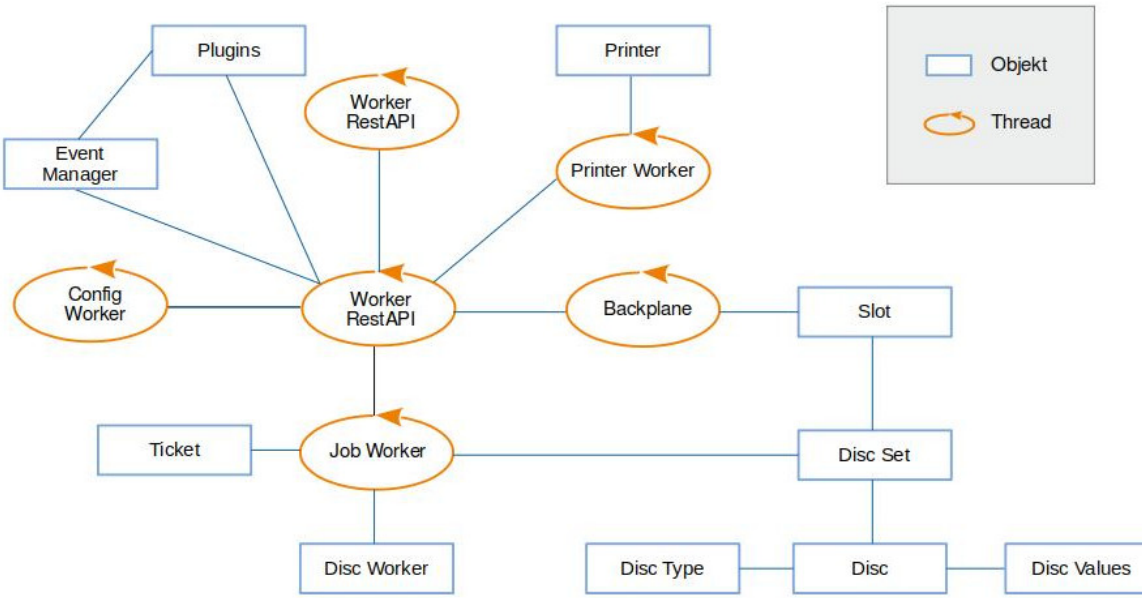


*Figure 16: SBI flash recording demontrator working system*

The following configurations are available:

- number of max. tickets cached per module, max. running tickets
- clean up of database and data (days after finished ticket, faulty tickets are deleted)
- email settings (hostname / IP, TLS, ...)
- printer settings (label printer: dimensions, color, font)
- user settings

The software supports several processes and work flow in factory, as several sources, targets and methods can be chosen. This enables e.g. the separation of the location of the hardware and the controlling or de-centralized data sources. Jobs to start recording processes can either be generated using the web-interface directly on the hardware (touch screen) or on a network attached PC. Job tickets can also be created automatically using the existing interfaces. The following information is defined in these tickets:

- number of copies (no limitations)
- type of device(s): a ticket must have one or more targets. A target is always a device (e.g. USB or SSD). A ticket has multiple targets if a multiadapter is used (e.g. SSD and two SD adapter).
- data source: there are currently five sources supported. The local filesystem ("*local*"), FTP ("*ftp*"), SMB ("*smb*"), NFS ("*nfs*") and FTPS ("*ftps*") servers.
- verification method: two possible values for the verification (md5 hashes, sha hashes) are available.
- label: the label section is optional, depending whether a label print is specified in the settings or not. When set, a label is automatically printed for each device after the copying process. These settings are defined in the block "*label*" of the JSON file.
- device: optionally the ticket can define the modules and slots that are used for recording. If no device is specified, a free slot is chosen.

- Interfaces

The SBI flash recording demonstrator uses REST-API and JSON

- REST-API: provides all information about the systems and enables status requests, e.g. of the whole system, modules, slots or even a single medium. It allows the connection of other systems like manufacturing execution systems, enterprise planning systems or document management systems. They can e.g. retrieve the degree of capacity utilization of each SBI flash recording system or control recording (which media is recorded at which time and on which slot), which enables timely finishes without the need of stock holding.
- JSON: allows the exchange of data (tickets are e.g. sent via JSON)

A web-interface enables manual control and starting of recording processes. The web-interface can be used on-site with the integrated touch screen, network attached PCs or over the internet using secure connections. This enables the connection with mobile device or the secure controlling of externally located SBI flash recording systems.

The web-interface provides an overview, status of single modules and slots, limited configuration for system parameters and user administration.

## 7. Conclusion

During the project IoT4CPS, test-beds to secure IoT products and for a secure set-up of production environments demonstrated functionalities for the industrial manufacturing and satisfy the needs of IoT. The next steps in direction to Industry 4.0 will be the development of solutions for the “Shared Level” (see figure 1 for further details), which brings several standards and systems in interaction.

There must not be one standard, one cloud and one system for all. We have to learn out of the mistakes of the past during the digitalisation in the private environment. Open source and transparent solution which give the opportunity to implement high security levels into the environment of companies have to be used depending on individual needs. The exchange between the different systems will need global standards, which should be driven by a community model instead a group of some monopolists or single countries.

Similar to standards in the machine 2 machine communication (e.g. OPC Unified Architecture), new exchange standards should control the exchange between different cloud systems for following tasks:

- secure exchange from machine data on demand with the option for anonymization
- secure remote service including encrypted audit logs to save privacy
- possibility to include security provider for maintenance

The outputs of IoT4CPS show requirements of these new standards and point out possible solutions that have the potential to succeed on the market. Though a lot of work has to be done in the next years to provide trustworthy networks and CPU components.

## 8. References

[1] EUROSTAT: Small and medium-sized enterprises: an overview. Online available: https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/DDN-20200514-1

[2] Eurostat : ICT usage in eterprises in 2019. (9-13012020-BP-EN) Online available: https://ec.europa.eu/eurostat/documents/2995521/10335060/9-13012020-BP-EN.pdf/f1060f2b-b141-b250-7f51-85c9704a5a5f

[3] Nick G.: How Many IoT Devices Are There in 2020? [All You Need To Know]. Online available: https://techjury.net/blog/how-many-iot-devices-are-there/

[4] Bitkom e.V.: Industrie 4.0 – so digital sind Deutschlands Fabriken. Online available: https://www.bitkom.org/Presse/Presseinformation/Industrie-40-so-digital-sind-Deutschlands-Fabriken

[5] A. Philipp, Drei wichtige IIoT-Security-Trends 2020. Online available: https://www.infopoint-security.de/drei-wichtige-iiot-security-trends-2020/a22503/

[6] General Data Protection Regulation. Online available: http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv%3AOJ.L_.2016.119.01.0001.01.DEU&toc=OJ%3AL%3A2016%3A119%3ATOC

[7] Telecommunications Act Austria. Online available: https://www.jusline.at/gesetz/tkg

[8] Commission Implementing Regulation (EU) 2018/151. Online available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R0151&qid=1562582916048&from=EN

[9] https://epdf.pub/functional-safety-iec-61508-stds.html

[10] RFC2473 Generic Packet Tunneling in IPv6 Specification; Online available: https://www.rfc-editor.org/info/rfc2473

[11] RFC 6147 DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers; Online available: https://www.rfc-editor-.org/info/rfc6147

[12] Open Web Application Security Project, Top 10 Internet of Things 2018

[13] ET Open Rules for Suricata. Online available: https://rules.emerging-threats.net/open/suricata/rules/