# CyberFactory#1

## T2.3 Misuse-Cases

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Revised By</th>
<th>Approved By</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.0</td>
<td>16/01/2020</td>
<td>Murat Lostar</td>
<td></td>
<td>Consolidated first version (break out documents have their own change control)</td>
</tr>
</tbody>
</table>
Table of Contents

1 Introduction .............................................................................................................................................. 4
  1.1 General Misuse-Case Information ................................................................................................. 4
  1.2 Misuse-Case Development Methodology ..................................................................................... 4
  1.3 Risks Overview ............................................................................................................................... 5

2 Misuse-Cases on Electronics use-case ................................................................................................. 7
  2.1 Vestel Use-Case Overview ................................................................................................................ 8
  2.2 Vestel Misuse-Case Overview ......................................................................................................... 9
    2.2.1 Misuse-Case 1: Service interruption of AGVs .......................................................................... 9
    2.2.2 Misuse-Case 2: Abnormal behaviour of IoT devices ................................................................. 9
    2.2.3 Misuse-Case 3: Unauthorized Access to Computers and Servers .......................................... 10
  2.3 Electronics Misuse-Case – Detailed Review .................................................................................. 12
    2.3.1 Misuse-Case 1a – Service Interruption of AGVs (Functional driven) ...................................... 12
    2.3.2 Misuse-Case 1b – Service Interruption of AGVs (Security driven) .......................................... 13
    2.3.3 Misuse-Case 2a – Abnormal Behaviour of IoT Devices (Functional Driven) ........................... 16
    2.3.4 Misuse-Case 2b – Abnormal Behaviour of IoT Devices (Security Driven) ............................ 17
    2.3.5 Misuse-case 3a – Disclosure and alteration of company confidential data (Security Driven) 20
    2.3.6 Misuse-case 3b – Installation of Malware (Security Driven) ..................................................... 21

3 Misuse-Cases on Bittium use-case .......................................................................................................... 26
  3.1 Bittium misuse Case – Detailed Review ........................................................................................... 27
    3.1.1 Misuse-Case 1. Data manipulation at Bittium manufacturing or partners .............................. 28
    3.1.2 Misuse-Case 2 Industrial espionage via Secure Product Commissioning ................................ 33

4 Misuse-Cases on “CPS-based manufacturing on auxiliary automotive industry” use-case ............................................................... 39
  4.1 “CPS-based manufacturing on auxiliary automotive industry” Use-Case Overview .................. 40
  4.2 "CPS-based manufacturing on auxiliary automotive industry" Misuse-Case Overview ............. 42
  4.3 “CPS-based manufacturing on auxiliary automotive industry” Misuse-Case – Detailed Review .................................................................................. 45
    4.3.1 Misuse-Case 1a – Wi-Fi network interruption affecting cobot fleets (Functional) .................. 45
    4.3.2 Misuse-Case 2 – Wireless Sensor Network (WSN) affecting indoor tracking systems .......... 50
    4.3.3 Misuse-Case 3 – Cybersecurity-related services misbehaving .............................................. 55

5 Misuse-Cases on InSystems Automation GmbH use-case ..................................................................... 60
  5.1 InSystems Use Case Overview ........................................................................................................ 61
  5.2 InSystems Automation Misuse-Case Overview ............................................................................. 62
  5.3 InSystems Automation Misuse-Case – Detailed Review ................................................................ 64
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.3.1</td>
<td>Misuse-Case 1 – Misbehaving Robot</td>
<td>64</td>
</tr>
<tr>
<td>5.3.2</td>
<td>Assumptions (for all of the following three MUCs)</td>
<td>70</td>
</tr>
<tr>
<td>5.3.3</td>
<td>MUC 2 – Increasing number of transport tasks</td>
<td>70</td>
</tr>
<tr>
<td>5.3.4</td>
<td>MUC 3 – Machine breakdown &amp; involvement of humans</td>
<td>74</td>
</tr>
<tr>
<td>5.3.5</td>
<td>MUC 4 – Robot breakdown &amp; insufficient strategy choice as response</td>
<td>76</td>
</tr>
<tr>
<td>5.3.6</td>
<td>MUC 5 - Machine learning related MUC (Frauenhofer AISEC)</td>
<td>78</td>
</tr>
<tr>
<td>6</td>
<td>Misuse-Cases on Bombardier Transportation GmbH use-case</td>
<td>81</td>
</tr>
<tr>
<td>6.1</td>
<td>Bombardier Transportation Use-Case overview</td>
<td>82</td>
</tr>
<tr>
<td>6.2</td>
<td>Bombardier Transportation GmbH misuse case overview</td>
<td>83</td>
</tr>
<tr>
<td>6.3</td>
<td>Bombardier Transportation GmbH misuse Case – Detailed Review</td>
<td>84</td>
</tr>
<tr>
<td>6.3.1</td>
<td>Misuse-Case 1a (Manipulation by external attacker)</td>
<td>84</td>
</tr>
<tr>
<td>7</td>
<td>Misuse-Cases on Machine use-case</td>
<td>90</td>
</tr>
<tr>
<td>7.1</td>
<td>High Metal Overview</td>
<td>91</td>
</tr>
<tr>
<td>7.2</td>
<td>High Metal misuse case - Detailed Review</td>
<td>92</td>
</tr>
<tr>
<td>7.2.1</td>
<td>Misuse-Case - Traceability incident affecting health and safety</td>
<td>92</td>
</tr>
<tr>
<td>8</td>
<td>Misuse-Cases on IDEPA use-case</td>
<td>98</td>
</tr>
<tr>
<td>8.1</td>
<td>IDEPA Use-Case Overview</td>
<td>99</td>
</tr>
<tr>
<td>8.2</td>
<td>IDEPA Misuse-Case Overview</td>
<td>100</td>
</tr>
<tr>
<td>8.3</td>
<td>IDEPA Misuse-Case – Detailed Review</td>
<td>101</td>
</tr>
<tr>
<td>8.3.1</td>
<td>Misuse-Case 1a</td>
<td>101</td>
</tr>
<tr>
<td>8.3.2</td>
<td>Misuse-Case 1b</td>
<td>104</td>
</tr>
<tr>
<td>8.3.3</td>
<td>IDEPA Use-Case Overview</td>
<td>107</td>
</tr>
<tr>
<td>8.3.4</td>
<td>IDEPA Misuse-Case Overview</td>
<td>107</td>
</tr>
<tr>
<td>8.3.5</td>
<td>IDEPA Misuse-Case – Detailed Review</td>
<td>108</td>
</tr>
<tr>
<td>8.3.6</td>
<td>Misuse-Case 1 – Wrong user access (Technical/Security)</td>
<td>108</td>
</tr>
</tbody>
</table>
1 Introduction

1.1 General Misuse-Case Information

A Misuse Case, which is derived from a Use-Case, describes the steps and scenarios which a user/actor performs in order to accomplish a malicious act against a system or business process. They are still use cases in the sense that they define the steps that a user performs to achieve a goal, even if the goal isn't a positive one or a desired one from the perspective of the business process or system designers.

Misuse-cases correspond one to one to defined use-cases, addressing most likely and most dreadful scenarios for each Pilot factory.

Misuse case will cover
- safety hazards, irrespective of originating from security vulnerabilities or inherent to the novel technologies developed in the project,
- security attacks by outsiders
- workers attacks,
- insider threats will also be considered in the misuse cases, giving the required attention to economical, psychological and societal aspects.

1.2 Misuse-Case Development Methodology

To be able to document the right misuse cases, the project team first worked on selecting the right approach. Two phased approach of first working on generic and independent risks and then consolidating them inti misuse cases was the preferred approach.
1.3 Risks Overview

The full list of documented risks are in appendix A (filename: CyberFactory T2.3 Misuse-Cases App #1 Consolidated Risks Table v3.xlsx) file. This section is intended to point out some facts on the risks:

- Total number of documented risks: 153
- Risks grouped by Risk Level:

![Risks by Risk Level](image)

- Risks grouped by Impact Nature:

![Risks by Impact Nature](image)
Risks grouped by Source Type:

Risks by Target Asset:
2 Misuse-Cases on Electronics use-case
### 2.1 Vestel Use-Case Overview

Vestel is a consumer electronics original design manufacturer (ODM) company manufacturing TVs, smartphones, tablets, set-top boxes and home appliances (about 25 million devices per year). Vestel Electronics is responsible for the design and assembly of electronic control and power boards for those products and has several PCB assembly (PcbA) lines.

Vestel targets to solve material handling problems by completing the digital transformation of PCB assembly processes securely with the capabilities that will be developed through CyberFactory#1 project. Currently, data created by assembly machines (sensor data, material usage numbers and etc) can be seen on machine dashboards but cannot be taken out of the machine because some machines are old or using different protocols and etc. In the scope of the Cyber Factory#1 project, those machines will be connected to a MES system that will allow all machines to connect factory network and communicate with a common language. An IoT platform will be established between the shop floor, warehouse, ERP and automated guided vehicles (AGVs). Then the platform will request necessary materials with correct amounts according to production plan from the warehouse automatically. Once the materials are ready, the AGVs will take those materials from warehouse and carry to correct production line when needed. AGVs also carry assembled PCBs back to the warehouse.

The solution will also help to make predictions for the maintenance of the machines. By using different machine learning techniques with the integrated sensor data, unexpected production stops and high maintenance cost will be reduced. This solution will be integrated with the existing factory systems.
2.2 Vestel Misuse-Case Overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

The analysis focuses on risks that are linked to the production network and the communication between systems. The source of the risks must derive from the use case itself. Legacy systems are not in the scope of the misuse case and are seen as a Blackbox.

2.2.1 Misuse-Case 1: Service interruption of AGVs

AGVs are the automated robots that are used to carry materials inside the factory. They follow the routes which were defined with electromagnetic tapes before. They will communicate with MES over Wifi to get jobs. A problem in communication or a technical problem of the device can stop the logistics inside the factory. Production would slow down or stop if some robots were affected from the problem.

Above mentioned unwanted effects on the use case could be caused by two types of disruption: a malfunctioning device and an external attacker.

**Misuse-Case 1a:**

Misuse-Case Type: Functional

The antenna of the AGV may be broken or the magnetic strips that the AGVs follow may be damaged and material logistics inside the factory may slow down because some AGVs are not functioning. Moreover, an immobile AGV can adversely affect entire system because AGVs are moving on predefined lines on the floor. A standing still AGV on that line will be perceived as an obstacle by other AGVs on that line and they will stop until that broken AGV is removed from that line.

**Misuse-Case 1b:**

Misuse-Case Type: Security

The communication of AGVs with the IoT platform can be interrupted by a deauthentication attack to Wifi network. Deauthentication attack is a type of denial of service attack that targets communication between a user (AGV in this case) and a Wi-Fi access point. Someone (a visitor, vendor or an internal) may leave a Wifi device inside the factory Wifi range. Then, the attacker can start a deauthentication attack and disable the communication between AGV and Wifi router. As a result, AGVs cannot get commands from the control platform and may stop functioning completely.

2.2.2 Misuse-Case 2: Abnormal behaviour of IoT devices

The second Misuse-Case focuses on the factory network and connected devices. Factory network is the network that IoT devices and other systems communicate in a production facility. Examples of some IoT devices are component assembly machines, test machines, robot arms.
and AGVs in our use case. The devices send sensed or other internal data related with the device or production to control platform over factory network. Similarly, the control platform sends commands to devices over the same network. Any physical problem in that network results in communication loss or losing control over the devices. This kind of abnormalities can be caused by functional problems or by an attack to the network.

**Misuse-Case 2a:**
Type: Functional

The control platform communicate with the machines over factory network. If there is a problem in the network, platform cannot send tasks to machines and cannot get the data updates for material usage from the machines. The problem can be caused by a broken router/network device or any rupture on the physical network and etc. Depending on the disconnection type, whole system may be effected or just some machines cannot function properly.

**Misuse-Case 2b:**
Type: Security

Another type of disruption is the targeted manipulation of the use case by an external attacker. In this case the attacker gain access to factory network. Then he/she can take control of the devices connected to network. The attacker can send commands to manipulate the machines or send wrong information to control platform about material usage numbers. This will result in chaos in the operation.

### 2.2.3 Misuse-Case 3: Unauthorized Access to Computers and Servers

The data required for the production such as order numbers/plans, product designs, component/material specs are stored on servers which are accessible by computers in shop floor. A possible misuse case is that the data on the servers can be stolen or manipulated by attackers. Another possibility is that a malware for different goals can be installed in one of the computers and cause system to crash or do other manipulation.

**Misuse-Case 3a:** Disclosure and alteration of company confidential data

Type: Security

Company confidential data such as product designs, materials, costs, customers, orders, forecasts etc are stored in company servers.

A hacker can gain access to company servers through the network. Then he/she can get company confidential data mentioned above and sell those data to competitors. Then competitors learn the confidential data for production plans, designs and can increase their competitiveness. Another result of the attack can be the encryption of company confidential data for ransom.

**Misuse-Case 3b:** Installation of malware

Type: Security
The computers in production network requires authenticated entrance to system and ask for admin privileges for program installation.

An insider can stole the credentials of an authorized worker and install a malware in one of the computers in production network. He/she can stole the password by just standing nearby the authorized person and staring the keystrokes and then install the malware later with that credentials. Another possibility is that the attacker waits for the authorized person to leave the computer without logging out, and then he/she can install the malware. Depending on the malware capabilities, it may crash the system and stop the production. Or the malware can take control of the system and send commands to machines and other systems.
2.3 Electronics Misuse-Case – Detailed Review

Time: 18-20 months
Location: Vestel Electronics (Manisa)
Scope: Taking countermeasures against misuse cases which aroused by the implementation of use cases

2.3.1 Misuse-Case 1a – Service Interruption of AGVs (Functional driven)

Assumptions:

For this misuse case scenario, we assume that the AGVs are called by the control platform via Wifi. Also, their routes are determined by the magnetic stripes on the floor and they cannot move out of that line.

Attacker:

The misuse case attacker wants to achieve the following goals:
Disrupt production environment
Unintentional

The attacker’s skill level:
The attacker should has prior knowledge about how AGVs communicate and move. Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 1 attacker. The Level 1 attacker drives causal or coincidental violations, with non-intentional means and individual resources. He/she has no attack skills and mistakes motivation.

Misuse-Case Staging:

The Misuse case has one stages:

- Physically damage the AGV
- Physically damage the environment that the AGV work

<table>
<thead>
<tr>
<th>Option #1: Physically damage AGV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage the antenna of AGV and it cannot communicate with the control platform to get jobs</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Option #2: Damage the environment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physically damage the paths that the AGV follow or put obstacles on the route.</td>
</tr>
</tbody>
</table>
2.3.2 Misuse-Case 1b – Service Interruption of AGVs (Security driven)

Assumptions:

For the misuse case scenario, we assume that the Wifi network is secured by standard methods and a deauthentication attack can disconnect an AGV from the Wifi router. Furthermore, we assume that there is no other backup communication system between the AGVs and the control platform. The used hacking tools are based on open source software.

Attacker:

The misuse case attacker wants to achieve the following goals:

- Create bad reputation for the company
- Gain competitive advantage
- Prove skills
- Stop production for a while and have a rest
- Demonstrate vulnerabilities of the system and sell own products

The attacker’s skill level:

The attacker should have the social capability/network or privileges to enter the production facility together with the attacking device. He/she should has basic knowledge for wireless networks, creating a deauthentication attack and its results. He/she can use open source software, which is a simple script on the web, and run it to reach his/her goals.

Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 2 attacker. The Level 2 attacker drives intentional attacks, with simple means and low resources. He has generic skills and low motivation.

Misuse-Case Staging:

The Misuse case has three stages:

- Entering the factory Wifi range physically
- Getting mac addresses of the router and the victim device
- Start a deauthentication attack

1. Entering the factory Wifi range

A wireless adaptor is left in factory Wifi range

2. Get information about connected devices
2. Get information about connected devices

Monitor the traffic on the network with airmon-ng (Kali)
Find MACs of the router and victim devices with airdump-ng

3. Start an infinite deauthentication attack

Run the command aireplay-ng --deauth 0 -c [DEVICES MAC ADDRESS] -a [ROUTERS MAC ADDRESS] xxx

### Countermeasures and mitigations

In this section possible mitigations are briefly listed.

**Mitigation 1: Not leaving outsiders alone inside the factory**

- Trustable staff should accompany outsiders inside the factory
- Allow outsiders to enter only permitted areas such as meeting rooms and check the room physically after they left

**Mitigation 2: Detection of the rogue devices**

- Using a device that can detect the location of the rogue device

**Mitigation 3: Apply latest security standards**

- Implement more secure standards such as 802.11w to both router and devices.

**Mitigation Gaps**

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that due to new or unknown vulnerabilities of the AGV or the wireless network, it will be possible to perform the Misuse-Case. In these cases capabilities are needed to detect the abnormal behaviour of a robot.

In order to detect the abnormal behaviour, capabilities need to be developed to track the AGVs in real time. Since AGVs operate according to the defined rules in control platform, their location can be estimated in advance. The current locations of them can be tracked with Real time tracking methods. Comparing those locations help to detect an unexpected condition in the system. The development of these capabilities will be addressed as a part of Task 4.1 “Real Time Sensing & Tracking”.
Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the KPI</td>
<td>Value without new countermeasures</td>
<td>Value after introduction of new countermeasures</td>
<td>How to measure, how often to measure (yearly, monthly, etc.)</td>
</tr>
<tr>
<td>Reduction of the response time to AGV related problems with real time monitoring of AGVs</td>
<td>Historical value</td>
<td>Half of the historical value</td>
<td>Realization of the problem</td>
</tr>
</tbody>
</table>

Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGV</td>
<td>HW</td>
<td>Vestel</td>
<td>All</td>
<td>SSA</td>
</tr>
<tr>
<td>Wifi router</td>
<td>HW</td>
<td>Vestel</td>
<td>All</td>
<td>SSA</td>
</tr>
</tbody>
</table>

2 Data, Hardware, Software, Operational System, Information System, Testing Platform
3 Select one or several: development, testing, validation, training, demonstration
4 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^2)</th>
<th>Owner</th>
<th>Uses(^3)</th>
<th>Access(^4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control platform</td>
<td>Operational System</td>
<td>Vestel</td>
<td>All</td>
<td>SSA</td>
</tr>
</tbody>
</table>

**Identification of key assets (misuse case)**

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^5)</th>
<th>Owner</th>
<th>Uses(^6)</th>
<th>Access(^7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless adapter</td>
<td>HW</td>
<td>Attacker</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Hacking sw</td>
<td>SW</td>
<td>Attacker</td>
<td>-</td>
<td>Open source</td>
</tr>
</tbody>
</table>

### 2.3.3 Misuse-Case 2a- Abnormal Behaviour of IoT Devices (Functional Driven)

**Assumptions:**

For this misuse case, we assume that the factory network has hardware components such as Ethernet cables, routers, etc which are open to external manipulation.

**Attacker:**

The misuse case attacker wants to achieve the following goals:

Disrupt the production environment
Have no intention to harm (accidentally)

The attacker’s skill level:
The attacker should have prior knowledge about connection of the factory network and devices.

Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 1 attacker. The Level 1 attacker drives causal or coincidental violations, with non-intentional means and individual resources. He/she has no attack skills and mistakes motivation.

**Misuse-Case Staging:**

The Misuse case has one stage:

Physically disconnect the factory network

---

\(^1\) Data, Hardware, Software, Operational System, Information System, Testing Platform
\(^2\) Select one or several: development, testing, validation, training, demonstration
\(^3\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
2.3.4 Misuse-Case 2b- Abnormal Behaviour of IoT Devices (Security Driven)

Assumptions:

For this misuse case, we assume that some external people such as some privileged suppliers or some critical internal employee has VPN access to network.

Attacker:

The misuse case attacker wants to achieve the following goals:

- Take control of the connected devices and disrupt the production environment
- Stole data from devices
- Prove skills

The attacker’s skill level:
The attacker should has prior knowledge about network and devices, how they are connected and how the devices are controlled. Also, the attacker should has the ability to steal the credentials to enter VPN.

Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 3 attacker. The Level 3 attacker drives intentional attacks, with sophisticated means and moderate resources. He has ICS specific skills and moderate motivation.

Misuse-Case Staging:

The Misuse case has three stages:

- Infiltration in production network
- Imitate a connected device to send wrong data to MES
- Imitate MES to send wrong commands to connected devices

1. Infiltration to the network

Stole the credentials of an authorized person
Log in the platform with stolen credentials (username-password) through VPN
2. Imitate an IoT device

Monitor the traffic and learn the device ID
Send wrong messages to MES with stolen ID

3. Imitate MES

Monitor the traffic and learn the device ID
Send wrong messages to device pretending MES

Countermeasures and mitigations
In this section possible mitigations are briefly listed.
Mitigation 1: Use the strongest possible authentication method for VPN access
Use the most secure authentication provided by the server
Mitigation 2: Use the strongest possible encryption method for VPN access

Mitigation 3: Secure remote wireless networks

Require the remote users to configure their wireless routers and computers for WPA with a pre-shared key, configure their personal firewalls, and keep their home networks secure

Mitigation 4: Secure the hardware of the network

Make it difficult to reach network cables and devices
Take precautions them to keep away from external factors

Mitigation Gaps
Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case, it always has to be expected that it will be possible to perform the Misuse-Case because it is vulnerable to human mistakes. In these cases capabilities are needed to detect the malicious activities in connected devices.
In order to detect the abnormal activities, capabilities need to be developed to secure factory network and devices. Developing more secure methods for M2M communication and trust management may help to prevent the system from attacks and failures. Installing an edge SIEM to monitor the network, detect any suspicious activity and create an alarm may mitigate risks. The development of these capabilities will be addressed as a part of Task 5.1 “Human/Machine Access & Trust Management”.
Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the KPI</td>
<td><em>Value without new countermeasures</em></td>
<td><em>Value after introduction of new countermeasures</em></td>
<td><em>How to measure, how often to measure (yearly, monthly, etc.)</em></td>
</tr>
</tbody>
</table>

| # of suspicious activities in the network | Not available | Available | Yearly |

Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factory network</td>
<td>HW</td>
<td>Vestel</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Connected devices</td>
<td>Operational</td>
<td>Vestel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Identification of key assets (misuse case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{11})</th>
<th>Owner</th>
<th>Uses(^{12})</th>
<th>Access(^{13})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remote computer</td>
<td>Operational</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2.3.5 Misuse-case 3a- Disclosure and alteration of company confidential data (Security Driven)

Assumptions:
For the misuse case scenario, we assume that the company confidential data is stored in servers which are located in factory network and some privileged people, external or internal have access to that network. The servers store data about product designs, materials/components, process data, customer info, stock numbers, orders and plans.

Attacker:

The misuse case attacker wants to achieve the following goals:
- Gain competitive advantage
- Economical advantage
- Ransom
- Prove of skills

The attacker’s skill level:
The attacker should has knowledge about hacking a server, how to block and encrypt data.

Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 3 attacker. The Level 3 attacker drives intentional attacks, with sophisticated means and moderate resources. He has ICS specific skills and moderate motivation.

Misuse-Case Staging:

The Misuse case has three stages:
- Infiltrate in company server
- Stole data
- Perform malicious activity

1. Infiltration

The attacker infiltrates in a computer with a delivery channel such as the user opening a phishing

\(^{11}\) Data, Hardware, Software, Operational System, Information System, Testing Platform

\(^{12}\) Select one or several: development, testing, validation, training, demonstration

\(^{13}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
1. Infiltration

email

2. Infection

The malicious code is downloaded and the code execution begins

Option 1. Data theft

Company confidential data is stolen.

Option 2. Ransom

Staging
The malware determines the data to encrypt.

Malicious code ensures connectivity with its command and control server

Encryption
The local and shared files on the network are encrypted

2.3.6 Misuse-case 3b- Installation of Malware (Security Driven)

Assumptions:
For the misuse case scenario we assume that the computers in the production network are secured by username-passwords for allowing only authorized staff to enter the system. Also, some precautions are taken for malware such as antivirus programs. We also assume that the attacker has some privilege to use that computer but has no authority for installation.

Attacker:

The misuse case attacker wants to achieve the following goals:
- Stop production to create economical loss
- Take control of the devices
- Stole confidential data

The attacker’s skill level:
The attacker should have basic knowledge for computer usage and program installation.

Involving the aforementioned skills and in relation to the IEC62443, the attacker is classified as level 2 attacker. The Level 2 attacker drives intentional attacks, with simple means and low resources. He has generic skills and low motivation.

Misuse-Case Staging:

The Misuse case has three stages:
- Stole credentials of an authorized staff
- Log in production network with stolen credentials
- Perform malicious activity

1. Stealing credentials

The attacker steals the username and password of an authorized user by:
- Staring the authorized person entering user name and password
- Waiting the moment when the authorized person leaves the computer without logging out

2. Logging in with stolen credentials

The attacker uses the stolen username and password in order to have increased privileges in the system for program installation.

3. Installing a malware

The attacker inserts a memory device such as a USB or hard disk, which contains the malware, to one of the USB ports of the computer.
- Malware can be installed automatically
- Attacker can download the malware and setup in a specific location

4. Malware becomes operational

Depending on the malware capabilities
### 4. Malware becomes operational

| The system may be down | May stole information about the system |

**Countermeasures and mitigations**

In this section possible mitigations are briefly listed.

**Mitigation 1: Prevent unauthorized access**
- Select usernames different from predictable ones such as name, surname, registration number, etc.
- Select passwords which are complex sufficiently
- Change passwords periodically
- Be careful and keep privacy while entering username/password
- Avoid the system to save username and passwords

**Mitigation 2: Apply latest security patches**
- Update the system to have latest security patches for malware

**Mitigation 3: Put restrictions to ports on computers**
- Disable the unneeded USB ports in computers.
- Let a few privileged people to have USB port usage permissions

**Mitigation 4: Avoid opening emails from unknown users**

**Mitigation Gaps**

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case, it always has to be expected that it will be possible to perform the Misuse-Case because it is vulnerable to human mistakes. In these cases capabilities are needed to detect the malicious activities in computers.

In order to detect the abnormal activities, capabilities need to be developed to secure authorized access to machines. Installing an edge SIEM to monitor the network, detect any suspicious activity and create an alarm may mitigate risks. The development of these capabilities will be addressed as a part of Task 5.1 “Human/Machine Access & Trust Management”.

---

**Based on the ITEA 3 PO Template v4.0 (August 2017)**
### Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the KPI</td>
<td>Value without new countermeasures</td>
<td>Value after introduction of new countermeasures</td>
<td>How to measure, how often to measure (yearly, monthly, etc.)</td>
</tr>
<tr>
<td># of suspicious activities in computers</td>
<td>Not available</td>
<td>Available</td>
<td>Yearly</td>
</tr>
</tbody>
</table>

### Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Computer</td>
<td>Operational system</td>
<td>Vestel</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Server</td>
<td>Operational system</td>
<td>Vestel</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1 Data, Hardware, Software, Operational Syem, Information System, Testing Platform  
15 Select one or several: development, testing, validation, training, demonstration  
16 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
Identification of key assets (misuse case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware</td>
<td>SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

17 Data, Hardware, Software, Operational System, Information System, Testing Platform
18 Select one or several: development, testing, validation, training, demonstration
19 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
3 Misuse-Cases on Bittium use-case
3.1 Bittium misuse Case – Detailed Review

**Time:** 24 months  
**Location:** Bittium headquarters (Oulu, Finland)  
**Scope:** Scope of the misuse case is a competitor or intelligence services doing industrial sabotage or looking for exploiting the system and gaining access to manipulate Bittium´s data or products. Bittium`s use case is related the Delivery and maintenance of secure mobile devices or equipment with help of partnered manufacturing, and related coordination systems as well as information architecture.

![Diagram of Information Architecture of the Use Case](image)

*Picture: Overview of Information Architecture of the Use Case*

The following picture demonstrates the connection of the relation of the Bittium use/misuse case related to manufacturing from both Information Architecture and the Value Chains perspective. It also addresses the potential main Cybersecurity attack interfaces like; Value chain from Bittium partners to Bittium´s customers  
HW, SW, Product Data, Product security functions (all layers)  
Related Data (e.g. manufacturing, testing, commissioning, delivery)  
*Manufacturing, Maintenance and Support Services*  
*Interfaces and interconnections*, incl. API within the above mentioned environments
3.1.1 Misuse-Case 1. Data manipulation at Bittium manufacturing or partners

**Misuse-case:** Industrial espionage and logistics data manipulation

In regard of the market we address, a competitor or intelligence services doing industrial sabotage or looking for exploiting the system and gaining access to manipulate data, in a context of subcontracting players, might generate critical damages to the company.

**Assumptions**

For this misuse case, we assume that attacker would be able somehow access to production facilities of Bittium partner and Bittium Prose secure production system.

**Attacker:**

The attacker wants to achieve the following goals:
• Create bad reputation of the company by destroying the product or manipulating the data
• Gain competitive advantage for competitor or hostile security actor of the solutions provided for security

The attacker’s skill level:

The attacker should have the social capability/network to enter the production facility, pass the secure controls of the partnered manufacturer site and also be able to destroy the signs of the attack. Attacker should have gained somehow the information where Bittium’s products are actually manufactured in the manufacturing partners.

Attacker should have very high and advanced security control know-how to access to product related information, or pass the security controls or product secure architecture to be able read, write or otherwise manipulate data. After that attacker should have technical knowledge for download and run a script. Attacker should also be able to understand how to attack and what would happen.

Misuse-Case Staging:

The Misuse case has three stages:
• Enter the facility and pass the security controls
• Access to the product or related manufacturing equipment
• Perform the attack

1. Enter the facility and pass the security controls

Stage 1:
Attacker should be able to access to production facility (see Risk ID IoT0014)

2. Access to the product related manufacturing equipment

Stage 2:
In the next step the attacker accesses to the product related manufacturing process and performs the attack (See e.g. Risk ID:s Textile 0010, Electronics 0002).

Stage 3: Perform the attacks
Option 1: Recording of production data

Recording of production data is performed to be able to create manipulated functionalities or software to utilize the data. This option can include manipulated information or features of the product. This requires however access to secure encryption keys or secure boot functionalities.

Option 2: Update/manipulate data into production system

Update/manipulate data into production requires access through secure production system. After that several options would be feasible (See e.g Risk IDs Textile 0010, Electronics 0002)

Option 3. Send information of product production via sending testing information to hostile (malicious/competing) companies

This option requires access to product testing information and secure access to be able to perform the attack.

Counter measures and mitigations

The possible mitigations are the following:

Mitigation 1: Prevent unauthorized access
- Ensure that passwords are having sufficient complexity and are changed periodically (strong two-factor authentication)
- Access to the premises: Ensure that there is sufficient access control system monitoring the accesses to Bittium and its suppliers premises in relation to Bittium related manufacturing activities

Mitigation 2: Implement strong authentication for communication or message exchange
- To mitigate the exchange of unwanted communication messages, message authentication codes (MAC) with a one-time session or any other strong identification key means should be implemented to verify the authenticity of the messages and to mitigate potential attack replay

Mitigation 3: Simulation of cyber resilience activities like seamless network failover, update of assets or firmware or dynamic reconfiguration (in relation to task T5.4)
- To prevent unwanted effects, any change or modification of the system should be simulated and acknowledged before going into service.
- On the other hand the simulation of cyber resilience activities like seamless network failover, update of assets or firmware or dynamic reconfiguration should be enabled.
These principles shall be based on T5.4

**Mitigation 4: Continuous monitoring of assets**

- To reduce the attack surface of each of the assets a continuous monitoring should be enabled.
- Based on continuous monitoring of the assets the health status (like latest security batch, SW version) of each asset is known. Continuous monitoring enables an overview which tasks do the FoF assets have and in which status they are.
- These shall be demonstrated in T5.4 (in misuse case based on Bittium Prose and SafeMove).

**Mitigation 5: Secure network hardware configuration**

- Review the network settings of network hardware to avoid any faulty settings to be exploited.
- If possible combine the status of the hardware to continuous monitoring of assets.

**Mitigation 6: Implement only necessary network services**

- To reduce the attack surface all unneeded/unnecessary network services should be disabled.
- Create monitoring system to monitor the status of network services and to detect any misbehaving services.

**Mitigation 7: Apply the latest security patches**

- Implement latest security patches to all software running on assets.
- Create a system to monitor the status of all assets (like version, SW update, misbehavior of the system).
- These will be demonstrated based on Bittium SafeMove.

**Mitigation Gaps**

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that due to new or unknown vulnerabilities to the factory it will be possible to perform the Misuse-Case.

Developing such capabilities will be addressed as part of Tasks 5.1 “Human/Machine access & trust management” and Task 5.4 “Cyber-resilience mechanisms”. Also with further capabilities of trust management highly resilient FoF systems have further to expect an breach of current and future security mechanisms which afterwards enables an attacker to perform the described Misuse-Case.

To develop the capability to detect the abnormal behaviour capabilities need to be developed to monitor the behaviour of production system with the manufacturing partner. Also capabilities need to be developed to train employers to detect abnormal behaviour and to analyse the underlying reason leading to the abnormal behaviour including forensic support. The development of these capabilities will be addressed as part of Task 5.3 “H/M-Behaviour Watch.”
A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”. Digital models created as part of this task should also be used as base for training employers regarding abnormal behaviour.

For distributed manufacturing cases the optimization of Data-lake (like visualisation) (T4.2) and means of distributed manufacturing (T4.4.) control are mandatory to take into consideration.

### Identification of key assets (misuse case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack SW/HW</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bittium PROSE and related systems.</td>
<td>Operational System Information System</td>
<td>Bittium</td>
<td>Development Testing Validation Demonstration</td>
<td>(SSA)</td>
</tr>
</tbody>
</table>

---

20 Data, Hardware, Software, Operational System, Information System, Testing Platform
21 Select one or several: development, testing, validation, training, demonstration
22 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{20})</th>
<th>Owner</th>
<th>Uses(^{21})</th>
<th>Access(^{22})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bittium SafeMove ® Mobile VPN</td>
<td>Software</td>
<td>Bittium</td>
<td>Validation Demonstration</td>
<td>(SSA)</td>
</tr>
<tr>
<td>Bittium SafeMove ® Analytics</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td># of abnormalities in the Bittium manufacturing value chain</td>
<td>Not fully available</td>
<td>Real-time measurement</td>
<td>Continuous</td>
</tr>
<tr>
<td># share of online and monitored manufacturing assets (SW,HW, version, Bittium manufacturing value chain)</td>
<td>Partially available</td>
<td>Continuous monitoring of assets (&gt;90%)</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

3.1.2 Misuse-Case 2 Industrial espionage via Secure Product Commissioning

Assumptions:

Secure products require secure product commissioning, software installation, delivery and maintenance. Potential attacker would like to gain access to a secure product to be able to potential cause harm, or spy product utilization by accessing to a commissioning phase of the product. This could include e.g. hostile features installation or product use monitoring of secure products through product secure commissioning, delivery and maintenance. Assumption is that the attack is performed in the production facility.

Attacker:
The misuse case attacker wants to achieve the following goals:
Create bad reputation of the company by accessing to the product by manipulating the data or features of the product
Gain competitive advantage for competitor or hostile security actor of the solutions provided for security
Potentially install hostile monitoring software to be able to identify the product use, where products are being used or to be able to start malicious attack for the users of the product

The attacker’s skill level:

Attacker should have direct access to Bittium´s products or predenting to being Bittium employee or production worker. The attacker should be able to destroy the signs of the attack
Attacker should have very high and advanced security control know-how to gain access to product related information, or pass the security controls or product secure architecture to be able read, write or otherwise manipulate data. After that attacker should have technical knowledge for download and run a script. Attacker should also be able to understand how to attack and what would happen.

Misuse-Case Staging:

1. Gain access to Commissioning phase of the product

Stage 1:
Attacker should be able to have ability to access or right to use the equipment for product commissioning (access to production facility). See Risk ID IoT0014

2. Access to commissioning place

Stage 2:
In the next step the attacker should have capability to use the commissioning tools and perform the attack
Attacker should especially have information how to correctly commission Bittium product.

Stage 3: Drive the attacks

Option 1; Perform malicious commissioning

Due to the fact that the attacker has gained direct access to the commissioning communication that occurs between the product and related commissioning tools, attacker can drive replay attacks or execute malicious commissioning.
This requires very advanced know-how how to intercept commissioning and related security functions (like flashing, key management, test functions etc.).

Option 2: Perform data manipulation

Due to the fact that the attacker has gained direct access to the commissioning communication that occurs between the product and related commissioning tools, attacker can drive modified commissioning and related data manipulation. Attacker should be able to intercept the secure
Option 2: Perform data manipulation

functionality within commissioning or the product (software/data / secure commissioning / product). Attacker would like to gain ownership of the device and then manipulate the user or the product fleet where product is connected. Sometimes the information where the product is being used is essential. This requires very advanced know-how how to intercept commissioning and related security functions (like flashing, key management, test functions etc.). See e.g. Risk ID: Electronics 0004.

Countermeasures and mitigations
The possible mitigations are the following:

Mitigation 1: Prevent unauthorized access
- System: Ensure that passwords are having sufficient complexity and changed periodically, e.g. permissioning with two-factor authentication etc.
- Various personnel security and premises security arrangements including
  - Access to the premises: Ensure that there is sufficient access control system monitoring the accesses to Bittium and its suppliers premises in relation to Bittium related manufacturing activities
  - Access to the commissioning system is monitored via Bittium Prose systems

Mitigation 2: Implement strong authentication for communication or message exchange within the commissioning tools and the product itself.
- To mitigate the exchange of unwanted communication messages, message authentication codes (MAC) with a one-time session or any other strong identification key means should be implemented to verify the authenticity of the messages and to mitigate potential attack replay
- Implementation of PKI tree key and certificate structure and verifying connections with those certificates between product and commissioning services is recommended to ensure secure connection.

Mitigation 3: Continuous monitoring of assets
- To reduce the attack surface of each of the asset continuous monitoring should be enabled including the commissioning tools
- The used tools are verified (traceability, auditability, events) – trace should be enabled
- Based on continuous monitoring of the assets the health status (like latest security batch, SW version) of each asset is known. Continuous monitoring enables an overview which tasks do the FoF assets have and in which status they are.

Mitigation 4: Secure network hardware and segments configuration
- Review the network settings of network hardware to avoid any faulty settings to be exploited (network segmentation, firewall, IP filtering practices)
- If possible combine the status of the hardware to continuous monitoring of assets with advanced SIEM functionality
- These are monitored e.g. via Bittium Prose and Bittium SafeMove systems in Bittium misuse cases

Mitigation 5: Implement only necessary network services
- To reduce the attack surface all unnecessary network services should be disabled and use increasingly secure point to point connections.
- Create monitoring system to monitor the status of network services and to detect any misbehaving services

**Mitigation 6: Apply the latest security patches**

- Implement latest security patches to all software running on assets
- Create a system to monitor the status of all assets (like version, SW update, misbehavior) and alert from abnormalities
- These will be demonstrated based on Bittium SafeMove

**Mitigation Gaps**

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that due to access to production facilities it will be possible to perform the Misuse-Case.

Developing such capabilities will be addressed as part of Tasks 5.1 “Human/Machine access & trust management” and Task 5.4 “Cyber-resilience mechanisms”. Also with further capabilities of trust management highly resilient FoF systems have further to expect an breach of current and future security mechanisms which afterwards enables an attacker to perform the described Misuse-Case.

To develop the capability to detect the abnormal behaviour capabilities need to be developed to monitor the behaviour of production system with the manufacturing partner. Also capabilities need to be developed to train employers to detect abnormal behaviour or to analyse the underlying reason leading to the abnormal behaviour. The development of these capabilities will be addressed as part of Task 5.3 “H/M-Behaviour Watch”.

A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”. Digital models created as part of this task should also be used as base for training employers regarding abnormal behaviour.

For distributed manufacturing cases the optimization of Data-lake (like visualisation) (T4.2) and means of distributed manufacturing (T4.4.) control are mandatory to take into consideration.
Identification of key assets (Misuse case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{23})</th>
<th>Owner</th>
<th>Uses(^{24})</th>
<th>Access(^{25})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack SW/HW</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment PKI tree key and certificate structure</td>
<td>SW Presentation</td>
<td>Bittium</td>
<td>Demonstration</td>
<td>(SSA)</td>
</tr>
<tr>
<td>Equipment commissioning principles, (e.g. roles, rights) in a secure product manufacturing, delivery and maintenance</td>
<td>SW Presentation</td>
<td>Bittium</td>
<td>Demonstration</td>
<td>(SSA)</td>
</tr>
<tr>
<td>Bittium PROSE and related systems.</td>
<td>Operational System Information System</td>
<td>Bittium</td>
<td>Development Testing Validation Demonstration</td>
<td>(SSA)</td>
</tr>
<tr>
<td>Bittium SafeMove ® Mobile VPN</td>
<td>Software</td>
<td>Bittium</td>
<td>Validation</td>
<td>(SSA)</td>
</tr>
</tbody>
</table>

\(^{23}\) Data, Hardware, Software, Operational System, Information System, Testing Platform  
\(^{24}\) Select one or several: development, testing, validation, training, demonstration  
\(^{25}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type²³</th>
<th>Owner</th>
<th>Uses²⁴</th>
<th>Access²⁵</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bittium SafeMove ® Analytics</td>
<td></td>
<td></td>
<td>Demonstration</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td># of potential misuse case attacks (product commissioning)</td>
<td>Not fully available</td>
<td>Real-time measurement</td>
<td>As continuous as possible</td>
</tr>
<tr>
<td># share of online assets (commissioning)</td>
<td>Partially available</td>
<td>Continuous monitoring of assets</td>
<td>Continuous</td>
</tr>
</tbody>
</table>
4 Misuse-Cases on “CPS-based manufacturing on auxiliary automotive industry” use-case
4.1 “CPS-based manufacturing on auxiliary automotive industry” Use-Case Overview

Auxiliary automotive industry is composed by traditional and growing companies that need to meet the big requirements of a highly technological industry. The technification of the manufacturing processes comes with production enhancement and new threats that need to be addressed. Automated devices require cyber security measures but offer new ways of measuring the environment, and thus, applying new generation of techniques to improve production and safety.

In this context, Trimek’s “MetroLab” genscenario aims at working towards CPS (Cyber Physical System) for zero defect manufacturing (ZDM). For this purpose a cybergauge system is used, composed by a scanning system/CMM (Coordinates Measuring Machines) in charge of creating digital twins of the manufactured parts connected with wireless temperature sensors, to enable temperature compensation measurements, and to a cloud based system to enable automation of contextual information visualization.

The current “MetroLab” involves a manual scanning process in an isolated (not externally connected) laboratory environment where external variables such as temperature and humidity are properly controlled. Additionally, the work is performed by expert metrologists. The target scenario aims at evolving it to a more interconnected shop floor environment where the process itself can be fully automated. This leads to a not so controlled environment, with variable conditions and not specialized operators, which require new powerful communication infrastructure, wireless sensors and a set of cybersecurity systems/tools to provide monitoring capabilities to ensure the proper functioning of the use case.

The scope of the use case involves the following components:
- Scanning system (robotic arm plus scanning system/CMM)
- Wireless communication infrastructure (Wi-Fi)
- Wireless Sensor Networks (WSN) for environmental variable measurement and indoor tracking of assets/workers
- Collaborative robots
- Cybersecurity-related mechanisms
Figure: Use case overall architecture.
4.2 "CPS-based manufacturing on auxiliary automotive industry" Misuse-Case Overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

The analysis performed in the current chapter focuses on risks that are linked to the different components that take part in the use case.

**Misuse-Case 1: Wi-Fi Network interruption**

The Wi-Fi network infrastructure deployed within the factory shop floor provides connectivity to the systems involved in the scanning process (robot arms, scanning sensor) as well as to the cobots performing material transportation jobs. In addition, it also provides network connectivity to the gateways connecting the WSN with IT level backhaul.

Within the Wi-Fi range, several type of attacks can be performed by different kind of attackers (intruders, visitors, customers, vendors, or even insiders). These wireless attacks can come through different methods. Some of them rely on tricking users, others using brute force, and some others look for Wi-Fi network deployments where required security measures have not been enabled.

A Wi-Fi network interruption will affect the communications involving the scanning systems present in the "MetroLab" as well as the cobots participating in the transportation of the materials.

**Misuse-Case 1a: Affecting scanning systems**

Misuse-Case Type: Security

The communication in the scanning systems is vital not only for the output data but for the input too. Focusing on the output data communication, if the Wi-Fi network fell down, data which scanning systems sensors is getting will not be sent. Some of this data can be crucial for the rest of the process (if there is a product that needs to be taken out of the process and the order can’t be sent, the whole process could be in danger). Input data is related with this problem too, it is necessary to receive orders from other robots of the process.

**Misuse-Case 1b: Affecting cobot fleets**

Misuse-Case Type: Security

The communications with the deployed cobots depends fully on the existing Wi-Fi infrastructure. Any lack of Wi-Fi network availability affects the normal functioning of the cobots in charge of providing material across the shopfloor. No tracking or monitoring of these cobots could be performed resulting in an isolated and vulnerable fleet of cobots.

The global planner is done outside of the robots in a centralized server. In the event of a temporary Wi-fi outage, the cobots will continue working until the last goal received has been satisfied but there will be no information regarding the status of the fleet. The path taken by the cobots might not be the optimum because they will not have global information. Nevertheless, even without Wi-fi, the cobots will not collide with people, other cobots or the environment.
because the local planner is done locally (per-cobot). The log of events of the robots will continue locally until the Wi-fi is reestablished and can be published again.

If the Wi-fi outage lasts over time and some of the cobots are moved (also known as robot kidnapping) from their location, they will require a manual re-localization.

**Misuse-Case 2: Wireless Sensor Network (WSN) interruption**

The second Misuse-Case focuses on the WSN deployed in the shop floor for measurement of environmental conditions as well as for assets/devices/workers indoor tracking.

The interruption of any of the Wireless Sensor Networks (WSN) deployed throughout the factory will cause the loss of critical context related information needed for the manufacturing process.

**Misuse-Case 2a: Affecting environmental variables measurement**
Misuse-Case Type: Security

Sensors are deployed to measure environmental variables such as temperature and humidity which provide critical information that ensures the quality of the scanning processes performed in the "MetroLab". These sensors, deployed in a ZigBee WSN, can be exposed to different type of attacks with the consequent risk of data exposure and manipulation.

**Misuse-Case 2b: Affecting indoor tracking system**
Misuse-Case Type: Security

The indoor tracking of assets/workers is based on Ultra-Wideband (UWB) WSN. This type of networks is specially promising in high density scenarios (i.e.: parking structures, factories, hospitals, airports, etc.) due to the level of accuracy, power consumption and robustness in wireless connectivity they provide. However, attacks performed to any of the network elements conforming the UWB infrastructure will result in erroneous measures or in the worst case a total loss of indoor tracking of the different assets/workers.

**Misuse-Case 3: Cybersecurity-related services misbehaving**

In addition to the network infrastructures deployed in the shop floor, several cybersecurity related tools and services are deployed providing the following features:
- Authorization server for a global policy-based assets/nodes secure interaction
- ML-based data correlation and detection subsystem
- SOC M&C visualization dashboard for ML analytics, tracking monitoring and security events detection.

The current Misuse-Case describes the abnormal operation and even the service interruption of these services due to unauthorized access, data/configuration manipulation with aim of making them unavailable and resulting in an undetected attack.

**Misuse-Case 3:**
Misuse-Case Type: Security
The misbehaving or complete unavailability of the aforementioned cybersecurity services/tools could lead to a lack of awareness and monitoring capabilities regarding the security status of the use case scenario.
4.3 “CPS-based manufacturing on auxiliary automotive industry”
Misuse-Case – Detailed Review

Time: 24 months?
Location: TRIMEK factory (Bilbao/Vitoria - Spain)
Scope:

4.3.1 Misuse-Case 1a – Wi-Fi network interruption affecting cobot fleets
(Functional)

Assumptions:

For the “Wi-Fi network interruption” misuse-case we assume that the network is secured by Redborder that can be broken with cyber-attacks. As a consequence of this, the scanning system involved in the ZDM process would be exposed and be vulnerable to potential attacks that could lead to take control of the computer/systems in charge of controlling the robotic arm and CMM.

In addition to the consequences of having a vulnerable Wi-Fi network affecting the different scanning system elements, the assumption of cobots connected to this network has also been taken into consideration. Furthermore, the cobots lack of specific security features/modules that could avoid this kind of risk scenarios leaving an open gate to potential attacks to the cobots as well as the backend services in charge of the cobot fleet management. In the event of an attack will render the monitoring of the cobots useless.

Attacker:

The misuse case attacker wants to achieve the following goals:

- Disrupt the production environment of the factory
- Create bad reputation of the company
- Competitive advantage by data leakage of the scanned parts, access to blueprints, etc.
- Proof of hacker skills
- Bad intentional employee
- Sell own manufacturing parts
- Sell own cobots

The attacker’s skill level:

In case of an external attacker, she/he should have social engineering skills in order to have access to enter the production facility where the manufacturing network is deployed. Additionally, basic technical knowledge is required for downloading and running the required Wi-Fi exploitation toolkit/scripts as well as to have the “know how” to understand how the attack is being performed and what kind of accesses and assets are being compromised on both scanning systems and cobots.

If the attacker not also penetrates the wireless but access gains access to the cobot may cause physical damage to the other cobots or to the factory.
Misuse-Case Staging:

The Misuse case has three stages:

1. Enter the facility and have access to the manufacturing area where the Wi-Fi network is deployed.
2. Deploy the required hardware to perform the attack.
3. Perform the attack.

1) Breaking of Wi-Fi communication protocol

Stage 1:

- WPA:
  1. Monitor network traffic with tools such as “airmon-ng” and get a list of the MAC addresses corresponding to the existing devices/clients connected to the different wireless routers/AP.
  2. Perform a deauthentication attack in order to force the victim to reauthenticate while the attacker sniffs the WPA 4-way handshake and perform a WPA bruteforce attack on the password.

- WPA2-PSK:
  1. PAL cobots use WPA2-PSK. WPA2 can use AES algorithm with is safer and it is implemented in hardware sometimes to increase computational speed. The problem is also that people don’t use the best passwords, they can be predictable.

2) Getting access to:

- The systems/services involved in the “Scanning System”
- Cobots

Stage 2:

Once the Wi-Fi network has been compromised, access to the target devices/systems must be obtained:

- “Scanning System” services/devices
  Systems/services involved in the “Scanning system”
  o Get access to the data extract from the scanning system.
  o Get access to the input data that is arriving to the scanning system.
  o Enable the modification of parameters measured by the scanning system and transmit this data to the next process’s machine.

- Cobots
  o Get access to the backend where Cobots management process is being performed.
  o Get individual access to the Cobots.
3) Wrong WO/commands are sent to the target systems/devices

Stage 3:
The attacker can intercept the communications inside the scanning systems (between the computer/device and the robotic arm + CMM) in order to inject wrong WO to the system performing the scanning process.

In the case of cobots, the data intercepted between the cobot and the backend systems, could be potentially manipulated so that wrong status information (battery status, work order, location info, etc.) could lead them to undesired behavior.

Countermeasures and mitigations
In this section possible mitigations are briefly listed.

Mitigation 1: External personnel must always be accompanied by internal personnel.

Mitigation 2: Perform an internal vulnerability assessment as well as a pentesting of the deployed Wi-Fi network infrastructure to ensure every security measure is adopted.

- Avoid:
  - Default configuration settings
  - Un-authorized APs
  - Unencrypted wireless traffic
  - Easily circumvented MAC address controls
  - Wireless equipment that is physically accessible
  - Weak wireless protocols

- Make sure:
  - Proper Wi-Fi coverage (avoid unnecessary areas coverage)
  - Hide network SSID
  - Disable Wi-Fi protected setup (WPS)
  - Strong and unique password
  - Network encryption is enabled
  - Change default IP address configuration on the APs
Mitigation 3: Systems/devices hardening in order to ensure:

- Apply latest security patches
- Disable unneeded network services
- Proper access policy enforcement (authorization)

Mitigation Gaps

The aforementioned countermeasures and mitigations allow to evolve towards a more secure and resilient network. However, because the Wi-Fi network is critical to the normal operation of the scenario, a continuous monitoring of the adopted security measures is recommended due to new or unknown vulnerabilities that could arise. For that reason, the above-mentioned measures are taken into consideration together with monitoring capabilities/tools which provide proper authorization policy enforcement, systems/devices data monitoring and Wi-Fi network traffic analysis.

Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
</table>

Based on the ITEA 3 PO Template v4.0 (August 2017)
<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Downtime of the manufacturing parts scanning process [%]</td>
<td>Not available</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disturb cobot fleet:</td>
<td>Not available</td>
<td>Available</td>
<td>Real-time monitoring</td>
</tr>
<tr>
<td>• # of WO not performed</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of no data sharing from scanning systems [%]</td>
<td>Not available</td>
<td></td>
<td>Real-time monitoring</td>
</tr>
<tr>
<td># of actions no carry out due to error in communication</td>
<td>Not available</td>
<td></td>
<td>Real-time monitoring</td>
</tr>
</tbody>
</table>

**Identification of key assets (use case)**

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{26})</th>
<th>Owner</th>
<th>Uses(^{27})</th>
<th>Access(^{28})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi routers</td>
<td>HW</td>
<td>ENEO</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cobots</td>
<td>HW</td>
<td>PAL Robotics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indoor tracking devices (anchors, gateways, tags)</td>
<td>HW</td>
<td>S21sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Identification of key assets (misuse case)**

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{29})</th>
<th>Owner</th>
<th>Uses(^{30})</th>
<th>Access(^{31})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi hacking tools (Wi-Fi adapter, SoC, rogue WAP, SW toolkit)</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\(^{26}\) Data, Hardware, Software, Operational System, Information System, Testing Platform
\(^{27}\) Select one or several: development, testing, validation, training, demonstration
\(^{28}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
\(^{29}\) Data, Hardware, Software, Operational System, Information System, Testing Platform
\(^{30}\) Select one or several: development, testing, validation, training, demonstration
\(^{31}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
4.3.2 Misuse-Case 2 -- Wireless Sensor Network (WSN) affecting indoor tracking systems

Assumptions:

This misuse-case relies on the fact that the Wireless communication is vulnerable and acts as an entrance gate to the gateway elements present on both ZigBee and UWB networks that connects each of these WSN networks to the deployed Wi-Fi infrastructure. Thus, an unauthorized access to the Wi-Fi (backhaul) network followed by a successful attack on these gateway elements could cause the WSN system failure and unavailability of the environmental sensing and assets/workers indoor tracking services.

Attacker:

The misuse case attacker wants to achieve the following goals:
- Disrupt the production environment of the factory
- Create bad reputation of the company
- Fake environmental data insertion affecting the scanning system process
- Unprecise indoor tracking data
- Proof of hacker skills
- Bad intentional employee

The attacker’s skill level:

In case of an external attacker, she/he should have social engineering skills in order to have access to enter the production facility where the manufacturing network is deployed. Additionally, basic technical knowledge is required for downloading and running the required ZigBee/UWB exploitation toolkit/scripts as well as to have the “know how” to understand how the attack is being performed and what kind of accesses and assets are being compromised on both networks.

Misuse-Case Staging:

Depending on the attacker’s final goal, the misuse-case staging process will change. Thus, if the attacker’s intention is to eavesdrop the communications for data exposure or malicious data replay/injection, attacks such as man in the middle (MITM) or nodes tampering will be performed.

On the other hand, if the aim of the attacker is to disrupt the WSN itself, the attacks will be focused on tampering the nodes or gaining access over the element acting as the gateway towards the backhaul network.

In both cases, the misuse case will be composed of the following stages:
1. Enter the facility and have access to the manufacturing area where the WSN networks are deployed.
2. Deploy the required hardware to perform the attack.
3. Perform the attack.

### 1) Breaking of WSN network

**Stage 1:**

Access to the WSN can be achieved either by carrying out a prior attack to the Wi-Fi network from which the access to the WSN network could be made or by performing a direct attack to the WSN itself.

The attack can be detected/tracked due to the Wi-Fi traffic management performed by the “Redborder Protection” system. In case there is no protection enabled, the WSN network could be exposed to potential hacker attacks enabling access to the machines connected in this network.

In order to perform a direct attack to the WSN (not involving Wi-Fi network), the attacker needs to gain physical access to the factory and be close enough to the machine that wants to get access.

It is important to highlight the fact that the PAL Robotic’s Cobots do not interact WSN or integrate any kind of WSN sensors/actuators per se but it might include them.

### 2) Getting access to WSN nodes and/or gateway elements of the network

**Stage 2:**

Once the WSN network has been compromised, the attacker will try to perform the following actions:

1) Eavesdrop the communications between the WSN nodes and the central gateway.

2) Access and get control of the gateway element of both WSN networks. This element, responsible of receiving and relaying measured data towards the services where they will be consumed, should be properly hardened and protected.

### 3) Option 1: WSN system interruption
3) Option 1: WSN system interruption

The attacker gains access to the gateway element of the WSN by exploiting existing vulnerabilities. Once the attacker is able to control the gateway, the system can be disabled or modified so that data is exposed and redirected to different backend servers.

4) Option 2: WSN data manipulation/leakage

The attacker gains access to the gateway element of the WSN and is able to inject modified data into the system affecting the scanning process.

In the case of the indoor tracking of assets/worker, the injection of fake data causes the misbehaving of the tracking service due to the lack of accuracy of the measured positioning data.

Countermeasures and mitigations

In this section possible mitigations are briefly listed.

Mitigation 1: External personnel must always be accompanied by internal personnel.

Mitigation 2: Perform an internal vulnerability assessment plus pentesting of the deployed Wi-Fi network infrastructure to ensure every security measure is adopted.

- Avoid:
  - Default configuration settings
  - Un-authorized APs
  - Unencrypted wireless traffic
  - Easily circumvented MAC address controls
  - Wireless equipment that is physically accessible
  - Weak wireless protocols

- Make sure:
  - Proper Wi-Fi coverage (avoid unnecessary areas coverage)
  - Hide network SSID
  - Disable Wi-Fi protected setup (WPS)
  - Strong and unique password
  - Network encryption is enabled
  - Change default IP address configuration on the APs
  - Disable DHCP functionality
  - Keep firmware-updated routers/APs

Mitigation 3: Hardening of the different elements conforming the WSN

- Apply latest security patches
- Proper access policy enforcement (authorization)
Mitigation 4: WSN network inventory

- Up to date inventory of the deployed WSN devices

Mitigation Gaps

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case. However, it always has to be expected that due to the new or unknown vulnerabilities to the WSN deployed in the factory it will be possible to perform the Misuse-Case.

In order to decrease the exposure level of the WSN deployed throughout the factory, capabilities that ensures a proper Human/Machine interaction will be addressed.

Additionally, some capabilities to detect abnormal behavior of the WSN by performing monitoring activities and analysis of the underlying traffic will be developed.

Key Performance Indicators (KPIs) and Targets

| KPI                              | Historical Value | Target Value | Measurement |
|----------------------------------|------------------|--------------|-------------|-------------|

Page 53 of 111 Based on the ITEA 3 PO Template v4.0 (August 2017)
### KPI

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td># of wrong scans due to environmental sensors misbehaving</td>
<td>Not available</td>
<td></td>
<td>Real-time detection</td>
</tr>
<tr>
<td># of no scanning due to cyber-attacks</td>
<td>Not available</td>
<td></td>
<td>Real-time detection</td>
</tr>
<tr>
<td># of data theft from scans due to cyber-attacks</td>
<td>Not available</td>
<td></td>
<td>Real-time detection</td>
</tr>
<tr>
<td># of worker safety incidents due to wrong tracking</td>
<td>Not available</td>
<td></td>
<td>Real-time measurement</td>
</tr>
<tr>
<td># of assets/material lost</td>
<td>Not available</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Identification of key assets (use case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN for environmental measurement</td>
<td>HW</td>
<td>ENEO/TRIMEK</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indoor tracking devices (anchors, gateways, tags)</td>
<td>HW</td>
<td>S21sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Identification of key assets (misuse case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN specific and Wi-Fi hacking tools (Wi-Fi adapter, SoC, rogue WAP, SW toolkit)</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

32 Data, Hardware, Software, Operational System, Information System, Testing Platform
33 Select one or several: development, testing, validation, training, demonstration
34 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
35 Data, Hardware, Software, Operational System, Information System, Testing Platform
36 Select one or several: development, testing, validation, training, demonstration
37 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
### Asset description

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSN (ZigBee and UWB) hardware and software toolkit</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 4.3.3 Misuse-Case 3 -- Cybersecurity-related services misbehaving

#### Assumptions:

The current Misuse-case assumes that the supporting cybersecurity-related tools/services are installed on the servers located in the enterprise level of the factory where only privileged users have access to them. These applications aim at providing the following cybersecurity features:

- Authorization server: provides a global policy for a secure assets/nodes secure interaction.
- ML-based data correlation and detection subsystem.
- SOC M&C visualization dashboard for ML analytics, tracking monitoring and security events detection.

Therefore, we assume that the attacker is aware of the existence of these cybersecurity services.

#### Attacker:

The attacker in the current misuse wants to achieve the following goals:

- Disable cybersecurity-enabled features/measures prior to performing any further attack.
- Disrupt the production environment of the factory
- Create bad reputation of the company
- Proof of hacker skills

The attacker’s skill level:

In case of an external attacker, she/he should have social engineering skills in order to have physical access to the enterprise level facility from where the IT-backhaul network could be reach. Both the external or internal users should have medium to high network and applications security skills in order to be able to perform network assets discovery prior to performing vulnerability discovery and subsequent exploitation before gaining control of the systems.

#### Misuse-Case Staging:

The Misuse case has three stages:

1. Enter the facility to the enterprise level area with IT-backhaul network connectivity.
2. Perform a network assets discovery
3. Perform the attack and malicious activity
1) Enter the facility and access the enterprise level area

Stage 1:
The attacker should get access to the factory and enter the enterprise level area with IT-backhaul network connectivity.

2) Network Infiltration

Stage 2:
Once the attacker has physical access to the enterprise level area, network connectivity infiltration phase should be accomplished. For that, she/he could obtain access in any of the following ways:
- Stealing credentials from an authorized user
- Obtaining credentials by performing a vishing/phishing campaign

3) Discovery and Exploitation

Stage 3:
Once the user has gained access to the network, she/he would perform a network discovery analysis searching for the already known cybersecurity services/tools. Then, a vulnerability analysis of the systems/services would present the vulnerabilities to be exploited.

4) Cybersecurity services manipulation

Stage 4:
The attacker would perform some cybersecurity services/tools data update/manipulation in order to disable or alter the normal operation so that a subsequent attack (WSN, Wi-Fi network, etc.) could be performed in an undetectable manner.

Countermeasures and mitigations
In this section possible mitigations are briefly listed.
Mitigation 1: External personnel must always be accompanied by internal personnel.

- Outsiders only permitted in controlled areas such as meeting rooms.
- Trustable insiders should accompany outsiders if accessing non-controlled areas.
- Background checking after their visit/access.

Mitigation 2: Avoid unattended physical network connectors and network devices

- Avoid unattended network connectors and devices (routers, etc.)

Mitigation 3: Hardening of the servers running the cybersecurity-related services as well as the stored data

- Apply latest security patches
- Proper access policy enforcement (authorization)
- Self-vulnerability assessment of the OS, systems, etc.

Mitigation 4: Network segmentation

- Perform a proper virtual/physical network segmentation separating groups of systems or applications from each other.

Mitigation Gaps

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case. However, it always has to be expected that due to access to the servers (where the aforementioned supporting cybersecurity services/tools reside) will continue to exist, it will be possible to perform the Misuse-Case.

Hence, capabilities that provides additional monitoring and awareness of the underlying communications for potential deviations will be tackled by the different tasks such as “5.1 Human/Machine access & trust management” and “5.4 Human/Machine Behavior”.
Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td># of suspicious activities in the network</td>
<td>Not available</td>
<td>Real-time awareness</td>
<td>Continuous</td>
</tr>
<tr>
<td># of suspicious activities in the cybersecurity-related servers/systems</td>
<td>Not available</td>
<td>Real-time awareness</td>
<td>Continuous</td>
</tr>
</tbody>
</table>

Identification of key assets (use case)

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{38})</th>
<th>Owner</th>
<th>Uses(^{39})</th>
<th>Access(^{40})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity-related services/tools</td>
<td>SW</td>
<td>ENEO/S21sec</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Identification of key assets (misuse case)

\(^{38}\) Data, Hardware, Software, Operational System, Information System, Testing Platform

\(^{39}\) Select one or several: development, testing, validation, training, demonstration

\(^{40}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type&lt;sup&gt;41&lt;/sup&gt;</th>
<th>Owner</th>
<th>Uses&lt;sup&gt;42&lt;/sup&gt;</th>
<th>Access&lt;sup&gt;43&lt;/sup&gt;</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking tools (Wi-Fi adapter, SoC, rogue WAP, SW toolkit)</td>
<td>HW+SW</td>
<td>Attacker</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<sup>41</sup> Data, Hardware, Software, Operational System, Information System, Testing Platform  
<sup>42</sup> Select one or several: development, testing, validation, training, demonstration  
<sup>43</sup> Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
5 Misuse-Cases on InSystems Automation GmbH use-case
5.1 InSystems Use Case Overview

InSystems Automation develops automated transport systems that perform factory internal logistics tasks independently and autonomously. The transport robots developed by InSystems Automation localize themselves within a pre-scanned map using live sensor data from a laser scanner, among others. This new decentralized Robot to Robot communication is realized via the COATY Framework and data is exchanged with the MQTT protocol.

The scope of this use case is a robot fleet, consisting of minimum of two robots which communicate between each other but also with a MES (manufacturing execution system) system and the strategy component:

- **MES:** The MES component generates and delivers jobs that include all necessary data to fulfill the job.
- **Strategy Component:** The strategy component works together with the MES and all robots. It calculates and generates strategies how to handle and prioritize the jobs and pushes the strategies to the robots.
- **Robot:** The robots communicate over the Wi-Fi router with each other and each robot has a connection to the MES via a so called MES Adapter which is running on each robot.
- **Broker:** The broker is the central element of the COATY framework. It coordinates the communication in-between robots with a publish/subscribe principle.

New jobs are generated by the MES. The MES publishes the job to the robot fleet. Each robot checks his local job queue and the time needed to fulfill this queue and add the predicted processing time of the incoming job to his queue. He then generates a bid value and sends this to the broker. The broker gets all bid values from the other robots and announces the winner with smallest bid value.
5.2 InSystems Automation Misuse-Case Overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

The analysis focuses on risks that are linked to the robots and their communications. The source of the risks must derive from the use case itself. Legacy systems like the used controllers on a robot or the implementation of the used protocols like MQTT are not in the scope of the misuse case and are seen as a Blackbox.

**Misuse-Case 1: Misbehaving Robot**
Inserting wrong data into the system might influence the strategy component and the broker into changing workflows or the bidding process of new tasks. This can influence other robots and lead to strategy changes, production decrease or a complete robot failure. Also the insertion of wrong information like information on obstacles inside the transportation area can reduce the efficiency of the transportation system and by this can have effects on the assigned production systems.

Under consideration are two types of disruption that could lead to the above mentioned unwanted effects on the use case: a malfunctioning robot and an external attacker.

**Misuse-Case 1a:**
Misuse-Case Type: Functional

For example a robot can be malfunctioning due to a hardware failure like a broken antenna. This will lead to a negative effect on the use case, because the robot can’t reach the broker or other robots and furthermore the robot can’t get new job orders assigned. This will lead to less efficiency.

**Misuse-Case 1b:**
Misuse-Case Type: Security

The other type of disruption is the targeted manipulation of the use case. This can be triggered by the external attacker who gains access to the industrial network so that he can manipulate the communication between the robots or by hijacking a robot to insert wrong data into the robot fleet.

**Misuse-Case 2: Increasing number of transport tasks**
This MUC deals with an overload of the fleet of transport robots due to a significant increase in the number of transport tasks. The fleet is incapable of changing its behavior in advance or in time, leading to unfulfilled transport tasks and blocked machines.

We distinguish here between two different categories of situations with increasing number of transport tasks: regularly appearing peaks in the number of transport tasks and unpredictable peaks. While the short-term effects on the fleet of transport robots are the same for both kinds of situations, the mitigation approaches – and especially approaches for closing mitigation gaps differ.

**Misuse-Case 3: Machine breakdown & involvement of humans**
This MUC deals with the effect insufficient reaction of the fleet to changes the production dynamics due to a machine breakdown.

The MUC is divided into two stages: In the first stage a machine breaks down, which changes the importance of transport tasks raised by another machine. In the second stage, the broken machine gets repaired, leading to human obstacles in the factory floor.

**Misuse-Case 4: Robot breakdown & insufficient strategy choice as response**

This MUC deals with unexpected and undesirable robot behavior and risks in manually changed strategies. In stage 1, we describe wrong behavior because of a robot malfunction and the resulting effects on the task fulfillment. In stage 2, we describe unexpected situations caused by strategy changes.

**Misuse-Case 5:**

If a robot is trained by machine learning techniques, it suffers frequently from adversarial attacks. Adversarial attacks can cause both security and functional damage of industrial systems. Therefore, we defined the machine learning related misuse case in detail and its possible mitigations, to make machine learning models more robust and secure.
5.3 InSystems Automation Misuse-Case – Detailed Review

Time: 12 - 36
Location: InSystems Automation GmbH (Berlin)

5.3.1 Misuse-Case 1 – Misbehaving Robot

5.3.1.1 Misuse-Case 1a – Misbehaving Robot (Functional driven)

5.3.1.2 Misuse-Case 1b – Misbehaving Robot (Security driven)

Assumptions:

For the misuse case scenario we assume that the network is secured by WPA2 and can be broken with a dictionary attack. Furthermore we assume that the robots are already configured and part of the network and the used protocols and frameworks are configured as standard with no individual extensions or adaptations. Authentication of robots is not considered. If authentication is used, it should be the same for all robots. The used hacking tools are based on open source software.

This use case uses the fact that the Wireless communication between the robots is vulnerable and acts as an entrance gate into the further backend. In a staged attack the wireless communication should be broken and malicious messages should be inserted into the communication between the COATY elements. For this purpose a rogue, simulated robot must be created. After the rogue robot became part of the fleet the use case can be sabotaged by inserting wrong data.

Attacker:

The misuse case attacker wants to achieve the following goals:
- Disrupt production environment
- Financial gains and damage
- Prove skills

The attacker’s skill level:
The observed attacker in this misuse case has knowledge about the COATY framework and the MQTT communication protocol as well as the industrial environment. Furthermore he has knowledge about networks specifically wireless networks and uses open source software to reach his goals.
Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 3 attacker. The Level 3 attacker drives intentional attacks, with sophisticated means and moderate resources. He has ICS specific skills and moderate motivation.

Misuse-Case Staging:

The Misuse case has three stages:
1. Breaking of Communication protocol between robot and IT infrastructure (Robot – router) WPA2
2. Replaying or manipulating Data to confuse one robot
3. Attacking the subscribe / unsubscribe / disconnect cycle of the MQTT Framework

4) Breaking of Communication protocol

Stage 1:
- Create A wordlist
- Record WPA communication with Airodump-ng (Kali)
- Catch Password being transmitted by deauthorisation packages
- WPA2 Password with Wordlists

5) Risk ID# 21 (Wrong data communication between robots) or Risk ID# 28 (Wrong data communication between robot and the strategy)

Stage 2:
A replay attack can be used to confuse a robot or to disrupt the systems consistency by injecting already known and in process information. For example an attacker can intercept the communication between the Broker and a robot. The attacker extracts the Job ID and resends this information to the same robot. The victim robot will have two of the same job IDs and can’t decide which job is the valid one. In this case the system is not aware about the two jobs with the same ID.

Possible manipulation could be:
- Mis-use case Risk ID# 26 (Wrong status information is sent)
  - For. Example: manipulating the bid value of a robot during a bidding process can lead to the exclusion of this robot. As described above the robot with the smallest bid value gets a job assigned. If the bid value is everytime manipulated to a bigger value than others the robot will never get a job assigned.
  - Manipulating the order values can lead to a massive delay in fulfilling the job queue in time.
- Mis-use case Risk ID# 30 (Robot sent wrong data to the strategy component)
  - Manipulation of status information can lead also to unwanted effects. An adversary can manipulate the battery health status or the recharge flag value.
  - Robot status information include:
    - Hardware failures
    - Battery health status
    - Token information
    - Job status
6) Option 1: Risk ID#10: Robot can’t reach the broker (Attacking the subscribe / unsubscribe / disconnect cycle of the MQTT Framework)

Another possibility to disrupt the system is to attack the subscribe / unsubscribe / disconnect cycle of the MQTT Framework. MQTT stands for Message Queuing Telemetry Transport. The MQTT Framework is an open messaging protocol for Machine-to-Machine communication (M2M). It transmits telemetry data as messages between devices.

- Already existing robots can be unsubscribed or disconnected from the broker by using the following commands:

5.3.1.3 Unsubscribe robot

To unsubscribe a robot from a topic, the attacker sends the robot ID, the topic(s) he wants the robot to unsubscribe from and the unsubscribe pattern to the broker.

`libmosq_EXPORT int mosquitto_unsubscribe(struct mosquitto *mosq,
int *mid,
const char *sub )`

5.3.1.4 Disconnect a robot

To disconnect a robot from the fleet, the attacker sends the disconnect command with the corresponding robot ID to the broker.

`libmosq_EXPORT int mosquitto_disconnect(struct mosquitto *mosq)`
7) Option 2: Adding a Rogue Robot which publishes wrong data to the broker

5.3.1.5 Connect robot to fleet

To connect a new robot to a fleet, the attacker uses the MQTT CONNECT Function. He includes a valid unique robot ID, the IP address and port number for the communication as well as a keepalive value and sends this to the broker.

```c
libmosq_EXPORT int mosquitto_connect(struct mosquitto *mosq,
    const char *host,
    int port,
    int keepalive)
```

5.3.1.6 Publish new topic

To publish a new topic that other robots can assign, the attacker sends a valid robot ID and the topic to the broker.

```c
libmosq_EXPORT int mosquitto_publish(struct mosquitto *mosq,
    int *mid,
    const char *topic,
    int payloadlen,
    const void *payload,
    int qos,
    bool retain )
```
Countermeasures and mitigations
In this section possible mitigations are briefly listed.

Mitigation 1: Implement signature-based authentication for robots
- To mitigate the risk that the attacker can introduce a rogue device, authentication can be used to hinder unknown devices to be connected to the fleet.

Mitigation 2: Implement authentication for message exchange
- To mitigate the exchange of unwanted communication messages, message authentication codes (MAC) with a one-time session key should be implemented to verify the authenticity of the messages

Mitigation 3: Secure network hardware configuration
- Review the network settings of network hardware to avoid default settings to be exploited

Mitigation 4: Disable unneeded network service
- To reduce the attack surface all unneeded network services should be disabled

Mitigation 5: Apply latest security patches
- Implement latest security patches to all software running on robot fleet ecosystem devices

Mitigation 6: Prevent unauthorized access
- Ensure that passwords are of sufficient complexity and changed periodically

Mitigation Gaps
Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that due to new or unknown vulnerabilities to the robot or the wireless network it will be possible to perform the Misuse-Case. In these cases capabilities are needed to detect the abnormal behaviour of a robot. To develop the capability to detect the abnormal behaviour capabilities need to be developed to monitor the behaviour of the transportation system and the included robots. The development of these capabilities will be addressed as part of Task 5.3 “H/M-Behaviour Watch”.

A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a simulation/model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”
Based on the ITEA 3 PO Template v4.0 (August 2017)
Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay the average transport time [%]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decreasing throughput [Transport per hour]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disturb Robot Fleet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type 44</th>
<th>Owner</th>
<th>Uses 45</th>
<th>Access 46</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Hacking Tool (Aircrackng)</td>
<td>Software</td>
<td>Open-source</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

5.3.2 Assumptions (for all of the following three MUCs)

- The capabilities of the fleet of robots is as described in D2.2:
  - Robots can navigate autonomously.
  - Robots communicate with each other (via a broker) for distributing transport tasks among the fleet. The distribution is induced by a given strategy that is shared by all robots of the fleet.
  - The strategy of a fleet can only be changed manually (e.g. by the plant manager). The robots do not change their behavior on their own.
  (In the risk table, we already refer to a „strategy component“, which is supposed to manage automated changes of strategies. This is not yet implemented, but one of the desired results of the project.)

5.3.3 MUC 2 – Increasing number of transport tasks

This MUC deals with an overload of the fleet of transport robots due to a significant increase in the number of transport tasks. The fleet is incapable of changing its behavior in advance or in time, leading to unfulfilled transport tasks and blocked machines.

We distinguish here between two different categories of situations with increasing number of transport tasks: regularly appearing peaks in the number of transport tasks and unpredictable peaks. While the short-term effects on the fleet of transport robots are the same for both kinds of situations, the mitigation approaches – and especially approaches for closing mitigation gaps – differ.

44 Data, Hardware, Software, Operational System, Information System, Testing Platform
45 Select one or several: development, testing, validation, training, demonstration
46 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
5.3.3.1 Initial Situation

- operating fleet of robots in the plant
- no malfunctions on robots, machines and related components
- Utilization of machines and robots is low – only a low number of transport tasks is raised by machines, fleet has no problem by fulfilling all tasks in time
- All robots are behaving according a given strategy: new tasks are distributed among all robots that will finish their local queue in the next 20 min. The robot with the highest battery level gets the task. Robots add a charging job to their queue, if they only have 40% battery left (charging up to 60%, mandatory charging job). All robots use spare time for charging (optional charging job). Charging in spare time can be cancelled at any time for starting a transport job.
- 4 machines M1, M2, M3, M4. M1 & M2 are producing the same product, just using some resource from the storage. M3 and M4 are producing the final product. M3 and M4 need the output of M1/M2 and some additional resources from the storage as input. The whole resource flow between machines and the store is shown in Figure 1.

![Figure 1: Flow of resources in the plant example](image)

5.3.3.2 MUC 2a: regularly appearing peak

The initial situation is as described above: the utilization of machines is low and the robots can fulfill all of their transport tasks by following their strategy.

As every day around at 8am, the factory is switching from night mode to day mode, as the human employees start their shift: The part of the storage, which is used by the robots, gets refilled since new material arrives and machines that were turned off at night are now switched on and are waiting for material for starting production. Hence, the number of transport tasks per time span is increasing.

The robots receive those transport requests and are distributing them as before: the robot with the highest level of battery which will finish is local queue in the next 20 minutes is taking the job. While the number of tasks increases, the idle time of robots decreases, leading to reduced number of possibilities for optional charging jobs. Therefore, the robots now rely on mandatory charging jobs. As more and more transport tasks are requested by machines, the local queues of
Based on the ITEA 3 PO Template v4.0 (August 2017)

all robots get longer and longer, still all robots are occupied for at least 20 Minutes. Consequently, no robot offers to take over a new transport task and new tasks are no longer fulfilled. This causes the respective machines to stop due to a lack of input material or an overflow of produced goods. In the worst case, the production totally stops. Since this peak of transport tasks is appearing every morning, machines regularly have to stop due to unfulfilled transport tasks.

This misuse case is related to the following risks

- RobotFleet010 (Lack of information): The choice of strategy for the fleet is based on incorrect information/predictions, since here is no information given at all to entities that can reconfigure the chosen strategy.
- RobotFleet27 (Incomplete model): The fleet does not consider reoccurring production patterns in its context model.
- RobotFleet28 (Unaccomplished goals): Since there is no adaption of the chosen strategy, the fleet is no longer fulfilling the goal of fulfilling all transport jobs; another strategy could have accomplished the goal.

Mitigations

- Human employees can observe the fleet and the machines, and take care of transport tasks that are not considered by robots. Of course, this solution is expensive, especially as the problems are occurring on a regular basis.
- The number of robots in the fleet can be increased.
- The strategy of robots can be reconfigured manually whenever the plant manager observes problems.
- If it is possible to adjust the utilization of the machines in night mode and in day mode, regularly appearing peaks can be avoided. This mitigation requires a major change in the whole production flow.

Mitigation Gaps

At the actual development status, the fleet of transport robots is not able to adapt its behavior in terms of strategy-reselection on its own. Additionally, the fleet is not able to identify patterns in the behavior of machines (like a daily reoccurring increase in the utilization) or even use information on those patterns for predictive behavior reconfiguration. In more detail, the following capabilities of the fleet are missing, but would help to avoid this misuse case:

- Identification of reoccurring patterns in the production dynamic
- Ability to predictively adapt the behavior in order to deal with reoccurring situations. This capability is mitigating the likelihood of the occurrence of risks like RobotFleet27 and RobotFleet28.
- Ability to check if a strategy is suitable for a situation or time frame before actually applying the strategy. This capability is mitigating the likelihood of the occurrence of risks like RobotFleet27 and RobotFleet28.
- Ability to check if the above mentioned methods for mitigation are really leading to mitigations of the effect of the risks. For example, additional robots in the fleet may not lead to increased efficiency of the fleet, but to jams of robots on some paths in the factory.

Those mitigation approaches will be tackled in T4.2 (characterization of production dynamics) and T5.4 (increasing resilience of the fleet by supporting decision making). In T3.1 (simulation and modeling of CPS), needed models as input for T4.2 and T5.4 are developed.
5.3.3.3 MUC 2b: unpredictable increase

The initial situation is as before. Due to an urgent and unexpected order of an important costumer, the utilization of the machines is raised, i.e. more final products in the same time are required. Hence, the number of transport tasks is increasing. Even if the types of transport tasks remain the same (e.g. no change in the sources & sinks, types of goods to be transported remains as before), the robots are occupied most of the time with fulfilling transport jobs or doing mandatory charging jobs. As in MUC 1a, there is nearly no time left for optional charging jobs. Hence, it can happen that all transport robots are occupied for the next 20 minutes, such that there is no robot available for taking over new transport tasks. Those tasks are not fulfilled at all, leading to machines running out of material or having to stop due to material jams. In summary, the strategy of the robots does not fit to the situation anymore, which causes production delays.

This scenario is related to risk RobotFleet28 (unaccomplished goals): The robots do not adapt their behaviour to the actual situation. In the actual implementation, the only possibility to change the strategy of robots is by manual changes, which is not done here.

Countermeasures and Mitigations
In this section possible mitigations are briefly listed.

- Human employees can observe the fleet and the machines, and take care of transport tasks that are not considered by robots. Of course, this solution is expensive, especially as the problems are occurring on a regular basis.
- The number of robots in the fleet can be increased.
- The strategy of robots can be reconfigured manually whenever the plant manager observes problems.

Mitigation Gaps
Unpredictable changes in the plant can always occur, no existing model can deal with all possible behavior of an open context in an appropriate way. During the project runtime, we plan to develop methods for the identification of such unpredicted behavior of the plant (anomalies) in T5.3. This requires a characterization of anomalies and methods for observing the plant behavior and comparing it to assumptions on plant behavior. The results can be used for supporting appropriate decision making (T5.4). T3.1 is developing the underlying models for supporting decision making and for later evaluation purposes.

5.3.4 MUC 3 – Machine breakdown & involvement of humans

This MUC deals with the effect of insufficient reaction of the fleet to changes the production dynamics due to a machine breakdown. The MUC is divided into two stages: In the first stage a machine breaks down, which changes the importance of transport tasks raised by another machine. In the second stage, the broken machine gets repaired, leading to human obstacles in the factory floor.

5.3.4.1 Initial Situation

- Same plant, machine set and robot fleet as in MUC2
- Machine utilization is increased (because of reasons like in MUC2), such that the robots have nearly no time for optional charging jobs and there are delays in the fulfillment of transport tasks

Stage 1: Machine breakdown
Machine M1 is shutting down due to a hardware failure. Hence, M1 is no longer able to produce anything and stops generating transport tasks. Since M2 is producing the same intermediate product as M2 and machine M2 is still operating, the overall production process can go on without M1. Nevertheless, machine M2 is now crucial for the overall production flow, because it is the only
remaining machine producing material as input for M3 and M4. The utilization of all remaining machines is still high. Even if M2 produces the same product as M1, M2 cannot balance the production loss by its own. This decreases the number of transport tasks in a given frame of the product from M1 and M2. Even if the request of M3 and M4 is still high, they get fewer resources and can’t produce the same number of products as before. Hence, the number of transport requests ordered by M3 and M4 decrease.

Due to the high utilization of the machines and the currently applied strategy of the robots (cf. MUC 1), there already are delays in the fulfillment of transport tasks. This delay is also applying to the transport jobs raised by machine M2. The fleet is behaving as before, transport jobs of M2 are treated as transport tasks of all other machines. This leads to a higher probability of production stops: machines M3 and M4 are depending on products of M2. If M2 has to wait for the fulfillment of transport tasks, M3 and M4 also have to wait, which lowers the production rate of the plant.

**Stage 2: Blocked path**

In this stage, M1 is still broken and problems described in Stage 1 still hold. A handyman arrived to fix machine M1. The repair process for M1 consumes some space, such that the path in front of M1 is blocked. Robots can’t pass the path anymore, but there are alternative but longer routes which avoid the area around M1. The robots do not know about the blocked path and can’t communicate any information on that obstacle. Hence, if a robot tries to use the path in front of M1, it learns about the obstacle the moment it identifies it with its own sensors. After the obstacle recognition, the robot locally plans a new path to its destination, using an alternative and longer route, which takes more time and leads to an increase in the transportation time.

In the distribution of transport jobs over the fleet of robots, the robots which have not yet faced the obstacle, do not consider information on blocked paths. Hence, some robots calculate their bids under the assumption of being able to pass M1. Consequently, the bids of those robots are lower than their actual costs for doing the transport job. The robot with the lowest bid gets the transport job. Due to bid calculation under wrong assumptions, a robot can win the bid which not has the lowest costs. We get a suboptimal distribution of transport tasks, which results in more task delays and violation of optimization goals like equal wear and tear of robots.

This misuse case is related to the following risks

- RobotFleet010 (Lack of information): The current strategy assumed, that M1 is still working.
- RobotFleet027 (Incomplete model): Current model doesn’t consider effects by broken machines
- RobotFleet028 (Unaccomplished goals): Since there is no adaption of the chosen strategy after the failure of M1, the fleet is no longer fulfilling the goal of fulfilling all transport jobs according to optimization goals; another strategy could have accomplished the goal.
- RobotFleet036 (Wrong map information): Robots don’t know the existence of the road blocking toolbox until they notice themselves.
- RobotFleet042 (Bid value too low)
- RobotFleet044 (Wrong robot is picked as winner)
- RobotFleet049 (Obstacle information is not shared)

**Countermeasures and Mitigations**

In this section possible mitigations are briefly listed.
- Decrease utilization of M3, M4
- Human employees can observe the fleet and the machines, and take care of transport tasks that are not considered by robots. Of course, this solution is expensive, especially as the problems are occurring on a regular basis.
- The number of robots in the fleet can be increased.
- Establishment of additional behavioral rules for humans on the production floor, such that the handyman is not blocking any paths

Mitigation Gaps
This MUC describes how changes in the production flow without the ability to react to those changes lead to suboptimal behavior (task distribution) of robots and hence to a reduction of efficiency of the whole factory. Actually, the robots are neither able to observe nor to understand the production flow and cannot detect irregularities. Additionally, implausible robot behavior, for instance caused by incorrect bidding or task delays by longer transport routes, is not observed. In task T4.2, we plan to tackle the problem of missing characterization of production dynamics and monitors for observing production dynamics. This enables the identification of anomalies (T5.3) as triggers for reconfigurations of the fleet behavior. Task T3.1 is delivering needed models for WP4 and WP5 and for the later demonstration of the methods resulting from T4.2 and T5.3.

5.3.5 MUC 4 – Robot breakdown & insufficient strategy choice as response
This MUC deals with unexpected and undesirable robot behavior and risks in manually changed strategies. In stage 1, we describe wrong behavior because of a robot malfunction and the resulting effects on the task fulfillment. In stage 2, we describe unexpected situations caused by strategy changes.
Initial situation:
- End of MUC2
- M1 is still not working because the handyman has to wait for a hardware delivery
- But the handyman has removed his toolbox, such that all paths in the plant are again free of obstacles

Stage 1
In this stage, one robot has a hardware failure and is not able to move any more. Nevertheless, the communication to the fleet is still working. Hence it is still communicating, calculating bid values and getting new transport tasks, but cannot execute any jobs. The transport tasks are not fulfilled, although all tasks are distributed among the fleet. We notice that an entry in a robot queue does not guarantee, that the task is in execution or will in the future. Because the robot can’t move to its charging station, his battery decreases monotonously until it becomes empty. Then all tasks in his queue will be lost for the future. The missed delivery will reduce the production rate of the factory. Additionally the robot blocks other robots and becomes an obstacle for them. This leads to longer transport paths and more task delays.

Stage 2
Up to Stage 1 of this MUC several problems occurred. Now the plant manager decides to react to the upcoming issues and change the strategy for the robots. He chooses a strategy that prioritizes transport tasks involving machine M2 by always demanding robots to wait in the area around M2, whenever robots are idling. Additionally, all robots exclude the broken robot from the bidding process according to the new strategy. As a consequence, more robots are transporting products from and to M2 or are idling around M2. This intuitively fits to plant manager’s intention. Unfortunately, the new task distribution leads to much more traffic near M2. The result is a jam of robots near M2, such that all robots stop and wait instead of fulfilling tasks. No products are delivered and the production of the factory is totally shutting down. Obviously, this is not desired from the plant manager.

This misuse case is related to the following risks:
- RobotFleet011 (Wrong information): When the initial strategy of the robots was applied, it was assumed that all of the robots of the fleet are able to fulfill all tasks of their local queue.
- RobotFleet019 (Wrong status information is sent): The broken robots sends transport ability
- RobotFleet022 (Robot sent wrong data to the strategy component).
- RobotFleet024 (Robot sends wrong job status information): The broken robot still sends information on future fulfillment his transport tasks.
- RobotFleet028 (Unaccomplished goals): Since there is no adaption of the chosen strategy after the failure of M1 and the broken robot, the fleet is no longer fulfilling the goal of fulfilling all transport jobs; another strategy could have accomplished the goal.
- RobotFleet029 (Unintentional wrong strategy implementation): The plant manager changes to a new strategy without knowing upcoming issues like jams of robots, leading to a shutdown of the logistic system.
- RobotFleet039 (Wrong status information).

Countermeasures and Mitigations
In this section possible mitigations are briefly listed.

- Human employees can turn off the broken robot manually, such that it can no longer take over new transport jobs.
- The number of robots can be decreased to solve the robot jam.
- Local jam handling (by humans or by a protocol/algorithm)

Mitigation Gaps

In this MUC we observed a robot who is not moving and fulfilling transport tasks but still sending contrary status information. In order to react to such drawbacks by reconfiguration of the used strategy, the ability to find differences between the predicted behavior of robots and the observed behavior is needed. This capability is planned to be developed in task T5.3.

Even if there are plausible reasons to change to a specific strategy, it can lead to unintended and suboptimal effects like sketched in stage 2 of the MUC. Hence, we need to check the consequences of strategy reconfigurations before actually applying it. If the consequences of applying a specific strategy is known, this information allows the choice of strategies such that the overall performance of the fleet of transport robots is increasing.

To realize this by simulation, we need basic models of production relations and robots behavior, which will be done in T3.1. These predictions of strategy effects and countermeasures to upcoming anomalies is covered by T4.2 and T5.4.

---

5.3.6 MUC 5 - Machine learning related MUC (Frauenhofer AISEC)

Mis-use cases (Machine learning related) can be divided into two phases:

During/before the training:
1. Wrong strategy (incorrect loss/reward function)
If the robot is trained by machine learning technique, especially reinforcement learning, it suffers from a bad reward function problem. Wrong or improper reward function can cause undesired/inefficient behaviors.

2. Data poisoning (Data in the data lake is wrong labeled)
Data poisoning can be intentional or unintentional, both will lead to a wrong result/prediction.

**After model/system is learned:**

1. Adversarial attack (trained model/system is not robust against perturbed inputs)
   - Modification by manipulating input data, such as modified images/signals or different nature condition to a single robot, in order to change robots' prediction. It can cause damages of (single) hardware and injuries of surrounding mankind. If the robots are machine learning based, this can be considered as an adversarial attack.
   - For example:
     - Dim the light (human intended) will change sensor behaviour/prediction (speeding up instead of stopping).
     - Wrong strategy: the robot is trained by using wrong reward function, which is related to RobotFleet010' and 'RobotFleet011'
     - **Wrong detection the obstacle or other inputs, this is similar to 'RobotFleet015'**
     - Robot doesn't correctly recognise signs/symbols
     - The robot predict wrong result and send it out to other robots, which is related to 'RobotFleet019'

2. Anomaly samples
   - Detail: Anomaly samples means the correct samples which have unusual features, the possible result is wrong prediction of robots.

**Countermeasures and Mitigations**

In this section possible mitigations are briefly listed.

- Incorrect reward function can be observed by training results of robots.
- Human recheck, more data inputs and regularization terms can mitigate the effect of wrong data labels
- Estimation of robustness can measure the severity level of adversarial attack
- Adversarial training can mitigate the cause of adversarial attack
- Anomaly detection methods can find out anomaly samples

**Mitigation Gaps**

In this machine learning related MUC we find out machine learning based robots easily suffer from adversarial attack by receiving manipulated inputs. Although those manipulated modification can be intentional and unintentional, both will lead to wrong prediction. These unpredictable results can cause possible consequences, such as damage of hardware and injuries of human beings, the effect of adversarial is wide and severe.

Before training process, we have to ensure we have the proper reward function by observing the performance of robots. Besides, we need to make sure we have amount of correctly labelled data.

After the robot is trained, we first need to evaluate its robustness by state-of-the-art criteria, if the model is not robust as we need, we apply the adversarial defences, such as adversarial training to trained model. The capability is planned to be developed in task T5.2.

The capability to detect anomaly samples will be presented in task T5.4
6 Misuse-Cases on Bombardier Transportation GmbH use-case
6.1 Bombardier Transportation Use-Case overview

Bombardier Transportation is in the process of transforming its individual locations. The Bautzen site becomes a lead site for the final assembly of various types of rail vehicles. The provision of small parts and large components on the various levels of the production lines is currently carried out exclusively manually. The goal is to have a safe and automated provision of the material with its various dimensions.

The use case consists of the following components:

- **MES**: The MES component delivers the jobs to the work station and collects the responses of the work station that are triggered by the worker.
- **ERP**: The ERP component generates and distributes jobs to the MES and GANTT systems.
- **GANTT**: The GANTT System knows which task is currently active and in progress as well as when it is due. The GANTT System feed the robots with new jobs.
- **Robot**: The robots are connected to the GANTT over the Wi-Fi router. The robots collect job and deliver material.
- **Work Station**: The work station is the place where the robot delivers the material to and the worker is installing the delivered material.
- **New box**: Stores material to be built in, can be picked up at lean zone
- **Old box**: Is empty, must be picked up at work station and delivered to lean zone

The ERP system generates and distributes new jobs to the MES and GANTT system. The MES sends the jobs to the work stations. The GANTT system gets the jobs from the ERP system and feeds the available robot(s). The jobs are assigned to available robots.

A work station can consist of three levels, named ground level (G), level 1 (L1) and level 2 (L2). Each level can hold one box at a time. Before a new box can be delivered the old box must be picked up.

A robot can’t exchange an empty box with a new box in one step. So before a robot can drop off a new box the destination work station must be empty. But the robot can offload a new box and on his way to the lean zone he can pick up old boxes from other workstations or levels.
6.2 Bombardier Transportation GmbH misuse case overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

The analysis focuses on risks that are linked to the robots and their communications. The source of the risks must derive from the use case itself. Legacy systems like the used controllers on a robot or the implementation of the used software and protocols are not in the scope of the misuse case and are seen as a blackbox.

**Misuse-Case 1: System manipulation**
In a staged attack the wireless communication should be broken and the central management of the robot fleet will be attacked.

Under consideration are two types of disruption that could lead to different unwanted effects on the use case: a malfunctioning robot and an external attacker.

**Misuse-Case 1a: Malfunctioning Robot**
*Misuse-Case Type: Functional*

For example a robot can be malfunctioning due to a hardware failure like a broken antenna. This will lead to a negative effect on the use case, because the robot can’t reach the GANTT system or other robots and furthermore the robot can’t get new job orders assigned. This will lead to less efficiency.

**Misuse-Case 1b: Manipulation by external attacker**
*Misuse-Case Type: Security*

The other type of disruption is the targeted manipulation of the use case. This can be triggered by the external attacker who gains access to the industrial network so that he can intercept the communication between the central management and the robots.
6.3 Bombardier Transportation GmbH misuse Case – Detailed Review

Time: (Type duration in months)
Location: Bombardier Transportation GmbH (Bautzen)
Scope:

Remark: Due to the fact, that the use case is in an early stage and no specific product was chosen before the creation of this document, it is possible that the following paragraphs include generic attacks and descriptions.

6.3.1 Misuse-Case 1a (Manipulation by external attacker)
In general robot central management systems generate json job files that are then send to the robot over an unencrypted wireless communication. This fact can be used by the attacker to drive replay attacks like inserting the same job instances but with different job information for example loading height, destination work stations, pick up zones and so on. Inserting the same jobs might influence the strategy and can influence other robots and lead to strategy inefficiency or production decrease.

One case where people and material damage can occur is, when the attacker manipulates the loading height. For example if there is a one level train in the assembly and the attacker manipulates the loading height like for a two level floor train and the robot then drops off his box from the second level then people and material damage is caused. Also the robot can break down by falling objects, what will lead to a decrease of efficiency.

Assumptions:
For the misuse case scenario we assume that the network is secured by WPA2 and can be broken with a dictionary attack. Furthermore we assume that the robots are already configured and part of the network and the used protocols and frameworks are configured as standard with no individual extensions or adaptions.

Attacker:
The misuse case attacker wants to achieve the following goals:
- Disrupt production environment
- Damage materials
- Damage people
- Prove skills

The observed attacker in this misuse case has knowledge about the industrial environment and the used robotic products. Furthermore he has knowledge about networks specifically wireless networks and uses open source software to reach his goals. Involving the aforementioned skills and in relation to the IEC62443 the attacker is classified as level 3 attacker. The Level 3 attacker drives intentional attacks, with sophisticated means and moderate resources. He has ICS specific skills and moderate motivation.
Misuse-Case Staging:

The Misuse-Case has three stages:

5. Gain access to the robot central management communication
6. Send

8) Break Communication Protocol

Stage 1:
- Create a wordlist
- Record WPA communication with Airodump-ng (Kali)
- Catch Password being transmitted by deauthorisation packages
- WPA2 Password with Wordlists

9) Gain access to Robot Central Management communication

Stage 2:
In the next step the attacker intercepts the communication between the central management of the robot fleet and the robots.

Commonly central management systems of robots are based on the json protocol. They generate jobs (json files) where all necessary information is stored to fulfill the jobs. The system sends this job file via an unencrypted wireless communication to the robot. This circumstance is utilized by the attacker to intercept packages and to manipulate the job information.

Stage 3: Drive attacks

10) Option 1: Insert fake tasks into robots queue (replay)

Due to the fact that the attacker has direct access to the jobs that are send between the central management and the robots, he can drive replay attacks. Replay attacks are used to resend the same messages/jobs, so that the robot or the system get confused and stop working. This will lead to decreased efficiency in production.
11) Option 2: Change box order / drop off destination

To disrupt the transportation system the attacker could change the destination work station in a job file. Imagine we have an assembly line with 10 work stations. The job for the robot is, take new box from lean zone pickup area 1 and drive the material to work station 5. The attacker manipulates the destination work station information from 5 to 1. The robot will deliver the box to the work station 1 instead to work station 5. This lead to a delay in the production process.

In another case the attacker can change the box order in the lean zone. For example imagine the lean zone has 6 pickup areas for new boxes. The attacker manipulates a job for a robot to lift the box from pickup area 1 and drop off the box at pickup area 5. This will lead to the problem that the next job that needs the box from area 5 will get the wrong material which was intended for area 1. To hide this attack, the attacker can do it once in two weeks, for example every Wednesday. This will lead to confusion in the assembly team and an unpredicted decrease in production.

12) Option 3. Change drop off height

Another serious attack aims at the drop off height of a job. In this case the attacker can adjust the drop off height from first floor (F1) to second floor (F2). This can cause serious damage to people and the material as well as the robot itself in the case the work station does not have a second floor. The box will then drop off the second floor height down to the first floor.

13) Option 4. Disconnect robot from fleet

To decrease the robot fleet and the interrelated efficiency the attacker can send a robot disconnect command, so that the robot disconnects from the robot fleet and is no longer able to fulfil his assigned tasks.

Countermeasures and mitigations

In this section possible mitigations are briefly listed

Mitigation 1: Implement authentication for message exchange

- To mitigate the exchange of unwanted communication messages, message authentication codes (MAC) with a one-time session key should be implemented to verify the authenticity of the messages and to mitigate replay attacks
Mitigation 2: Simulation
- To prevent unwanted effects, any change or modification of the system should be simulated and acknowledged before going into service. Simulations are cost effective and uncover blocking points or unwanted effects.

Mitigation 3: Monitoring
- Another mitigation strategy is the monitoring of the robot fleet to check the health status of each robot, and to have an overview which tasks do the robots have and in which status they are.

Mitigation 4: Secure network hardware configuration
- Review the network settings of network hardware to avoid default settings to be exploited

Mitigation 5: Disable unneeded network service
- To reduce the attack surface all unneeded network services should be disabled

Mitigation 6: Apply latest security patches
- Implement latest security patches to all software running on robot fleet ecosystem devices

Mitigation 7: Prevent unauthorized access
- Ensure that passwords are of sufficient complexity and changed periodically

Mitigation Gaps
Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that due to new or unknown vulnerabilities to the robot or the wireless network it will be possible to perform the Misuse-Case. To further protect the transportation systems capabilities have to be developed to ensure resilience and trust inside the robot fleet. Developing such capabilities will be addressed as art of Tasks 5.1 “Human/Machine access & trust management” and Task 5.4 “Cyber-resilience mechanisms”. Also with further capabilities of trust management highly resilient FoF systems have further to expect an breach of current and future security mechanisms which afterwards enables an attacker to perform the described Misuse-Case. In these cases capabilities are needed to detect the abnormal behaviour of a robot.

To develop the capability to detect the abnormal behaviour capabilities need to be developed to monitor the behaviour of the transportation system and the included robots. Also capabilities need to be developed to train employers to detect abnormal behaviour or to analyse the underlying reason leading to the abnormal behaviour. The development of these capabilities will be addressed as part of Task 5.3 “H/M-Behaviour Watch”.

A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a simulation/model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”. Digital models created as part of this task should also be used as base for training employers regarding abnormal behaviour.
Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delay the average transport time [%]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Decreasing throughput [Transport per hour]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disturb Robot Fleet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{47})</th>
<th>Owner</th>
<th>Uses(^{48})</th>
<th>Access(^{49})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wireless Hacking Tool (Aircracking)</td>
<td>Software</td>
<td>Open-source</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

\(^{47}\) Data, Hardware, Software, Operational System, Information System, Testing Platform  
\(^{48}\) Select one or several: development, testing, validation, training, demonstration  
\(^{49}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type\textsuperscript{47}</th>
<th>Owner</th>
<th>Uses\textsuperscript{48}</th>
<th>Access\textsuperscript{49}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
7 Misuse-Cases on Machine use-case
7.1 High Metal Overview

High Metal develops highly automated food production line of the future used for cheese making. The aimed functionalities are the more precise measurement of raw materials and product, and as brand new features, traceability and proactive process control that continuously predicts the process flow and adjusts set values in real time, e.g. based on the raw material attributes. This development has a great significance, from the perspective of consumers to manufacture food products with consistent quality and sufficient shelf-life, from the perspective of authorities with the food safety regulations, and from the perspective of production process with the quality control.
7.2 High Metal misuse case - Detailed Review

**Time:** 12 months  
**Location:** Vantaa, Finland  
**Scope:** Traceability and the continuous quality control are among the other important development issues. The most important issue is to ensure 100% cyber security in the whole cheese making process. Agri-food is a very demanding industry in which a malicious third party intending to disrupt food manufacturing or to add bacteria could make it easily, unless the sensors’ firmware and data chain are secured by suitable methods. We will develop continuous risk based threat management and automated firmware updates through reliable connections to prevent attackers from disrupting the cheese manufacturing process.

7.2.1 Misuse-Case - Traceability incident affecting health and safety  
**Misuse-Case:** Dangerous elements or other hazardous material (e.g. bacteria) from the production process ends up in the final product

This misuse-case comprises industrial sabotage done by either an employee or a malicious third party with the intention of disrupting the production line and causing production delays. In case the product ends up in the market shelf, this incident - when discovered - results into the need of pulling an entire product batch off the market, which is costly, but causes also critical harm to the company brand.

**Assumptions**

For this misuse case, we assume that the attacker would be able to gain access to the cheese production line in order to

1. add the hazardous material to the production process, and
2. manipulate or disable the sensors monitoring the cheese making process and warning about any anomalies in the process.

Another potential attack method relates to the production line remote access in which the attacker would try to change the temperature or other production line device settings in order to change the recipe or initiate bacterial growth that way. This would also require disabling the sensors monitoring the cheese making process. Since this would require extremely sophisticated attack methods and comprehensive understanding of the production line devices and systems, this attack method is considered to be almost impossible and thus not included in the misuse case.

**Attacker:**

The attacker wants to achieve the following goals:

- Cause additional costs by disrupting the cheese making process and/or manufacture products that do not meet the quality requirements
- Causing bad reputation to the company if contaminated or bad products end up in the market shelf and have to be pulled off
- Gain competitive advantage (competitor) or financial benefit (individual hacker) by causing production delays or shutting down the production line completely.
The attacker’s skill level:

The attacker needs to have the necessary social engineering skills and/or suitable network (e.g. production facility personnel) in order to gain access to the production facility. This can be made possible e.g. by gaining access to the device manufacturer, maintenance company or other third party actor. Since this is an agri-food misuse-case, the attacker should also have knowhow about the regulation and policies in order to pass the security and food safety measures.

The attacker should have extended knowledge about the production line devices, security controls and quality control/monitoring system in order to be able to add hazardous material into the production mass or manipulate the process in such a way that production personnel cannot discover the change. The attacked should also have the required technical knowledge to manipulate the quality control/monitoring system and sensors in such a way that they don’t detect this anomaly and also be able to delete any traces in the system about this manipulation.

In order to succeed in the task of products ending up in the market shelf and resulting into bad company reputation, the attacker should be able to understand how to manipulate the production process in just the right way so that it is not discovered until after a very long time.

Misuse-Case Staging:

The Misuse case has three stages:

1. Enter the facility and pass the necessary security and safety controls
2. Gain access to the cheese production line and manufacturing equipment
3. Perform the attack which consists of
   - manipulating the quality control/monitoring system sensors so that they cannot discover the changes in the production line
   - adding the hazardous material into the production line or manipulating the production line settings (e.g. temperature) in such a way that bad products are manufactured.

<table>
<thead>
<tr>
<th>1) Enter the facility and pass the necessary security and safety controls</th>
</tr>
</thead>
</table>
| Stage 1:  
The attacker should be able to gain access to the production facility (check similar Risk ID IoT0014) |

| 2) Gain access to the cheese production line and manufacturing equipment |

Based on the ITEA 3 PO Template v4.0 (August 2017)
2) Gain access to the cheese production line and manufacturing equipment

Stage 2:
In this step the attacker accesses to the cheese production line related manufacturing process and performs the attack (check similar Risk ID, e.g. Electronics 0002, Textile 0010).

Stage 3: Perform the attack

Phase 1: manipulate the quality control/monitoring system sensors so that they cannot discover the changes in the production line

Manipulation can be done by e.g. changing the quality control system settings so that the allowed temperature range is increased. Another way is to manipulate the sensors in such a way that the metrics data that they send is always within the allowed range.

Phase 2 - Option 1: add the hazardous material into the production line

Add bacteria or other hazardous material into the production line

Phase 2 - Option 2: manipulate the production line settings (e.g. temperature) in such a way that bad products are manufactured

This option requires access to e.g. production line devices controlling the temperature of the cheese

Countermeasures and risk mitigation methods
The possible mitigation measures are the following:

*Mitigation 1: Prevent unauthorized access via physical and digital access control mechanisms*
  - Access to the premises: Ensure that the cheese production facility has sufficient physical access control (passage control) system
  - Ensure that the production line manufacturing devices are using sufficient identity and access management (IAM) system consisting of personal usernames + passwords. The IAM system should also have periodically changing passwords or possibly strong two-factor authentication

*Mitigation 2: Implement access monitoring controls for passage control and IAM*
- The IAM system (including the physical passage control) should have a monitoring system for detecting unauthorized access (attempts) and any anomalies within the system should result into a notification to security personnel.

**Mitigation 3: Additional confirmation of any changes to critical system settings**

- To prevent any manipulation of the quality control/monitoring system, any changes to the sensor and/or system settings should be confirmed by some other user (e.g. supervisor) before putting the changes into production. For this purpose, we can use e.g. simulation in the digital twin to confirm that the setting changes are feasible and desirable.
- The monitoring system log files should consist of all changes along with user, timestamp and possible confirmation information.
- The monitoring system should

**Mitigation 4: Continuous monitoring of the production line and assets**

- To reduce the attack surface of each of the assets, continuous monitoring should be enabled. This requires extended knowledge about the assets, their software versions, default and current settings. The monitoring system should also include alerts related to any changes in critical systems (e.g. quality control system) or their settings. It should also be able to generate alerts if e.g. software patches result into a change of these aforementioned settings.
- Continuous monitoring of assets

**Mitigation 5: Implement only necessary network services and interfaces**

- To reduce the potential attack surface, all unused/unnecessary network services and interfaces should be disabled.
- The monitoring system should monitor the status of network services and interfaces and generate an alert in case any aforementioned ones are discovered (e.g. after a firmware patch)

**Mitigation 6: Apply the latest security patches**

- Implement latest security patches to all software running on assets
- Create a system to monitor the status of all assets (like version, SW update, misbehavior of the system)

**Mitigation Gaps**

Even though the mitigations listed in the previous section should result into a more resilient system thus making it harder for the misuse-case to occur, new functionalities and updates to the system firmware or software make it possible for the attacker to attack the system. An example of this is the previously mentioned attack using remote access to the production facility. Developing these aforementioned capabilities will be addressed as part of Tasks 5.1 “Human/Machine access & trust management” and Task 5.4 “Cyber-resilience mechanisms”.
To develop the capability of detecting anomalies, we need to also monitor the behaviour of the systems and users within the production line and monitoring should also include partner companies providing the cheese production manufacturing devices and companies performing maintenance to the devices and systems.

We also need to develop the capability of production line workers and supervisors to detect abnormal behaviour and other anomalies within the production line and perform immediate mitigation actions according to proactive training and provided guidelines. The development of these capabilities is done as part of Task 5.3 “H/M-Behaviour Watch”.

The detection of abnormal behaviour can be made by comparing the detected behaviour to normal behaviour. This requires generating an expected or normal behaviour model. Therefore we need to develop capabilities to model Cyber-Physical Systems and their normal behaviour. The development of these capabilities are addressed as part of Task 3.1 “CPS-Modelling and Simulation”. We should also use the digital models created as part of this task as a base for training employees to detect any abnormal behaviour.

In distributed manufacturing cases, the optimization of Data-lake through visualisation (T4.2) and means of distributed manufacturing (T4.4.) control are considered.

**Identification of key assets (misuse case)**

Please note that the following assets are at PoC level and not available for misuse case demonstration purposes at least currently.
<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{50})</th>
<th>Owner</th>
<th>Uses(^{51})</th>
<th>Access(^{52})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attack SW/HW</td>
<td>HW+SW</td>
<td>Attacker</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Cheese production devices</td>
<td>HW+SW</td>
<td>High Metal/Customer</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Identity and Access Management system</td>
<td>Information system</td>
<td>High Metal/Customer</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Sensors</td>
<td>HW</td>
<td>High Metal/Customer</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Quality control/monitoring system</td>
<td>Information system</td>
<td>High Metal/Customer</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td># of detected anomalies within the IAM system</td>
<td>Not available</td>
<td>Real-time measurement</td>
<td>Continuous</td>
</tr>
<tr>
<td># of detected anomalies within the quality control/monitoring system</td>
<td>Not available</td>
<td>Continuous monitoring by sensors</td>
<td>Continuous</td>
</tr>
</tbody>
</table>
8 Misuse-Cases on IDEPA use-case
8.1 IDEPA Use-Case Overview

In the context of its digitalization IDEPA invested in an ERP system in order to manage its whole activities. The goal here is to keep on investing in this system to increase efficiency, security, safety and resilience. Moreover, being able to provide Data and Knowledge as a service is a critical asset to answer the market needs and to achieve IDEPA business transformation. The main challenge of this use-case is to provide knowledge as a service and include a cyber-security awareness module into Sistrate ERP/MES and an increased set of services as such as environmental sensors or network sensors to assure the safety, security and resilience of manufacturing systems, achieving a holistic optimization and intelligent decision support of factories.
8.2 IDEPA Misuse-Case Overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

Misuse-Case 1: Misbehaving Machines/Services

Inserting wrong information into the loom or even inserting the incorrect raw material will influence the quality of the final product. This can also cause a complete failure of the loom, which will affect not only the current service order, but also the next ones. All these problems will conduct to a production decrease and bring additional costs to the company.

Misuse-Case 1a:
Misuse-Case Type: Functional

The final product can be affected by an accidental error caused by an operator. The error can be caused by the use of the wrong material or even to an error on the loom that the operator cannot avoid due to his/her lack of attention, fatigue, or even inexperience.

Misuse-Case 1b:
Misuse-Case Type: Functional/Security

A malicious person who may have access to the looms can intentionally damage the loom, for example causing technical problems; or can produce more pieces than the ones in the service order, causing economic damages to the company or selling counterfeit product.
8.3 IDEPA Misuse-Case – Detailed Review

Time: (Type duration in months)
Location: IDEPA Production Facility
Scope: Digitalization of a textile production line

8.3.1 Misuse-Case 1a

Assumptions:

For the misuse case scenario, we assume that the operator performs all actions on the loom, including restarting the loom after a stop, without any external intervention. We are also assuming that all the environmental sensors are working, and they are sending actual data to the data lake.

Attacker:

The misuse case attacker does not have any aim to cause damage, but due to his/her behaviour the damage occurs.

The attacker’s skill level:
The observed attacker in this misuse case is a typical operator of the company, who performs the assigned tasks. He/She may have a lot of experience performing his/her work but due to an external factor, as for example fatigue or stress, accidentally makes a mistake that causes damage to the loom and/or the final product. The same can happen with an operator who has less experience and therefore also causes a similar error.

Misuse-Case Staging:

The Misuse case has three stages:
1. Start the service order.
2. The loom raises an error.
3. The operator does not pay attention on the error and the service order proceeds.

1) Start the service order

- The operator receives the service order
- The operator selects the raw material needed to that service.
- The operator configures the loom and starts the service.
2) The loom raises an error

The loom raises an error and stops its operation.

Possible errors could be:

- **Problem with raw material**
  - The operator chooses the wrong raw material and the loom raises an error due to its specifications.
  - The raw material is the correct one, but because of some imperfection the loom stopped, and an intervention needs to be done (for example the line breaks).
- **Problem with the loom**
  - The loom has a technical problem and stops because it needs some intervention. For example, the temperature is so high that the loom stops as a security measure.

3) The operator does not pay attention on the error and the service order proceeds

- Due to external factors (fatigue, stress, etc.), the operator does not pay attention to the error and makes the loom proceed with the service order without ensuring that all measures that must be taken are actually performed.
- The operator’s inexperience in dealing with the loom problems, for example understanding the differences between the raw material, makes the loom proceed with the service order without ensuring that all steps are taken to solve the problem.

Countermeasures and mitigations

In this section possible mitigations are briefly listed.

*Mitigation 1:* Evaluate the fatigue, attention and stress of the operator, by continually monitoring the behaviour of his/her interaction with the machine.

*Mitigation 2:* Ensure the operator maintains the attention during the journey.

*Mitigation 3:* Support the training of new operators.
Mitigation Gaps

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always has to be expected that new or unknown problems may occur. In these cases, capabilities are needed to detect the abnormal behaviour of a loom. The abnormal behaviour capabilities need to be developed to monitor the behaviour of the operator and relate it with loom sensing. The development of these capabilities will be addressed as part of Task 3.3 “Human Behavior Modelling” and Task 5.3 “H/M-Behaviour Watch”.

A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a simulation/model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”, Task 4.2 “Manufacturing data-lake exploitation” and Task 4.3 “Human/Machine optimization”.

<table>
<thead>
<tr>
<th>CYberFactory#1: Key Capabilities</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CAP30</strong> Factory SoS Modelling</td>
</tr>
<tr>
<td>CAP31 CPS Modelling &amp; Digital Twins</td>
</tr>
<tr>
<td>CAP32 Ecosystem Modelling</td>
</tr>
<tr>
<td>CAP33 Human behavior Modelling</td>
</tr>
<tr>
<td>CAP34 Factory SoS Modelling</td>
</tr>
<tr>
<td><strong>CAP40</strong> FoF Optimization</td>
</tr>
<tr>
<td>CAP41 Real Time sensing &amp; tracking</td>
</tr>
<tr>
<td>CAP42 Manufacturing data lake exploitation</td>
</tr>
<tr>
<td>CAP43 Human / Machine optimization</td>
</tr>
<tr>
<td>CAP44 Distributed Manufacturing</td>
</tr>
<tr>
<td><strong>CAP50</strong> FoF Resilience</td>
</tr>
<tr>
<td>CAP51 Human / Machine access &amp; trust mgmt</td>
</tr>
<tr>
<td>CAP52 Adversarial / Robust learning ability</td>
</tr>
<tr>
<td>CAP53 Human / Machine behavior watch</td>
</tr>
<tr>
<td>CAP54 Cyber-resilience mechanisms</td>
</tr>
</tbody>
</table>

Behavior

- Real-time (or quasi-real-time) monitoring of the status of devices and equipment
- Not available
- Available
- Considering human learning and interaction Monthly.
- Using ML Service & Predictive System.
- KPI evaluated Hourly.

Identification of key assets
### 8.3.2 Misuse-Case 1b

#### Assumptions:

For this misuse case we assume that the operator has total control of the loom. Thus, it can insert information in the loom that does not coincide with the information that is in the service order. The operator does not need to insert in the loom the service order.

We are also assuming that all the environmental sensors are working, and they are sending actual data to the data lake.

#### Attacker:

The misuse case attacker wants to achieve the following goals:
- Create bad reputation of the company
- Competitive advantage
- Sell counterfeit product

The attacker’s skill level:
Should have the social capability/network to enter the production facility (if not an operator). It needs also to know how to work with the loom.

#### Misuse-Case Staging:

The Misuse case has three stages:

---

53 Data, Hardware, Software, Operational System, Information System, Testing Platform  
54 Select one or several: development, testing, validation, training, demonstration  
55 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)  
56 For more information see Deliverable T2.2. ‘Use cases – Portugal Use Cases’
4. Enter the looms facility
5. Insert wrong values in the loom
6. Cause damage in the loom or execute more pieces than the ones expected.

1) Enter the facility

- An external person gets access to the looms facility using social engineering.
- A malicious operator starts the work as expected.

2) Insert wrong values in the loom

The attacker (external person or malicious operator) insert values in the loom different from the service order in order to cause damage to the loom or to produce more pieces to sell in the black market.

Possible manipulation could be:
- **Produce some more pieces**
  - The aim of the attacker is producing extra pieces to sell in the black market, causing economic and reputation damage to the company.
- **Produce a really huge number of pieces**
  - The aim of the attacker is producing a huge number of pieces to cause damages in the loom and also cause economic damages to the company
- **Causing errors in the loom during the production**
  - The aim of the attacker is cause to errors in the loom in order to cause damages to the company (wrong raw material).

Countermeasures and mitigations

In this section possible mitigations are briefly listed.

Mitigation 1: Trustable people accompany outsiders while entering production sites. The outsiders are only allowed in permitted areas, such as meeting rooms.

Mitigation 2: Evaluate the attention of the operator by continuously monitoring the behaviour of his/her interaction with the machine, namely evaluating his/her actions when an error message occurs.
Mitigation Gaps

Even though the mitigations mentioned before lead to a more resilient system and by this make it harder to perform the Misuse-Case it always must be expected that new or unknown vulnerabilities it is possible to perform the Misuse-Case. In these cases, capabilities are needed to detect the abnormal behaviour of the loom. The development of these capabilities will be addressed as part of Task 3.3 “Human Behavior Modelling” and Task 5.3 “H/M-Behaviour Watch”. A possibility to detect abnormal behaviour based on the monitored behaviour might be a comparison of the monitored behaviour to a simulation/model of the expected or normal behaviour. This makes it necessary to develop capabilities to model Cyber-Physical Systems and their behaviour. The development of these capabilities will be addressed as part of Task 3.1 “CPS-Modelling and Simulation”, Task 4.2 “Manufacturing data-lake exploitation” and Task 4.3 “Human/Machine optimization”.

### Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>Description of the KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern discovery bet. humidity, temperature and Non Conformities</td>
<td>Not known</td>
<td>Known if significant</td>
<td>Using ML service. KPI evaluated Monthly.</td>
</tr>
<tr>
<td>Reduction of errors or efficiency failures by human behavior</td>
<td>Not available</td>
<td>Available</td>
<td>Using Affective computing considering human learning and interaction</td>
</tr>
<tr>
<td>Real-time (or quasi-real-time) monitoring of the status of devices and equipment</td>
<td>Not available</td>
<td>Available</td>
<td>Using ML Service &amp; Predictive System. KPI evaluated Hourly.</td>
</tr>
</tbody>
</table>

Identification of key assets
### Asset description

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type</th>
<th>Owner</th>
<th>Uses</th>
<th>Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>ML service</td>
<td>Software</td>
<td>ISEP</td>
<td>Testing, Validation, Training, Demonstration</td>
<td>Consortium Restricted</td>
</tr>
<tr>
<td>Predictive System (Affective Computing considering human learning and interaction)</td>
<td>Software</td>
<td>ISEP</td>
<td>Testing, Validation, Training, Demonstration</td>
<td>Consortium Restricted</td>
</tr>
<tr>
<td>Cyber Awareness Module</td>
<td>Software</td>
<td>ISEP</td>
<td>Testing, Validation, Training, Demonstration</td>
<td>Consortium Restricted</td>
</tr>
</tbody>
</table>

### 1.4 Misuse-Cases on IDEPA use-case

#### 8.3.3 IDEPA Use-Case Overview

In the project, ...

Components, ...

#### 8.3.4 IDEPA Misuse-Case Overview

This chapter describes the misuse case on a high level. In the following chapters/sections the detailed implementation is described.

The analysis focuses on risks that are linked to Access Authorizations. The source of the risks must derive from the use case itself.

**Misuse-Case 1: Unauthorized access to system or system areas**

---

57 Data, Hardware, Software, Operational System, Information System, Testing Platform  
58 Select one or several: development, testing, validation, training, demonstration  
59 Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)
Any access to the system that is not intended may lead to damages or interruptions on the production line.

**Misuse-Case 1a: Wrong user access**  
**Misuse-Case Type:** *Technological / Security*

Access to the ERP/MIS is done via browser, and the same device, usually in shop floor, is used by several different users; as the browser can automatically save passwords, it may hint a different login, which may have access to sensitive areas. This problem is magnified by the fact that there isn't an effective internal segregation of duties policy in place (the system roles do not match the organizational structure). Additionally, there are several users using the same ERP account, as there is no internal enforcement of a unique identification of users in the productive processes.

**Misuse-Case 1b: Accumulated permissions**  
**Misuse-Case Type:** *Technological / Security*

When users assume new responsibilities within the company, it is quite common to keep the old access profiles, potentially ending up with a powerful set of access rights that may enable them to cause disruption on the production line.

**Misuse-Case 2: ‘ISEP’ Misuse case**

8.3.5 IDEPA Misuse-Case – Detailed Review  
**Time:** (Type duration in months)  
**Location:** IDEPA – S. João da Madeira - Portugal  
**Scope:**

8.3.6 Misuse-Case 1 – Wrong user access (Technical/Security)  
**Assumptions:**

This use case relies on the fact that browsers usually offer to save login/passwords data and, later hints the user to use them. This may be a source of ill-intended logins, specially when the devices are used by more than one user without OS-Level authentication, as often is the case in the shop floor. A user with a powerful access profile logs in one device used to control a production machine, and inadvertently permits the browser to store the credentials; afterwards, an ill-intended machine operator logs in using these credentials and sabotages the production, or a curious user tries options that he usually doesn’t have access to and causes havoc on the system.

**Attacker:**

The misuse case attacker wants to achieve the following goals:  
- Disrupt production environment -The attacker is a disgruntled employee.
Experiment with options he usually doesn’t have access to – Curious user.

Misuse-Case Staging:

The Misuse case has three stages:

4. ‘Powerful’ user logs in a device used by multiple users, and allows the browser to save credentials.
5. Another user with less access rights, logs in the same device and accepts the hint from the browser to use the previous credentials.
6. Depending on the user social profile, either he uses the new access rights to sabotage production, or the user starts exploring the new options and creates havoc on the system.

4) ‘Powerful’ User logs in

Stage 1:
- A user with a powerful access profile logs in to the ERP/MIS on a shared computer;
- The browser automatically suggests to save the password;
- The user, inadvertently, clicks on the OK button.
- After having done what he was up to, the user logs off.

5) Risk ID# SCADA 0009 (Unintended access by multiple users in same device due to Browser saving login password)

Stage 2:
Another user logs in to the ERP/MIS on that same computer, and accepts the suggested ‘powerful’ credentials.

Possible manipulation could be:
- Disgruntled employee
  For example: erases production orders, manipulates material stocks, erases proposals, erases orders, manipulates prices/quantities.
- ‘Curious’ user
  May do the same actions as the disgruntled employee, but inadvertently, as he is just trying new option available.

Countermeasures and mitigations

In this section, possible mitigations are briefly listed.
Mitigation 1: Implement a Domain Group Policy disabling credentials saving on the browser. It should cover all browsers installed, and the user should not be allowed to install any other (or any application, in fact!).

Mitigation 2: Either there is a SSO (Single Sign On) system implemented or the user should not log in ERP/MIS without first doing log in to the system, with his own password.

Mitigation 3: Define a company-wide Segregation of Duties policy to effectively map ERP user permissions to their responsibilities on the Organization structure.

Mitigation 4: Management should enforce unique user authentication in every productive process.

Mitigation Gaps

Even though the mitigations mentioned before lead to a more resilient system, make it harder to perform the Misuse-Case it always has to be expected that other new or unknown vulnerabilities may arise. The implementation of real time user activity tracking applications is necessary even if the proposed mitigations are put in place, as malicious activity can always be performed (CAP41 and CAP53). In addition to this, there is the need of an effective modelling of organizational responsibilities and roles (CAP32), that could translate into more effective and secure shop floor operation and user access (CAP51).

Key Performance Indicators (KPIs) and Targets

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description of the KPI</td>
<td>Value without new</td>
<td>Value after introduction of</td>
<td>How to measure, how often to</td>
</tr>
</tbody>
</table>
### KPIs

<table>
<thead>
<tr>
<th>KPI</th>
<th>Historical Value</th>
<th>Target Value</th>
<th>Measurement</th>
</tr>
</thead>
<tbody>
<tr>
<td>countermeasures</td>
<td></td>
<td>new countermeasures</td>
<td>measure (yearly, monthly, etc.)</td>
</tr>
<tr>
<td>Unique user identifications</td>
<td>0%</td>
<td>100%</td>
<td>Authentication Logs; monthly</td>
</tr>
<tr>
<td>User permission matching with organizational structure</td>
<td>70%</td>
<td>90%</td>
<td>Matching degree measurement (by comparison); yearly</td>
</tr>
</tbody>
</table>

### Identification of key assets

<table>
<thead>
<tr>
<th>Asset description</th>
<th>Type(^{60})</th>
<th>Owner</th>
<th>Uses(^{61})</th>
<th>Access(^{62})</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sistrade ERP</td>
<td>Software</td>
<td>Sistrade</td>
<td>development, testing, validation, demonstration</td>
<td>CR</td>
</tr>
<tr>
<td>Sistrade SmartUX</td>
<td>Software</td>
<td>Sistrade</td>
<td>development, testing, validation, demonstration</td>
<td>CR</td>
</tr>
</tbody>
</table>

---

\(^{1}\) For more information see Deliverable T2.2. 'Use cases – Portugal Use Cases'

\(^{60}\) Data, Hardware, Software, Operational System, Information System, Testing Platform

\(^{61}\) Select one or several: development, testing, validation, training, demonstration

\(^{62}\) Open (O), Consortium Restricted (CR), Subject to Specific Agreement (SSA)