CyberFactory#1
Deliverable D2.1 – Business Models
## Change control

<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>V0.1</td>
<td>04/02/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Preliminary Version</td>
</tr>
<tr>
<td>V0.2</td>
<td>14/03/2019</td>
<td>Jari Partanen (Bittium)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>V0.3</td>
<td>19/03/2019</td>
<td>Regina M Correia (Sistrade)</td>
<td></td>
<td>Inclusion of the “Promotion” point in the “New Business Model Chapter”</td>
</tr>
<tr>
<td>V0.4</td>
<td>24/03/2019</td>
<td>Jari Partanen (Bittium)</td>
<td></td>
<td>Added Business Canvas to document</td>
</tr>
<tr>
<td>V0.5</td>
<td>26/03/2019</td>
<td>Jari Partanen (Bittium)</td>
<td></td>
<td>Additions of M2M context to complement IIoT</td>
</tr>
<tr>
<td>V0.6</td>
<td>4/4/2019</td>
<td>Jari Partanen (Bittium)</td>
<td></td>
<td>Revised version</td>
</tr>
<tr>
<td>V0.7</td>
<td>10/4/2019</td>
<td>Jari Partanen (Bittium)</td>
<td></td>
<td>Small adjustments</td>
</tr>
<tr>
<td>V0.8</td>
<td>06/05/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Added the Users Business Models Chapter</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Added the New Business Models for FOF Value Chain Chapter</td>
</tr>
<tr>
<td>V0.9</td>
<td>04/06/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Included Bittium new Contribution</td>
</tr>
<tr>
<td>V1.0</td>
<td>03/07/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Included Vestel contribution General Revision</td>
</tr>
<tr>
<td>V1.1</td>
<td>15/07/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Included IDEPA contribution General Revision</td>
</tr>
<tr>
<td>V1.2</td>
<td>06/08/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Included Vestel revised contribution</td>
</tr>
<tr>
<td>V1.7</td>
<td>06/09/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>General Formatting, Added Several important pieces</td>
</tr>
<tr>
<td>V1.8</td>
<td>09/09/2019</td>
<td>João Mourinho (Sistrade)</td>
<td></td>
<td>Added ADSS Contributions</td>
</tr>
<tr>
<td>V1.9</td>
<td>13/09/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Formatting revision.</td>
</tr>
<tr>
<td>V1.10</td>
<td>23/09/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Inserted revised contribution from Idepa and from Jari Partanen.</td>
</tr>
<tr>
<td>V1.11</td>
<td>26/09/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Minor revisions</td>
</tr>
<tr>
<td>V1.12</td>
<td>01/10/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Minor revisions, and comments from Markku Mikkola and İrem Hilavin.</td>
</tr>
<tr>
<td>V1.13</td>
<td>08/10/2019</td>
<td>Américo Nascimento (Sistrade)</td>
<td></td>
<td>Incorporating minor revisions, and comments from Matthias Glawe.</td>
</tr>
</tbody>
</table>
Table of Contents

ACRONYMS ......................................................................................................................... 7
1. EXECUTIVE SUMMARY ................................................................................................. 9
2. SCOPE ............................................................................................................................ 11
3. AEROSPACE .................................................................................................................. 12
   3.1. SWOT ANALYSIS ................................................................................................... 12
   3.2. COMPETITION ANALYSIS ................................................................................. 13
   3.3. NEW BUSINESS MODEL ...................................................................................... 18
       3.3.1. Value Proposition ......................................................................................... 18
       3.3.2. Customer Segments ..................................................................................... 18
       3.3.3. Key Partners ................................................................................................. 19
       3.3.4. Key Competitors ......................................................................................... 20
       3.3.5. Key Activities ............................................................................................... 20
       3.3.6. Key Resources .............................................................................................. 20
       3.3.7. Customer Relationships .............................................................................. 21
       3.3.8. Channels ....................................................................................................... 21
       3.3.9. Cost Structure .............................................................................................. 21
       3.3.10. Revenue Streams ....................................................................................... 21
       3.3.11. Promotion .................................................................................................... 22
4. TEXTILE ........................................................................................................................... 23
   4.1. SWOT ANALYSIS ................................................................................................... 23
       Strengths .................................................................................................................. 23
       Weaknesses ............................................................................................................. 23
       Opportunities ......................................................................................................... 23
       Threats .................................................................................................................... 24
   4.2. COMPETITION ANALYSIS ................................................................................. 24
   4.3. NEW BUSINESS MODEL ...................................................................................... 26
       4.3.1. Value Proposition ......................................................................................... 26
       4.3.2. Customer Segments ..................................................................................... 27
       4.3.3. Key Partners ................................................................................................. 28
       4.3.4. Key Activities ............................................................................................... 28
       4.3.5. Key Resources .............................................................................................. 28
       4.3.6. Customer Relationships .............................................................................. 29
       4.3.7. Channels ....................................................................................................... 29
       4.3.8. Cost Structure .............................................................................................. 29
       4.3.9. Revenue Streams ....................................................................................... 29
       4.3.10. Promotion .................................................................................................... 30
5. ELECTRONICS .................................................................................................................. 31
   5.1. SWOT ANALYSIS ................................................................................................... 31
       Strengths .................................................................................................................. 31
       Weaknesses ............................................................................................................. 31
       Opportunities ......................................................................................................... 31

Page 3 of 98 Based on the ITEA 3 PO Template v4.0 (August 2017)
5.2. **COMPETITION ANALYSIS** ........................................................................................................... 32
5.3. **NEW BUSINESS MODEL** ........................................................................................................... 34
  5.3.1. **Value Proposition** .................................................................................................................... 34
  6.3.2. **Customer Segments** .............................................................................................................. 35
  6.3.3. **Key Partners** .......................................................................................................................... 35
  6.3.4. **Key Competitors** ................................................................................................................... 35
  6.3.5. **Key Activities** ........................................................................................................................ 35
  6.3.6. **Key Resources** ....................................................................................................................... 35
  6.3.7. **Customer Relationships** ....................................................................................................... 36
  6.3.8. **Channels** .................................................................................................................................. 36
  6.3.9. **Cost Structure** ........................................................................................................................ 36
  6.3.10. **Revenue Streams** ................................................................................................................ 36
  6.3.11. **Promotion** ............................................................................................................................ 36

6. **MACHINE INDUSTRY** .................................................................................................................. 37
  6.1. **SWOT ANALYSIS** .................................................................................................................... 38
  6.2. **COMPETITION ANALYSIS** ...................................................................................................... 38
  6.3. **NEW BUSINESS MODEL** ......................................................................................................... 40
    6.3.1. **Value Proposition** ................................................................................................................ 40
    6.3.2. **Customer Segments** ............................................................................................................ 40
    6.3.3. **Key Partners** ....................................................................................................................... 40
    6.3.4. **Key Competitors** ................................................................................................................ 41
    6.3.5. **Key Activities** ..................................................................................................................... 41
    6.3.6. **Key Resources** .................................................................................................................... 41
    6.3.7. **Customer Relationships** ..................................................................................................... 42
    6.3.8. **Channels** ................................................................................................................................ 42
    6.3.9. **Cost Structure** ..................................................................................................................... 42
    6.3.10. **Revenue Streams** ............................................................................................................. 42
    6.3.11. **Promotion** .......................................................................................................................... 42

7. **ROBOTICS** ....................................................................................................................................... 43
  7.1. **SWOT ANALYSIS** .................................................................................................................... 44
    **Strengths** ........................................................................................................................................ 45
    **Weaknesses** .................................................................................................................................... 45
    **Opportunities** ............................................................................................................................... 45
    **Threats** .......................................................................................................................................... 46
  7.2. **COMPETITION ANALYSIS** ....................................................................................................... 47
  7.3. **NEW BUSINESS MODEL** ......................................................................................................... 48
    7.3.1. **Value Proposition** ................................................................................................................ 49
    7.3.2. **Customer Segments** ............................................................................................................ 49
    7.3.3. **Key Partners** ....................................................................................................................... 49
    7.3.4. **Key Competitors** ................................................................................................................ 50
    7.3.5. **Key Activities** ..................................................................................................................... 50
    7.3.6. **Key Resources** .................................................................................................................... 50
    7.3.7. **Customer Relationships** ..................................................................................................... 50
    7.3.8. **Channels** ................................................................................................................................ 50
    7.3.9. **Cost Structure** ..................................................................................................................... 51
8. **IIOT & M2M** .................................................................................................................. 52

8.1. **SWOT ANALYSIS** ........................................................................................................ 52  
   *Strengths* ......................................................................................................................... 52  
   *Weaknesses* ...................................................................................................................... 52  
   *Opportunities* .................................................................................................................. 52  
   *Threats* ............................................................................................................................ 52  

8.2. **COMPETITION ANALYSIS** .......................................................................................... 53  

8.3. **NEW BUSINESS MODEL** ............................................................................................. 59  

8.3.1. **Value Proposition** ..................................................................................................... 59  
8.3.2. **Customer Segments** .................................................................................................. 61  
8.3.3. **Key Partners** ............................................................................................................. 61  
8.3.4. **Key Competitors** ...................................................................................................... 62  
8.3.5. **Key Activities** ......................................................................................................... 62  
8.3.6. **Key Resources** ....................................................................................................... 63  
8.3.7. **Customers** ............................................................................................................... 63  
8.3.8. **Customer Relationships** .......................................................................................... 63  
8.3.9. **Channels** ................................................................................................................ 64  
8.3.10. **Cost Structure** ....................................................................................................... 64  
8.3.11. **Revenue Streams** .................................................................................................. 64  
8.3.12. **Promotion** .............................................................................................................. 64  

9. **ERP & SCADA** ............................................................................................................... 65  

9.1. **SWOT ANALYSIS** ......................................................................................................... 65  
   *Strengths* .......................................................................................................................... 65  
   *Weaknesses* ...................................................................................................................... 65  
   *Opportunities* .................................................................................................................. 66  
   *Threats* ............................................................................................................................ 66  

9.2. **COMPETITION ANALYSIS** .......................................................................................... 67  

9.3. **NEW BUSINESS MODEL** ............................................................................................. 70  

9.3.1. **Value Proposition** ..................................................................................................... 70  
9.3.2. **Customer Segments** .................................................................................................. 71  
9.3.3. **Key Partners** ............................................................................................................. 71  
9.3.4. **Key Competitors** ...................................................................................................... 71  
9.3.5. **Key Activities** ......................................................................................................... 71  
9.3.6. **Key Resources** ....................................................................................................... 71  
9.3.7. **Customer Relationships** .......................................................................................... 72  
9.3.8. **Channels** ................................................................................................................ 72  
9.3.9. **Cost Structure** ....................................................................................................... 72  
9.3.10. **Revenue Streams** .................................................................................................. 72  
9.3.11. **Promotion** .............................................................................................................. 72  

10. **SECURITY AND SAFETY** ............................................................................................ 73  

10.1. **SWOT – S4-SECURITY & SAFETY** ............................................................................. 73  
   *Strengths* .......................................................................................................................... 73
Weaknesses ........................................................................................................... 73
Opportunities ......................................................................................................... 73
Threats .................................................................................................................... 73

10.2. CAP51-H/M ACCESS & TRUST ................................................................. 74
Strengths .................................................................................................................. 74
Weaknesses .............................................................................................................. 74
Opportunities .......................................................................................................... 74
Threats ..................................................................................................................... 75
10.2.1. Competition analysis .................................................................................. 75
10.2.2. New Business Model .................................................................................. 77
10.2.2.1. Value Proposition .................................................................................... 77
10.2.2.2. Customer Segments ................................................................................ 77
10.2.2.3. Key Players ............................................................................................. 77
10.2.2.4. Key Resources ....................................................................................... 77
10.2.2.5. Customer Relationships ............................................................................ 78
10.2.2.6. Channels ................................................................................................ 78
10.2.2.7. Cost Structure ........................................................................................ 78
10.2.2.8. Revenue Streams ................................................................................... 78

10.3. CAP52-ROBUST ML ...................................................................................... 80
Strengths .................................................................................................................. 80
Weaknesses .............................................................................................................. 80
Opportunities .......................................................................................................... 80
Threats ..................................................................................................................... 80
10.3.1. Competition Analysis ................................................................................ 81
10.3.2. New Business Model .................................................................................. 84

10.4. CAP53-H/M BEHAVIOR WATCH ............................................................ 86
Strengths .................................................................................................................. 86
Weaknesses .............................................................................................................. 86
Opportunities .......................................................................................................... 86
Threats ..................................................................................................................... 86
10.4.1. Competition Analysis ................................................................................ 87
10.4.2. Business Model Canvas ............................................................................... 89

10.5. CAP54-CYBER-RESILIENCE ................................................................. 91
Strengths .................................................................................................................. 91
Weaknesses .............................................................................................................. 92
Opportunities .......................................................................................................... 92
Threats ..................................................................................................................... 92
10.5.1. Competition Analysis ................................................................................ 92
10.5.2. New Business Model .................................................................................. 95

10.6. CONCLUSION .............................................................................................. 97

11. CONCLUSIONS ............................................................................................... 98
## Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGV</td>
<td>Autonomous Guided Vehicle</td>
</tr>
<tr>
<td>AI</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>AIV</td>
<td>Autonomous Intelligent Vehicle</td>
</tr>
<tr>
<td>AMR</td>
<td>Autonomous Mobile Robot</td>
</tr>
<tr>
<td>aPaas</td>
<td>Application Platform as a Service</td>
</tr>
<tr>
<td>API</td>
<td>Application Programming Interface</td>
</tr>
<tr>
<td>CMR</td>
<td>Collaborative Mobile Robot</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>EDI</td>
<td>Electronic Data Interchange</td>
</tr>
<tr>
<td>ERP</td>
<td>Enterprise Resource Planning</td>
</tr>
<tr>
<td>FoF</td>
<td>Factories of the Future</td>
</tr>
<tr>
<td>IIoT</td>
<td>The industrial internet of things (IIoT) refers to the extension and use of the internet of things (IoT) in industrial sectors and applications. With a strong focus on machine-to-machine (M2M) communication, big data, and machine learning, the IIoT enables industries and enterprises to have better efficiency and reliability in their operations. The IIoT encompasses industrial applications, including robotics, medical devices, and software-defined production processes.</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine-to-machine, or M2M, is a broad label that can be used to describe any technology that enables networked devices to exchange information and perform actions without the manual assistance of humans</td>
</tr>
<tr>
<td>MP</td>
<td>Mobile Platform</td>
</tr>
<tr>
<td>ODM</td>
<td>Original Design Manufacturer</td>
</tr>
<tr>
<td>PLM</td>
<td>Product Life-cycle Management</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory Control and Data Acquisition</td>
</tr>
<tr>
<td>SCM</td>
<td>Supply Chain Management</td>
</tr>
<tr>
<td>SoS</td>
<td>System-of-Systems</td>
</tr>
<tr>
<td>SRM</td>
<td>Supplier Relationship Management</td>
</tr>
<tr>
<td>------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>TRL</td>
<td>Technology Readiness Level</td>
</tr>
</tbody>
</table>
1. Executive Summary

CyberFactory#1 main goal is to conciliate optimization of the supply and manufacturing chain of FoF with the need for security, safety and resilience against cyber and cyber-physical threats. The project maps eight paradigmatic sectors and actors in the FoF value chain, divided into two main value chain stages: users (i.e. Industrial sectors which represent the end users of the new technologies and approaches developed in CyberFactory - Figure 1) and suppliers (industrial sectors which provide enabling technologies to be applied in the end user activities - Figure 2).

CyberFactory#1 project strives to capitalize the new opportunities that arise from technology, customer needs and new demands. New technologies such as Big Data, Digital Twin, Industrial IOT open up new value creation opportunities as they power new data-driven approaches that are essential to improve security and efficiency of the FoF. On the other hand, there is an increasing demand for product optimization and customization and managed security services. Therefore, it is crucial that new business models can be designed in order to improve, optimize and transform the value creation throughout the value chain, both at supplier and user sides. This is achieved through a data-centric approach, where data is the core and presents a set of opportunities that arise from data capture, processing and treatment.
The business models presented at this document result from a thorough analysis of the inner environment versus the external environment of each business model leader. Additionally, each Business Model Leader has also analysed its current positioning in comparison with its competitors. This process culminated in the development of a Business Model Canvas, which was the base for the work presented at this document.

Each of the business model presents an innovative value proposal, describing the value that the company promises to deliver to the potential customers. It also presents the customer segments to which that value proposal is directed to, the important partners directly or indirectly related with it, the most important activities that need to be executed to deliver the promised value and the key resources needed. The interaction with the potential customers is also explained, as well as the channels to reach them. An economic assessment of the costs and revenues is also presented. The business model finalizes with the description of the promotion actions.
2. **Scope**

The current document defines and describes eight business models from two main areas of value: end user industries (Aerospace, Automotive, Electronics and Machine Industry) and supply chain (Robotics, IIOT & M2M, ERP and SCADA and Security and Safety) addressed in the CyberFactory#1 project.

The business models were developed throughout the execution of the Task 2.1 “New Business Model Definition”. They propose new approaches to enhance the creation of value and make use of data driven architectures and infrastructure/platform/software-as-a-service concepts.

The following sections present the new Business Models for the FOF Value Chain 8 main areas.
3. Aerospace

Airbus Defense & Space is an aerospace company whose parent company is the Airbus Group, the world's largest aerospace group. Within the aerospace industry, Airbus covers all phases of product development (keeping within its scope the processes it considers core, and subcontracting those it does not). Airbus D&S designs, manufactures and delivers aerospace products, services and solutions to customers on a global scale.

3.1. SWOT Analysis

**Strengths**

<table>
<thead>
<tr>
<th>As a company:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Established brand name: Airbus is now a forty-year-old success.</td>
</tr>
<tr>
<td>- Leading manufacturer of commercial aircrafts.</td>
</tr>
<tr>
<td>- Focus on research and innovation. Successful track record of developing new products.</td>
</tr>
<tr>
<td>- Manufacturing and design facilities located globally.</td>
</tr>
<tr>
<td>- Reliable suppliers enabling the company to overcome any supply chain bottlenecks.</td>
</tr>
<tr>
<td>- Strong distribution network that can reach majority of its potential market.</td>
</tr>
<tr>
<td>- Producer of a large range of modern and efficient products.</td>
</tr>
<tr>
<td>- Large gross market share.</td>
</tr>
<tr>
<td>- Increase presence in satellite business and (in space, in general)</td>
</tr>
<tr>
<td>- New aircraft models with higher fuel efficiency.</td>
</tr>
<tr>
<td>- High level of customer satisfaction.</td>
</tr>
<tr>
<td>- Success at entrance in new markets (new revenue stream and diversify the economic cycle risk in operated markets)</td>
</tr>
<tr>
<td>- Integration of complimentary firms (mergers and acquisition), to streamline its operations and to build a reliable supply chain.</td>
</tr>
</tbody>
</table>

**Weaknesses**

<table>
<thead>
<tr>
<th>As a company:</th>
</tr>
</thead>
<tbody>
<tr>
<td>- High costs of production and operations.</td>
</tr>
<tr>
<td>- Needs of more new technologies investments.</td>
</tr>
<tr>
<td>- Loss of small market share in the niche categories due to the challenges present by new entrants in the segment.</td>
</tr>
<tr>
<td>- Limited success outside core business.</td>
</tr>
</tbody>
</table>

**Inside Cyberfactory#1 project:**

| - Until today, no integrated security concept exists for devices/apps communications in some user companies. |
| - In some cases, totally isolated networks within a company since a standardized communication process with an acceptable level of security have not been defined. |
| - There is no common agreement between the companies belonging to the consortium on the communication protocol(s) to implement them in a secure and reliable Industrial Network system. |

**Inside Cyberfactory#1 project:**

| - Multidisciplinary consortium (user, researchers and suppliers working together). |
| - CyberFactory#1 integrates security, safety and resilience against cyber and cyber-physical threats as strategical |
13

CyberFactory#1

Based on the ITEA 3 PO Template v4.0 (August 2017)

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>As a company:</strong></td>
<td><strong>As a company:</strong></td>
</tr>
<tr>
<td>• Increased demand for air travel (decreasing cost of transportation).</td>
<td>• Intense competition on the aerospace market.</td>
</tr>
<tr>
<td>• Improvement of the global economics: opportunity to capture new customers and increase the market share.</td>
<td>• Technological developments by competitors.</td>
</tr>
<tr>
<td>• Technological innovation applied to all company (design of products, manufacturing, sales…)</td>
<td>• Regulatory pressure (regulations on international trade keep changing and different laws in customer countries).</td>
</tr>
<tr>
<td>• A large backlog of orders.</td>
<td>• Exposure to the political, economic and social fluctuations of the customers (company operating in numerous and different countries).</td>
</tr>
<tr>
<td><strong>Inside Cyberfactory#1 project:</strong></td>
<td>• The rise in prices of fuel that increases in the input costs for the company.</td>
</tr>
<tr>
<td>• Create a solid work ecosystem that will be a reference in future challenges of Industry 4.0</td>
<td><strong>Inside Cyberfactory#1 project:</strong></td>
</tr>
<tr>
<td>• Open possibilities for new business models (e.g. focusing on energy efficiency, customer centered).</td>
<td>• Global coordination of the partners of the project.</td>
</tr>
<tr>
<td>• Obtaining own production data in real time, with the possibility of modifying parameters, which can be decisive for competitiveness in the aeronautical sector.</td>
<td>• The lack of resources (time or money) in some of the lines of the project, could condition the success of the following developments within the project.</td>
</tr>
<tr>
<td>• Communication with subcontractors and obtaining real-time data on the situation of lead-time and tack-time of their production.</td>
<td>• Consideration of additional costs associated to the forced replacement of key production tools, due to be not possible the implementation of sensory systems in them.</td>
</tr>
</tbody>
</table>

3.2. **Competition Analysis**

Airbus D&S stands out from its competitors by the high quality of its products and services, the high technology of its products and by using digitization as a competitive advantage that reduces production costs and drives our business model (being ahead of our immediate competitors, for example Boeing). This fact is relevant as the so-called fourth industrial revolution is transforming the global economy into an information-centric economy. Fortunately, we have been able to interpret these signals in time, which is reflected in the fact that already more than 50% of the company’s profits come from platforms such as communication platforms, data-driven digital services for Defense and cyber security applications (the other 50% is shared equally
between the military sector and the Defense sector), although the reality is that there is still a long way to go.

For this reason, we see CyberFactory#1 project as a fundamental growth opportunity for the company, as it encompasses the different market players (User, suppliers, developers), drastically facilitating our own developments.

In addition, it is a project that has use cases from different industries in which Airbus D&S could discover new business niches not identified so far.

Airbus currently produces a wide range of products in both the defense and space sectors, developing cutting-edge products in these fields, providing solutions that guarantee sovereignty in foreign affairs and defence matters. However, the core of our activity in recent years is shifting from the manufacture of products (such as tactical and strategic airlifters, multi-role aerial tankers, advanced combat aircraft, UAS, satellites, space infrastructures, space equipment or launchers) to the creation of communication platforms (security solutions, cyber security, actionable intelligence secure communications and secure land communications) and services.

This portfolio of products and services is largely due to the different distribution channels that Airbus has today, both within the company (Procurement, Programs and Sales Departments) and external media (news, events, corporate magazine, social networks website and media). In addition, the segmentation of the market according to the needs of our customers (continuous feedback), the diversification of our business or the commitment to innovation have been and continue to be cornerstones of our business model.

Finally, in order to make a quick diagnosis about Airbus Defense and Space, a SWOT analysis, regarding the competition, is added below:

<table>
<thead>
<tr>
<th>Profile</th>
<th>Airbus</th>
<th>LEONARDO</th>
<th>BOEING</th>
<th>LOCKHEED MARTIN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Aerospace Industry. Designing, manufacturing and delivering aerospace products, services and solutions to customers on a global scale.</td>
<td>Leonardo is one of the world’s top ten players in Aerospace, Defense and Security, a trusted long-term partner of choice for governments, institutions and private customers, delivering cutting-edge and dual-use technologies.</td>
<td>The world’s leading aerospace company. Provides leading solutions for the design, production, modification, service and support of aerospace products. Connect, protect, explore and inspire the world through aerospace innovation.</td>
<td>Aerospace Industry. American global aerospace, defense, security and advanced technologies company with worldwide interests. Solve complex challenges, advance scientific discovery and deliver innovative solutions to help their customers keep people safe.</td>
</tr>
<tr>
<td>Key Competitive Advantage</td>
<td>Innovation, with the 12% of 2018 revenues dedicated to R&amp;D.</td>
<td>Wide range of products and services for different customer groups. Operating in critical businesses supporting the mainline businesses. Innovation: $3 billion invested annually in R&amp;D.</td>
<td>- Hypersonic technology. F-35 major designer and manufacturer. - Oligopolistic Market with good relationships in defense.</td>
<td></td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Target Market</td>
<td>25% Military Aircraft. 20% Space Systems, Missiles, UAV. 55% Platforms (communication platforms, data-driven digital services for defense and cyber security applications).</td>
<td>32% Aeronautics. 32% Electronics, Defense and Security Systems. 36% Helicopters.</td>
<td>39% Aeronautics. 16% Missiles and Fire. 26% Control, Rotary and Mission Systems. 18% Space.</td>
<td></td>
</tr>
<tr>
<td>Market Share</td>
<td>30% Military Sector. 20% Space Sector.</td>
<td>20% Aerospace and Defense.</td>
<td>58% Fighter Aircraft. 22.5% Military Transport Aircraft. 8% Missiles.</td>
<td></td>
</tr>
</tbody>
</table>
| Marketing Strategy        | Segmentation (demographic, geographic and psychographic to cater to the customer of different nations). Competitive advantage (Innovation, Research and development). Diversifying businesses into interrelated products and services. | **Customer-focused**
- Providing customized solutions
- Involving customers from the start of the design state
- Offering reliability in the execution of contracts on time and on budget
- Reinforcing after-sales support | Segmentation (demographic and geographic to cater to the customers of different nations). Positioning strategy is used to highlight the differentiated benefits of the offering. Targeting strategy is used as a different set of offerings are meant for a different set of customers. |
<p>|                           | Different media to attract their customers and gain contracts. Traditional and digital media. But, they connect with their clients to promote its products. It needs to keep improving and proving its credibility and needs to advertise itself so that it gains a similar market share and builds the same image in a few other countries as well. | | |</p>
<table>
<thead>
<tr>
<th>Products &amp; Services</th>
<th>Defense: Tactical and strategic airlifters, multi-role aerial tankers, advanced combat aircraft, UAS, Services, Security solutions, Cyber security, Actionable Intelligence Secure Communications, Secure Land communications. <strong>Space:</strong> Satellites, Space infrastructures, Space equipment, Launchers, Services (test services, on-orbit-service, etc...)</th>
<th>Helicopters, Commercial, public services and defense applications) Aeronautics (Trainers, combat and tactical transport aircraft, multi-role and regional turboprop aircraft and UAS Electronics, Defense and Security Systems Aeronautics. Trainers, combat and tactical transport aircraft, multi-role and regional turboprop aircraft. UAS (Unmanned Aerial Systems). <strong>Space</strong> Satellite services for communications and geo-information. Integrated Satellite Systems, launch services and in orbit satellite control.</th>
<th>Defense: fighter jets, rotorcraft, embedded product support, cybersecurity products, surveillance suites, advanced weapons, missile defense and commercial aircraft derivatives. <strong>Space:</strong> satellites, global positioning system, resilient aerospace connectivity, international space station, launchers, space and communication systems for military uses, commercial spacecraft.</th>
<th>Aeronautics: includes tactical aircraft, airlift, and aeronautical research and development lines of business. <strong>Missiles and Fire Control:</strong> Terminal High Altitude Area Defense System and PAC-3 Missiles as some of its high-profile programs. <strong>Rotary and Mission Systems:</strong> Sikorsky military and commercial helicopters, naval systems, platform integration, and simulation and training lines of business. <strong>Space:</strong> space launch, commercial satellites, government satellites, and strategic missiles lines of business.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pricing</td>
<td>Cost reduction through flexible production based on Industry 4.0</td>
<td>Value-added pricing strategy Premium quality + premium prices Striving to achieve economies of scale from its procurement process to designing and manufacturing.</td>
<td>Lockheed Martin follows a competitive pricing strategy. covers all costs and then set a price according to what the competitors are charging, and their margin profit.</td>
<td>---</td>
</tr>
</tbody>
</table>
| Strengths | - Airbus D&S is always focused on innovation in technology and design.  
- Strong support from its parent company Airbus (Revenues 64 billion €)  
- Diversified portfolio. | - Website  
- Media | 1. Strong backing by the US government as 85% revenue comes from US government contacts  
2. Wide range of services across four sectors – Aerospace and Defense, Information Technology, Space and emerging technologies  
3. Operates in an oligopolistic environment  
4. Customer base is small but stable  
5. Its specialized product portfolio  
6. Over 100,000+ people are employed in the organization  
7. Has been recognized by several awards |
| Weaknesses | Possible lack of foresight in the company’s internal structure and lack of flexibility in production, given the abrupt outcome of the Brexit process. | - Labour issues, higher dependency on US government contracts, suppliers bargaining power | 1. High dependence on US government for revenue and projects |
| Opportunities | Achieve the implementation of Industry 4.0. | - The Aerospace and defense market is increasing globally which is an opportunity to boost up revenue in the future.  
- Association with large companies for new projects | 1. Rising defense needs for countries from terrorists’ threats  
2. Modernization of defense in all countries will continuously lead to increase in demand in future |
### Threats

| Threats                                                                 | - Strong new competitors in the Space Market. (SpaceX, etc.) | - Intense competition in all categories Fixed-priced contracts (about 72% of Boeing revenue is from BDS contracts with fixed prices) | 1. Changes in global trade barriers  
2. Defense budget cuts will affect the company gravely  
3. Competition from other manufacturers  
4. Government regulating technology and security |
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Social and political environment drastically influences in our business.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### 3.3. New Business Model

#### 3.3.1. Value Proposition

Cyberfactory#1 is a project that aims to bring the company towards new business model, based on the interconnection of the manufacturing machines and lines with the business applications & systems, and also introducing the security dimensions (cybersecurity). The results and advances of Cyberfactory#1 will generate a new business model that not only improves our value proposition, but also:

- Keep our brand as a symbol of leadership and high quality in the aerospace sector.
- Reinforce quality, safety and security as non-negotiable and defining elements of our business model. (Critical in the actual aeronautical environment).
- Meet present and future defense and space requirements (Long and medium-range military transport, Satellites and Space rockets).
- Pioneering engineering (Innovative designs, reliable products with the latest technology)
- Develop new and more flexible manufacturing technologies that allow us a greater customization of the product.

To amplify and reinforce it:

- High-tech manufacturing processes, introducing more automation level across digital and IoT connectivity new technologies.
- Adaptive and smart manufacturing equipment and systems thanks to new technologies of data analytics.
- Data Management for increased production performance, across an automated process monitoring more effective.
- Networked factories linking dynamically supply chain to local production, with the introduction of technologies for distributed manufacturing developed into Cyberfactory#1 project.
- Human-centered manufacturing due to all the introduced technologies will be focused on helping/support the workers.
- Digitalization as a main way to increase our competitiveness.

#### 3.3.2. Customer Segments

On one hand, market segments that we have traditionally attended were:

- Military sector (30% of the market)
- Commercial sector (20% of the market)
- Airlines
- Defense Agencies and Governments
- Aerospace Agencies
- NASA
- European Space Agency
- Communications
- Industry 4.0 customers

Airbus has a worldwide presence, with customers in countries from different continents:
- Europe: France, Germany, Spain, United Kingdom, Turkey…
- America: United States, Canada, Mexico, Brazil…
- Africa: Nigeria, Morocco, Tunisia…
- Asia: Japan, China, South Korea, Singapore, India.

Figure 3 illustrates the global market presence of Airbus.

3.3.3. Key Partners

As key partners of the new business model, we have identified the following actors:
Governments within the European Union (Spain, Germany, France…)
Investors and shareholders
Universities & Research Centers
Suppliers (GKN, Safran, Alestis, Microsoft…)
Subcontractors (Ayesa, Altran, Alten…)
R&T/ R&D departments.
Other aero/space manufacturers (partners)
CyberFactory#1 project members

3.3.4. Key Competitors
As key competitors, we have identified aeronautical and aerospace companies such as:
- Boeing
- BAE
- Alenia
- Bombardier
- Embraer
- PJSC Sukhoi
- COMAC
- XAC
- Lockheed Martin

3.3.5. Key Activities
Among our key activities we have identified both traditional ones in our industry and others that can greatly benefit from the results of the Cyberfactory#1 project.
- R&T and R&D, brought innovations and new developments for the improvement of products, new products, improvement of manufacturing and sales process, and even more efficient relations with customers by using new technologies.
- Design of products, making possible new ways of work in design of products, more efficient, by means of the connectivity in real time of designers and with the use of new digital environments for developments in these activities. Also, opening new ways of feedback from customers, more effective and efficient than current ones.
- Manufacturing, across the modernization of the manufacturing lines by introducing new technologies of IoT, data analytics, artificial intelligent (based on Industry 4.0), taking the manufacturing process towards high automation and better productive efficiency.
- Products and Services to the customer, carrying on products highly and more easily customized, and a customer services more efficient and closer to the customer by the use of new connectivity technologies.
- Supply Chain management, across the modernization of the supply chain, introduction of connectivity in real time for tracking of process and products between factories.

3.3.6. Key Resources
The main asset of our company is our people (40,000 employees). Apart from that, we have important resources that are worth highlighting, such as:
• Staff and facilities (highly qualified and specialized)
• Intellectual property
• Support from European Governments
• Multicultural team, 35 locations all over the world.

3.3.7. Customer Relationships
About our relationship with the customer, we base our performance in the following bases:
• Long-term contracts
• Customization
• Trust
• Safety
• Quality
• Innovation
• Disruption
• Best in class services

3.3.8. Channels
There are different channels which we use to reach our customers, such as:
• Procurement, Programs and Sales Departments
• News
• Events
• Corporative Magazine
• Social Networks
• Website
• Media

3.3.9. Cost Structure
We identify the following cost structure elements:
• R&D/ R&T costs.
• Parts and components
• Manufacturing & Assembly lines
• Supply chain

3.3.10. Revenue Streams
Our main revenue streams are:
• Long term contracts (sales of products and contracts as-a-service, data-driven…)
• Sale of products
• Merges and acquisitions
• Aircraft Services
• Platforms (Skywise)
3.3.11. Promotion

This new business model will be promoted inside Airbus D&S Company, as an internal promotion of the new technologies developed into Cyberfactory#1 project across the presented use cases. The normal activities for that are presentations and demonstrations to the diverse departments involved into the design, manufacturing, sales and services of our products.

Also, this new business model will be promoted externally to Airbus D&S Company: through similar promoting ways, to Airbus Company (Civil Aircrafts) & Helicopters; but also, in the context of CyberFactory#1 project and ITEA consortium (partners), through the project website and promotional events. Finally, it will be very important the promotional missions to current and potential customers and social media also.
4. Textile

The textile industry – one of the key beneficiaries of the first industrial revolution – (considering the onset of the Industry 4.0 as the 4th industrial revolution), was at that time the symbol of European technological leadership and industrial power. Post World War 2 economic globalization has driven the delocalization of the textile industry to developing countries with low labour costs. Nevertheless, the textile industry still plays an important role in the European manufacturing industry, employing 1.7 million people and generating a turnover of 166 billion\(^1\). In order to improve its competitiveness, it needs to move toward higher value-added products and leverage the most recent advances in manufacturing technology, make use of the value of data and secure its intellectual property and knowledge from ill intended actors.

IDEPA is, in the CyberFactory#1 consortium, the paradigmatic example of the European textile industry, being a half a century company with decades-long experience, facing the same challenges than its European pairs and moving gradually to the Industry 4.0 paradigm.

4.1. SWOT Analysis

Strengths

IDEPA has a strong image and recognition in the market, benefiting from their quality recognition by its business clients. It has also moved towards the higher value-added products through diversification of its product mix (ex: automobile textiles) and by offering customized production. IDEPA can customize due to having a highly personalized service, a mix of production equipment with different capabilities (including legacy equipment).

Being a half a century old company brings a whole know-how and experience that newer eastern competitors do not possess.

Weaknesses

IDEPA is constrained by the high amount of waste produced due to production sub optimization, unbalanced mixing of equipment (causing uneven occupation rates, bottlenecks). This is leveraged by the need of supplying top brands which demand the highest possible quality. The equipment mix has also a large part of less flexible vintage equipment, which are not suitable for every type of work. For all these reasons, there are problems in meeting the deadlines for samples and orders. There is a dependency on some suppliers, and there are also low potential customers which require long time investment. The corporate processes are slow, and there are limitations on some IT tools that are used.

Opportunities

The CyberFactory#1 presents a great opportunity to establish new partnerships in the supplier value chain that can yield improvements in productivity and security. The improvement of efficiency, reduction of waste and quality enhancement due to new data-driven approaches are also opportunities. There is also a return of some textile productions to Europe and a lack of high-

\(^{1}\) Source: [https://ec.europa.eu/growth/sectors/fashion/textiles-clothing_en](https://ec.europa.eu/growth/sectors/fashion/textiles-clothing_en)
quality competition of elastics and ribbons products. All together has the potential to leverage the competitiveness of IDEPA, allowing it to further expand its activities and continue the transition to the industry 4.0 paradigm.

Threats

There is a series of threats that can be enlisted:

- Loss of intellectual property to competitors;
- Political instability in several countries;
- Competition with great technical potential;
- Instability of financial markets;
- Appearance of new markets capable of offering products at more competitive prices;
- Innovative products and rapid competition response;
- Competition competitive prices and deadlines;
- Lack of diversity of competitive suppliers for some materials;
- More dynamic, interactive and digital markets;
- Long and demanding customer specifications;

4.2. Competition Analysis

IDEPA is a 54 years old company with solutions in textile labels, paper labels, elastic and rigid ribbons, and elastane covered yarns. Positioning itself as a 2nd tier automotive supplier for the seat industry, IDEPA is a well-known supplier for prestigious garment and shoe brands.

IDEPA is a produce of woven and printed labels, rigid ribbons and elastics. IDEPA has, in the national market two main competitors: Heliotêxtil and Artefita. The first one has a similar product mix as IDEPA, while the second only produces rigid ribbons. IDEPA competitive advantages are the quality of their products and the customer diversification (also encompassing the automotive sector, where the national competitors aren’t present).

External competitors are Avery Dennison, an US company with revenue of 7.5 USD Billion, and SML, a Chinese company, a high-volume company who has acquired multiple companies in the United States and Spain. Avery Dennison is a strong player in the label market, intelligent labels, RFID, medical microreplication. IDEPA has not yet entered these markets. Avery is also diversifying into new cutting-edge markets such as vacuum insulation panels, windows displays and IOT labels. SML is already present in the brand protection, RFID, Trims, tags and packaging markets. It has also been entering the data management and software solutions for intelligent tag and ticket management.

IDEPA invests in long term relationships with its partners, proactively offering new solutions, making use of global logistics and always trying to improve the performance of its products. It is also investing in R&D, both through innovation projects with external business and academic partners or internally. The pricing strategy reflects a bet in the higher value segments (top textile brands which demand high quality products) and increasing differentiation. IDEPA uses the distribution channels common in its sector: direct b2b distribution. It does not rely in external distributors.
<table>
<thead>
<tr>
<th></th>
<th>IDEPA</th>
<th>Heliotêxtil</th>
<th>Avery Dennison</th>
<th>SML</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>Woven and printed labels, rigid and elastic ribbons, Data Management, Tags, Print shop</td>
<td>Producer of woven and printed labels, transfers, elastics, packaging solutions, rigid ribbons and elastics</td>
<td>Label and Packaging Materials, Reflective Solutions, Digital Ink Solutions, Retail Branding and Information Solutions, RFID, Printer Solutions</td>
<td>Brand Protection Creative Design Data Management Software Solutions RFID Trims Tags Packaging</td>
</tr>
<tr>
<td><strong>Key Competitive Advantage</strong></td>
<td>Product Quality Customization services Differentiation Flexibility Implemented Systems (IDI, ISO, FSC, OEKO-TEX) E-Business</td>
<td>TRANSFER technology</td>
<td>Worldwide operation, innovation, sustainability RFID;</td>
<td>Worldwide operation; Asian production; RFID;</td>
</tr>
<tr>
<td><strong>Target Market</strong></td>
<td>Branding Promo Automotive Knits for covered yarn application;</td>
<td>Branding Promo</td>
<td>Advertising &amp; Promotion, Apparel, Automotive, Consumer Packaged Goods, Electronics &amp; Electrical, Medical &amp; Healthcare, Retail, RFID, Supply Chain &amp; Logistics</td>
<td>Design, Logistics, Manufacturing, Retail</td>
</tr>
<tr>
<td><strong>Market Share</strong></td>
<td>Not Known</td>
<td>Not Known</td>
<td>Not Known</td>
<td>Not Known</td>
</tr>
<tr>
<td><strong>Marketing Strategy</strong></td>
<td>Long term relationship with partners  - Retain medium size international clients;  - Sustainable growth  - Proactively offering new solutions to our customers  - Efficient global logistics  - Improving our service  - Performance  - EDI  - Developing digital marketing  - Problem solving</td>
<td>Branding</td>
<td>Sustainability, creativity, determination, problem solving, develop new systems and solutions</td>
<td>Retailers worldwide, speed, flexibility, integrity and innovation</td>
</tr>
</tbody>
</table>
### New Business Model

#### 4.3.1. Value Proposition

IDEPA intends to deliver a high value proposition to the customer taking advantage of the participation in the CyberFactory#1 project.

The optimizations at production-level, driven by the use of intelligence-as-a-service and production-as-service will also allow IDEPA to improve its efficiency, production capacity, reliability and quality, potentially improving the responsiveness to its customers. Increased digitization of production will enhance the ability to respond more effectively and with more flexibility to complex order mix.

IDEPA proposes an improved customer brand protection against counterfeiting due to the increased traceability of goods, people and improved security. Counterfeiting is one of the main
concerns of manufacturers, and IDEPA will be capable of reinforcing the confidentiality towards the client.

4.3.2. Customer Segments

In geographical terms, IDEPA customers are located in Portugal (59%) and in external markets (41%) (Figure 4). Its customers can be divided in 4 sectors: Branding, yarns, promo and automotive. Branding represents the largest market segment with 68% of sales with the remaining 3 market segments yielding 14%, 10% and 8% of the sales volume, respectively (Figure 5).

![Customer Segments - Geography](image)
4.3.3. Key Partners

IDEPA main partners are the IT Providers (Sistrade providing ERP/MES solutions, Microsoft providing infrastructure and productivity software, HPE providing Servers, Veam for backups, Symantec for endpoint protection and Vodafone providing communications and IT security systems), the Production Equipment manufacturers (Jakob Muller AG, MEI International Srl and Willy Italiana, Horst kind and Automatsa Laser) and the Raw Materials providers (e.g. Sinterama, Fiofibra, Lipaco, Trivialtex, Emperil, W.Barnet GMBH, Fulgar S.P.A., Representações Gilberto Lima, Dtexcom-Têxtil, LDA., and others).

4.3.4. Key Activities

The value proposition implies the production, effective procurement and sales, coupled with customization activities. There is also a high focus on the e-commerce development, as a way of improving B2B relationships, decreasing customer waiting times and increasing the easiness of doing business with IDEPA. IDEPA production implies two main operations: weaving and looming, complemented with secondary activities such as cutting, dyeing, printing and finishing. There are support activities such as the design and warehouse management activities.

4.3.5. Key Resources

The resources needed by the value proposition are the human resources (designers and engineers) and equipment (looms, IT infrastructure and quality inspection).
4.3.6. Customer Relationships

IDEPA strives to achieve excellence and win-win partnerships with its customers through an effective network of worldwide logistics, a B2B online platform and EDI (electronic data interchange).

4.3.7. Channels

Customers will be reached by a dedicated sales team, •Resellers / Distributers, Online Sales Platforms and Business Exhibitions.

4.3.8. Cost Structure

The two major cost items are the salaries and raw materials (each item weighting 37% of the total costs). The equipment and its maintenance yield a 7% of the total costs sheet, while energy represents 3%. The I&D expenses are around 200,000€ and those costs are distributed with around 80% on labour costs and the rest on equipment. Other expenses include marketing and context costs (Figure 6).

Cost Breakdown Structure

![Cost Breakdown Structure](image)

Figure 6 - IDEPA Cost Breakdown Structure

4.3.9. Revenue Streams

As a manufacturing company, IDEPA revenue comes exclusively from the sales of the produced items. Nevertheless, IDEPA intends to further leverage the exploitation of the production data to improve its production scheduling, quality and deadline meeting, and new opportunities may arise regarding the exploration of new data-based revenue streams. The extension of its EDI application to further expand the data connection with suppliers and customers to enable the development of more effective production networks.
4.3.10. Promotion

Promotion of the new business model will be achieved through the sales department and marketing, the presence in international fairs, and continuous in-person contacts with its customers. Promoting IDEPA as a modern Smart Factory brings headlines and attention from advanced customers and enables the creation of production networks.
5. Electronics

The consumer electronics market is highly competitive in terms of offering high technology with affordable prices. Industry 4.0 transformation makes it possible to gather and analyse data across machines, enabling faster, more flexible, and more efficient processes to produce higher-quality goods at reduced costs. This manufacturing revolution will increase productivity, shift economics, foster industrial growth, and change the competitiveness of companies. However, one of the most important challenges of this digital transformation is to ensure the security of the systems.

As a part of the Cyberfactory#1 project, Vestel developed a SWOT analysis to describe its strengths & weaknesses and introduce opportunities & threats in consumer electronics sector. After that, this analysis results were blended with competition profile and the business model that accounts Cyberfactory#1 developments for electronics sector was created.

5.1. SWOT Analysis

5.1.1. Strengths

Vestel is one of the leading companies in consumer electronics sector (2nd largest TV supplier of Europe) with great knowledge in both design and mass production. What makes Vestel powerful in the sector is its ability to design and quickly produce products according to customer needs. This is achieved with strong R&D and flexible production capability. Vestel has 8 R&D centres (4 in Manisa, others in Istanbul, Ankara, Bristol, Shenzhen) with 1600+ R&D workers. There are 408 patent application to EPO and 1150 application to Turkish Patent Office in 2017. The production is made in Vestel City which is located in Manisa, with over 1.5 Million m². The production capacity is 35 Mn/year. High production quantities also bring economies of scale and Vestel can get cost advantages. Lower unit labour costs make Vestel stronger than the European competitors. Vestel also has logistical advantage in exports compared to Far Eastern competitors thanks to the proximity of production facilities to European market. Vestel has high experience in automation and robotic processes in the production side. Another important strength of Vestel is to be a pioneer in digital transformation of the factory. Vestel is investing in its factories in order to achieve the digital transformation called VESTEL 4.0 which is a “Smart Factory” where all processes are carried out by artificial intelligence software.

5.1.2. Weaknesses

There is a tough competition in consumer electronics market due to rapid improvements in technology. Since Vestel is not creating technology itself, it falls into the ‘technology followers’ category in global terms. It also has a strong dependency on key suppliers. The company structure is highly conservative which makes it difficult to make structural changes.

5.1.3. Opportunities

Consumer electronics sector is matured and saturated with big players. Therefore, any action that:

- reduces the production costs
improves the productivity & product quality  
reduces the time to market  
gives the ability to make products according to customer requests  
creates an opportunity for the company to step forward among its competitors. All these actions are in line with the opportunities offered by the Cyberfactory#1 project, and Vestel expects to get the highest benefit from those opportunities:  
- The real-time monitoring of the production and the communication of systems (production lines to warehouse/order management/logistics systems) offers acceleration in the manufacturing life-cycle and increase in the productivity & quality.  
- The communications between the systems also results in minimum operator intervention to the lines and reduces manual burden.  
- Collecting the production data and creating a data lake is another opportunity for making further analysis for predictive maintenance and performance analysis.  

**Threats**  
In spite of the opportunities brought by the digital transformation of the production, the system becomes more open to cyber-physical threats. Increased number of IT devices and services in the system makes it more vulnerable to cyber-physical attacks. Also, the threats become diversified with the increased attack surface. Any successful attack may stop production lines causing great time and money loss. Additionally, any gap with the key suppliers may hold up the processes. Since there is an increasing trend for digital transformation of factories, the implementation of more efficient manufacturing processes by the competitors may leave Vestel behind in the race.  

### 5.2. Competition Analysis  
Vestel is one of the leading ODM manufacturers in the world, operating in the consumer electronics and durables sector. The main scope of Vestel is the design and manufacturing of TV, white goods, smart phone, digital signage products and LED lighting products. However, flagship of all those are TV and white goods. Arçelik has a similar product range and it is the main competitor of Vestel. Arçelik is one the most important manufacturer of durables, consumer electronics and small household appliances in Turkey. Arçelik has 18 manufacturing facilities in 7 countries. B/S/H Home Appliances (Bosch) is the largest manufacturer of home appliances in Europe and one of the leading companies in the sector worldwide. It is a strong competitor in white goods and small household appliances sector. Samsung is another competitor which leads technology in TV, white goods and many other electronic devices.  

When regarding the TV, Vestel is the leader in both domestic market and in Turkey’s TV exports (90% share) with 10.2 Mn/year. Arçelik follows Vestel in domestic market and exports with 3.2 Mn/year for TV. When comes to white goods, Arçelik is the leader in domestic market and exports with 50% share and 14 Mn/year capacity. Vestel is the third player in domestic market and has 30% share in white good exports with 12 Mn/year capacity. Bosch is the leader in European market for white goods and increasing its share considerably in Asia-Pacific, Greater China and T-MEA-CIS region. Samsung is the leader in world’s flat TV market with 16.6% share².  

The competitiveness of Vestel in the sector is its ability to offer new technologies with affordable prices. This is achieved with reduced costs, thanks to Vestel’s experience in R&D,  

---  
innovation and manufacturing. Due to large production numbers, procurement costs are also lowered with economies of scale. Another point of competitiveness is the digital transformation of the Vestel factories, which brings the product quality and lower costs together. Arçelik’s competitiveness comes from its brand name. Since it is one of the pioneers in the sector, it has reputation for best quality products and good after sales support. Bosch have competitive advantages because it is a worldwide company and leading the technology in the sector, it is worldwide and has high technology & quality products in white goods and small household appliances. Samsung is the strongest competitor in both TV and white goods sector because the company itself is developing and producing the main technological assets of their products.

Main target markets of Vestel are Europe and the domestic market. Vestel follows multi-brand strategy. Vestel has Regal, Seg, Finlux, Luxor, Telefunken and Techwood brands in domestic market. In foreign market, Vestel brands are Vestfrost, Atlantic, Dikom, NewPol, Electra, Windsor, Graetz, Servis, Luxor and Finlux. Another important strategy of Vestel is to make license agreements with big brands in order to get the rights for production, marketing, distribution and sales of those brands. Sharp, Toshiba, JVC, Telefunken and Hitachi are among those brands. Arçelik’s target market is wider including Europe, domestic market, Asia-Pacific countries and South Africa. Arçelik owns Beko, Grundig, Altus, Defy, Leisure, Blomberg, Elektragregenz, Arctic, Flavel, Dlawance brands. Bosch serves worldwide with global brands - Bosch, Siemens, Gaggenau, Neff, local brands - Thermador, Balay, Coldex, Constructa, Pitso, Profilo, Zelmer and label brands - Junker, Viva. Samsung is a worldwide brand and their target is to increase the share in USA market.

Vestel has multi-channel strategy for distribution. Vestel products are sold in 1136 Vestel stores, 251 Regal stores, 10 Vestel outlets, in technology & chain markets and through web stores in Turkey. Vestel has 2750 selling points abroad. Vestel products are also sold abroad with other brands mentioned previously. Arçelik also has a similar strategy for distribution. Arçelik products are sold in 3000 Arçelik & Beko stores, in technology & chain markets and through web stores in Turkey. Arçelik has 33 sales and marketing offices in 31 countries. Bosch has a global network of sales and customer service firms: 80 companies in 50 countries. Samsung sells its products with its own brand all around the world through retailers.

As strengths, Vestel has a strong & flexible R&D complemented with great manufacturing experience. Innovation is another aspect that makes Vestel more competitive. Cost and geopolitical advantages are also important strengths. High dependency on key suppliers and conservative structure of the company for structural changes can be considered as the weaknesses. Completion of industry 4.0 transformation in production lines is an opportunity for process and quality improvement. Application of machine learning/artificial intelligence methods to obtained data will allow further analysis for the production and help to organize predictive maintenance. However, digitization brings new threats to the system such as cyber-attacks. Application of better production technologies by the competitors can negatively affect Vestel. Since the dependency on key suppliers is high, any gap or disagreement with them is another threat for the business.

When it comes to Arçelik, it has wide-spread production facilities in different countries and covers a large customer segment which are the most important strengths. Quality of its products, especially white goods is another strong point of Arçelik. However, lower quality in small household appliances and higher prices are its weaknesses. New mergers & acquisitions and completing the digital transformation of the factories might be an opportunity. New products or reduced prices offered by the competitors can be a threat for Arçelik business.
The main strength of Bosch Company is its worldwide reputation and credibility for quality. Also, it has great know-how in different technological areas. Increasing demand to high technology and communicating devices can be an opportunity for Bosch. Also, application of new, smart technologies to everyday devices can be an opportunity to increase their share in consumer goods sector. Similar to other companies in the sector, aftersales support problems in some countries and manufacturing defects in products are the main weaknesses. As a global company, fluctuations in economies is a threat that can reduce revenues. Also, security problems with the connected household devices can be an important threat for Bosch.

When it comes to Samsung, the main strength is the strong research and development capability which enables them to create a loyal customer base to their high-tech product portfolio. Another strength is the quality & cost focus which is achieved by outsourcing its production to different countries that have a competitive advantage in producing quality products at small costs. One of the important opportunities is the introducing new technologies in different product categories. Also, expanding in unchartered geographies is another opportunity to grow business. The growing middle-class customers in the developing world are an opportunity for the by increasing the demand for consumer electronics. Besides strengths and opportunities, threats are the factors that potentially harm the company in the future. One of them is the emergence and growth of Chinese players that dominate the mid-segment in Chinese and Indian market. Another threat is the controversies with other competitors. The weakness of the company is their dependence on Android OS. Too large product diversity is considered another weakness because it prevents giving concentration to each product with utmost importance.

5.3. New Business Model

5.3.1. Value Proposition

Completing the digitalization of the production lines securely is the driving force of Vestel’s business model in Cyberfactory#1 project.

Vestel wants to improve its presence and know-how in production with the achievements of the CyberFactory#1 project. Vestel aims to strengthen its value proposition by collecting & processing data from production lines, making predictive analysis and communicating with the warehouse and order management system. Analysis for machine performances will be possible. This will offer a better value in the electronic manufacturing sector.

With the automation of material management and its integration with the production lines, labour and man-made problems will be minimized and lower cost products will be offered.

Production errors can be prevented and higher quality products can be offered with the analysis of the data which is received from the lines.

Customized products according to customer requests will be provided faster, with better quality and cost, thanks to the optimization of material management.

The technical value chains addressed are as follows:

Table 1 - Technical Value Chains

<table>
<thead>
<tr>
<th>CyberFactory#1 Technical Value Chain</th>
<th>Description</th>
</tr>
</thead>
</table>
5.3.2. Customer Segments

Vestel main customer segment is direct consumers, customers which Vestel serves as an original design manufacturer (ODM) and brand customers which have licensing/branding agreements with Vestel. Private and public enterprises are another customer segment to which Vestel sell a wide range of products from lighting to smart boards especially with tenders.

5.3.3. Key Partners

Vestel has a wide range of key partners from design to manufacturing of the products. In design stage, the partners are electronic component suppliers (such as IC/panel) that support the project in technical means. In manufacturing side, the key partners are mainly ERP providers (SAP), robotics (Kuka), sensor & machine & software (Siemens).

Academia is also an important partner: Vestel gets consultancy from different universities in many areas.

Security actors in the consortium (Lostar and Gohm) also play an important role in the new business model.

5.3.4. Key Competitors

The competition in consumer electronics sector is great. In television side, the most powerful competitors are Samsung, LG, Sony, TCL, Hisense, Arçelik in worldwide. When it comes to white goods area, the competitors are Arçelik, Bosch, Samsung, Indesit and the other brands they own.

5.3.5. Key Activities

The key activities in the new business model are:

- Development: Communication of machines with systems, optimization;
- Data analysis: Creating data lake, predictive analytics;
- Collaboration: Providing security.

5.3.6. Key Resources

The business model relies on:

- Human: Especially experienced personnel in mass production, experienced personnel for AI, ML, optimization and predictive analytics;
- Infrastructure: Production lines as a data source for system development and as a test & validation area;
- Software: Development tools.

### 5.3.7. Customer Relationships

Since Vestel is a consumer goods manufacturer, the customer relationship relies mainly on direct sales of the products to consumers through retailers and continuous after sales support. Vestel has branding/licensing agreements with brand customers in order to get the rights to make design, production and sales of the products under their brands. Brand customers make regular onsite visits Vestel in order to audit the manufacturing processes. The earned innovations with CyberFactory#1 project will improve the product quality while reducing the manufacturing cost and positively impact the customer relationship.

### 5.3.8. Channels

Vestel has Vestel Trading Company to reach its customers. Vestel Electronics is responsible for the design and manufacturing of the products and Vestel Trading is the channel to reach the customers. Brand customers directly communicate with the trading company and have onsite visits in order to audit the products & manufacturing. Direct customers (domestic & foreign) are reached through retailers, chain markets, technology markets, outlets and web sales. Vestel also offers continuous after sales support and try to improve it as much as possible for customer satisfaction and brand reputation. There is a dedicated after sales service which is called Vestel Contact Centre for customer satisfaction. Trading fairs, advertisements and social networks offer other ways to reach our customers.

### 5.3.9. Cost Structure

The cost structure includes
- Research & development costs
- Installation
- Maintenance
- Labour cost
- Infrastructure
- Components & raw materials
- Logistics

### 5.3.10. Revenue Streams

Since Vestel is a consumer electronics company, the main revenue stream is the sales of the products. Vestel expects to reduce production, maintenance, logistics and labour costs with the Cyberfactory#1 project which might be thought as an indirect revenue.

### 5.3.11. Promotion

This new business model will be promoted to brand customers, in social media, advertisements and in fairs.
6. Machine Industry

High Metal is extensively researching market and business-driven applications of new technologies (automation, robotics, artificial intelligence, information security / cyber, materials, user-driven) in food and nutrient manufacturing and processing. Through its MKT brand, the company develops highly automated modular food production line of the future, which is used for cheese making. High Metal's CheeseRobot project aims to research, design, pilot and commercialize a robot-based cheese manufacturing concept that disrupts the current cheese-specific manufacturing line model. The central idea of the CheeseRobot project is that the new operating model will make it possible to produce several different types of cheese on the same CheeseRobot line in a much more flexible manner and in smaller batches.

CyberFactory#1 responds well to the future needs of the food industry. The key aim is an ability to measure more accurately the production process. Brand new features include 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 several perspectives: from the perspective of consumers to get food product with consistent quality and shelf life; from the perspective of authorities with the food safety regulations; and from perspective of production process with the quality control.

The project is also strongly related to the situation of the future food industry in Europe and especially in Finland. There are many innovative start-up companies in the food sector in Finland, and many established players are also seeking new directions for new raw materials and end products. The clear challenge is the lack of advanced suppliers of production machines, processes and equipment at present. This is a great opportunity for High Metal, as well as other machinery and equipment manufacturers in the technology industry. High Metal wants to take advantage of this opportunity and, at the same time, set an example for other companies that want to renew and grow their international business.

In the future, the concept can also be applied outside new dairy products to new food and nutrients (such as oat milk), and, in this sense, the project is very much involved in the future of Food 4.0. technologies and food sufficiency.

From the operations point of view, High Metal case is representing “as a service production line”, where autonomous machine reconfiguration is one of the key functionalities. High Metal expertise is focused on the development of cheese making processes with remarkable IoT solutions. In CyberFactory#1 FOF Value Chain Users, High Metal case is about Machine fabrication. The very important focus on the product development is on the sensor data collection, transfer, warehousing and processing in order to get more power to the cheese making process. Artificial intelligence will play a very important role in developing a self-learning system, which is able to control itself autonomously. Traceability and the continuous quality control are among the other important development issues. The most important issue is to ensure the 100% cyber security in the whole cheese making process with the related IoT system.
6.1. **SWOT Analysis**

<table>
<thead>
<tr>
<th>Strengths</th>
<th>Weaknesses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quality, Design, product development, manufacturing skills</td>
<td>Financial resources, so we must be certain our development brings us positive cash flow next few years</td>
</tr>
<tr>
<td>We do better design and manufacture fast and with good quality</td>
<td>Competitors have bigger resources and bigger teams</td>
</tr>
<tr>
<td>World class designers and great manufacturing skills</td>
<td>We must have better sales team and search for agents</td>
</tr>
<tr>
<td>Quality, product development, helping customers improve their business, machine know-how</td>
<td>Customers only in Scandinavia</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opportunities</th>
<th>Threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Local food is big trend and dairies want to flexibility and scalability to their products</td>
<td>Cybersecurity threats, cheese consumption, quality issues</td>
</tr>
<tr>
<td>With CheeseRobot we are able to increase our product range to hard cheese market.</td>
<td>Our competitors are much bigger companies, with bigger resources, so there might come other solutions that compete with us.</td>
</tr>
<tr>
<td>With data analyse we can learn more about cheese process and help our customers to improve their business more profitable.</td>
<td>Our financial resources are small, but solid at the moment</td>
</tr>
<tr>
<td>Too small customer range at the moment</td>
<td></td>
</tr>
</tbody>
</table>

### 6.2. Competition Analysis

High Metal’s very important business line is cheese making products and processes. During the last years, the industrial internet has brought totally new kind of possibilities to control the cheese making process locally and externally. However, before launching these new processes for customers, also their security needs to be assured.

<table>
<thead>
<tr>
<th>High Metal Solution (MKT brand)</th>
<th>TetraPak</th>
<th>Alpma</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>CheeseRobot</td>
<td>Standard process lines</td>
</tr>
<tr>
<td>Key Competitive Advantage</td>
<td>Yield, flexibility</td>
<td>Mass production</td>
</tr>
</tbody>
</table>
### Target Market
| Cheese Dairies | Cheese Dairies | Cheese dairies |

| Market Share | 30% | 20 % | 10 % |

| Marketing Strategy | Direct sales, agents, licensing | Direct sales, agents | Direct sales |

| Products & Services | Product & services | Product | Product |

| Pricing | 0,5-1,0 M€ | 4-5M€ (total line) | 5-8M€ (total line) |

| Distribution Channels | Direct sales, agents, licensing | Direct sales/partner | Direct sales/partner |

| Strengths | Combination of
- Flexibility
- Scalability
- Quality
- Yield
- Efficiency | Global organization, strong resources | Integrated production line |

| Weaknesses | Data availability | Flexibility, customization, R&D speed | Pricing |

| Opportunities | Product expansion and upgrade, service business | Channel to sell packaging materials | Data based cheese production |

| Threats | Cyber security | Agile production lines | Limited resources |

| Trends | Local food, product varieties, efficiency, space savings | Mass production in Asia | Continuous cheese production |

The benefits of the CheeseRobot project in relation to the current operating model of cheese making (where each type of cheese has its own process and equipment) are summarized below.

- Flexibility in product assortments -> multi-purpose cheese vat
- Multiple vats per robot -> flexibility in production, more uniform granularity in volume production
- The vat is simpler -> inexpensive, hygienic
- Common tools for vats
- Cooking specific choice of tool
- Scalable -> vat size can be selected case by case
- Can be retrofitted in old cheese factories -> no need for additional space / construction
- Future potential of the robot's mission field (machine vision, sampling, etc.)
- Expandability by adding vats
- Uniformity of granulation distribution -> knife cutters

6.3. **New Business Model**

6.3.1. **Value Proposition**

The value proposition of High Metal’s new cheese manufacturing concept is based on the following factors:

- Cheese production line as a service: the new concept enables High Metal’s customers to purchase a complete cheese production line as a turn-key solution combined with long-term operation services, all provided by High Metal.
- Flexibility to change production patches: Modular machinery structure combined with robotic control enables more flexible and efficient manufacturing process and subsequently improving the ROI and OPEX of the customers.
- Helping customers improve their business with machine know-how: Customers benefit from the unique combination of High Metal’s long experience and know-how of designing cheese production process equipment and their knowledge of the latest control systems.
- Safety and security against Cybersecurity threats: Using industry leading system components customers can be convinced of the solutions safety and security properties.

6.3.2. **Customer Segments**

The customers for the new solution are cheese producers, which can vary in size from local small cheese producers to large dairies. From geographical market perspective High Metal has identified the following regional segments:

- Cheese producers in Scandinavia – Large and small producers
- Cheese producers in Europe
- Cheese producers in US / Canada
- Cheese producers in Asia
- Optional: MKT solution for small local producers

6.3.3. **Key Partners**

The new cheese production concept increases the amount of technology in the product significantly. To provide best in class products, High Metal has to collaborate with key partners in the following areas:

- Robot manufacturers
- Automation companies
- Component suppliers
- IoT suppliers
- Material suppliers
- Software companies
- Simulation partner
6.3.4. Key Competitors

Main competition comes from the larger dairy equipment manufacturing firms. The figure below illustrates in particular dairy equipment suppliers, many of which are large global players, and whose flexibility and adaptability are not particularly strong. High Metal sees that a growing SME can challenge the global competitors through innovative combination of technology, networking, solution-centricity, and flexibility.

![Competition landscape of High Metal’s MKT brand (Cheese production equipment).](image)

6.3.5. Key Activities

To offer the next generation cheese production lines the following key activities have been identified:

- Design & product development, Manufacturing of cheese robots and production lines
- Understanding cheese manufacturing process
- Quality management
- Management of Cybersecurity threats

6.3.6. Key Resources

The following resources are essential to carry out the key activities and achieving market leading outcome:

- World class designers
- Great manufacturing skills
- Quality manager
- Product development engineers
- Cheese masters
6.3.7. Customer Relationships

High Metal aims to be the highest quality supplier of cheese production equipment. The foundation for this is the highly customizable product line concept, which can be configured to the specific needs of a particular customer, and can be upgraded easily through its life cycle. This way High Metal can be a long-term business partner for its customers.

6.3.8. Channels

To reach the potential customers High Metal has identified the following channels:

- Direct sales by MKT
- Sales agents
- Dairy production engineers and consultants
- Licensing partners for MKT technology

6.3.9. Cost Structure

- Materials / component costs (compared to traditional equipment)
- Work force for production / engineering / project management
- Sales costs
- Other costs

6.3.10. Revenue Streams

- Possible consulting fees regarding the improvement potentiality
- Pre-engineering of sites
- Project deliveries
- After sales
- Data services

6.3.11. Promotion

The CheeseRobot concept is still at the development phase. Considering this, the most practical way to promote the concept is to involve pilot customers to the development work. Discussions with one of the most advanced customers are currently going on concerning co-developing and testing of the concept.
7. Robotics

Autonomous Guided Vehicle Systems (AGVs) are capable of performing transportation tasks fully unattended at a low price. Applications can be found throughout all industrial branches, from the automotive, printing and pharmaceutical sectors over metal and food processing to aerospace and port facilities. In fact, sales show a continuous increase from 1980 till today, thanks to the new technologies applied from the first prototypes, that reduce costs and increase performance. Since the transportation task of AGVs requires efficient and intelligent routing, actual control systems allow to control a fleet of vehicles reducing deadlocks, collision and inefficient routes. Those systems mark for example sections as occupied, until the task is finished, to avoid deadlocks. Also allow the generation of buffers or queues, as for example in the unloading area.

But probably the most disruptive innovation during the last years, has been the development of platforms based on laser or visual navigation. Those platforms, called autonomous mobile robots (AMRs), reduce highly the integration cost while noticeably improve the flexibility and adaptability in the environment. Those AMRs navigate via maps instead of marked routes which usually require extensive and expensive updates to install. The AMR uses data from cameras and built-in sensors and laser scanners as well as sophisticated software that enables it to detect its surroundings and choose the most efficient route to the target. It works completely autonomous and safe manoeuvre around the different actors from the scenario. The AMRs only need simple software adjustments to change its mission. This lets the robot to perform a variety of tasks at different locations adapting to production requirements. Also reduces the costs of integration, because this technology could be easily and quickly deployed without the need to install expensive modifications to the building infrastructure.

In order to give examples of the current market situation we analysed a set of competitors depicted in Figure 9.

![Companies analysed](image-url)
As the volume and sophistication of cyber-attacks against not only computers but also networks like robotics increases exponentially, it is fundamental to safeguard information of personal interest, as well as national security. Cybersecurity may be defined as the state of being protected against the criminal or unauthorized use of electronic data or the measures to achieve this. Computers have been facing the problem of cybersecurity for decades and considering that the Internet of Things is showing a steady growth, the protection for autonomous vehicles/robotics against criminal or unauthorized use of electronic data is becoming more and more important. On one hand, safety problems cover the consciences associated with the physical integrity of the individuals, but on the other hand hacked robots constitute a danger for society as they could be controlled by unknown third parties. Considering the expected growth of autonomous robots as you can see in the graphics below, it becomes essential to ensure safety against cyberattacks and provide AMRs protection against those issues.

One of Cyberfactory#1 aim is to solve the cybersecurity issue in the above-mentioned AMRs by integrating new developed modules into such a platform in order to demonstrate safe networking. The use case will target a manufacturing scenario where different partners of the project are going to cooperate and intend to solve the cybersecurity issues for AMRs, especially focusing on the development of applications which imply the use of a fleet of robots working together and sharing tasks.

7.1. SWOT Analysis

SWOT analysis involves specifying the objective of the project and identifying the internal and external factors that are favourable or unfavourable to achieve its goals. The identification of these elements is a key for planning later steps in order to reach these objectives. Being aware of the strengths of the project allows for fostering the advantage over others, and knowing its weaknesses can lead to act in order to minimize its effects. It is a tool that provides great insights and allows taking correct business decisions and strategies.
The following SWOT contains the strengths and weaknesses from inside of the project and the opportunities and threats of the market analysis such as technological growth and support, IT security and trends in logistics technology.

**Strengths**
- Long expertise in the new technologies and R&D market.
- Collaboration with other companies and leaders in their respective fields
- Cost and quality advantage with respect to competitors
- Competitive advantages compared with other solutions in the market
- Product differentiation thanks to a Safe and Secure integrated system
- High customization and adapting potential
- Diversification on many fields of robotics (expertise and use of knowledge from different areas)

**Weaknesses**
- Highly competitive market dominated by big players
- High innovation costs and need for a big infrastructure
- Continuous need for safety improved procedures and updates
- Focus on low payload and flexible charges (niche market in the logistics automation market)
- Less available budget than other respective big competitors

**Opportunities**
- Big increase in investment in R&D and new technologies.
- Support from government organizations and other European institutions
- Great growth prospects and scalability opportunities
- Industries are increasingly emphasizing on boosting productivity and optimizing costs through adopting automatized manufacturing techniques.
- Some competitors focus only on mobile and logistics robots (MIR or Robotnik for example).
- Great growth prospects and scalability opportunities.
- Incorporation opportunities and synergies with other emerging technologies in manufacturing such as Big Data.
- Market Increasing exponentially (and connected markets like e-commerce)
  - Global autonomous mobile robots market size is expected to grow by USD 8.47 billion during 2018-2022 at a CAGR of over 24%. Figure 11 shows the growth per region.
Threats

- Increase on potential damages caused by security breaches and cyber-attacks.
- Threat of new entrants. Market and technology still in the early stages.
- Increased reliance on vulnerable IT components and procedures.
- Widening complexity of the supply chain, increasing potential threats.
- Legislation and certification strengthening.
- Tough and strict regulations in robotics and FoF (Factory of the future).

Analysis and considerations:

- Strengths that overcome weaknesses, not just regarding quantity. The biggest concern might be the market being dominated by big players; that, of course, gives a disadvantage to anyone who tries to compete. However, being able to have competitive advantages (such as cost/quality, safety and customization), makes it a viable solution according to the presented aims of the project.
- Seize opportunities leveraging the respective strengths such as taking advantage of the long expertise in R&D and technologies to be used in the increasing investments due to more companies emphasizing in cost optimization. On the other hand, due to current collaborations with leading companies in their fields, more institutions will continue to seek alliances, as well as government organizations that will be of help for continued growth.
- Considering that strengths can predominate weaknesses and can minimize the threats, it is fundamental to keep working on those topics in order to maximize the positive outcome as much as possible. Even though there are still security and cyber-attack issues in autonomous mobile robots, it’s solid strength of already existing systems and still ongoing research (just like the Cyberfactory#1 project is aiming to improve) will overcome these threats in the near future. Furthermore, the growth of the market is showing that more and more SME’s are entering the market which could raise the concern of another threat. However, the cost, quality and competitive advantage thanks to long expertise in a variety of fields, turns this threat into another opportunity.
7.2. Competition Analysis

Altogether, there have been considered 8 companies worldwide as important to create a decent market analysis for the Cyberfactory#1 project. Table 2 shows an overview of those companies, showing information about the profile, the target market, products and services the companies are offering, a price range and distribution channels.

Table 2 - Competitor Overview

<table>
<thead>
<tr>
<th>Profile</th>
<th>Target Market</th>
<th>Products and Services</th>
<th>Pricing</th>
<th>Distribution Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAL Robotics</td>
<td>AIV</td>
<td>Smart Factories (manufacturing), e-commerce, Logistics in Hospitals, Food transportation</td>
<td>AIVs with different configurations</td>
<td>Low/Medium</td>
</tr>
<tr>
<td>MiR</td>
<td>AGV</td>
<td>Manufacturing sector</td>
<td>AGVs with different configurations and payloads</td>
<td>Medium</td>
</tr>
<tr>
<td>Omron</td>
<td>AIV</td>
<td>Smart Factories (manufacturing), e-commerce, Logistics in Hospitals, Food transportation</td>
<td>AIVs with different configurations</td>
<td>High</td>
</tr>
<tr>
<td>Fetch Locus</td>
<td>AMR</td>
<td>Manufacturing sector</td>
<td>AMRs with different configurations</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Courier</td>
<td>E-commerce warehousing</td>
<td></td>
<td>EEUU</td>
</tr>
<tr>
<td>Neobotix</td>
<td>MP</td>
<td>Factory automation</td>
<td>MPs with different configurations</td>
<td>Low/Medium</td>
</tr>
<tr>
<td>Robotnik</td>
<td>CRM</td>
<td>Indoors and outdoors logistics tasks</td>
<td>CMRs with different configurations</td>
<td></td>
</tr>
<tr>
<td>Swisslog</td>
<td>AGV</td>
<td>Smart Factories (manufacturing), e-commerce, Logistics in Hospitals, Food transportation</td>
<td>AGVs with different configurations and payloads</td>
<td></td>
</tr>
</tbody>
</table>

The variables market share, marketing strategy and key competitive advantage were merged as those indicators are presenting a comprehensive and precise overview of the competition analysis. Although MiR is having the biggest market share, selling 150 robots per month due to having external distributors worldwide, the key advantage in the sector of AMRs is the customizability and expertise.

PAL Robotics manufactures the TIAGo Base, which is an expandable small footprint autonomous mobile robot for transportation of up to 100Kg, being able to work in fleet management and has its great benefit of being adaptable to the customers’ needs in any way.
PAL Robotics is one of the market leaders thanks to their experience in producing and researching biped humanoids since 2004. Its marketing strategy “All-in-one modular solution for different sectors” underlines their achievement of being a provider of a very competitive AMR. These aspects are considered as the most important indicators as it is showing that facets like market share and revenue are not a crucial projection for deciding whether a company is a market leader in its sector.

Furthermore, it is necessary to consider the compactness of AMRs as a relevant issue, because it offers the possibility of being able to work even in narrow spaces which, for most of the companies, is still a barrier to achieve.

Figure 12 shows that customizability was important to consider as a key competitive advantage for the TIAGo Base by PAL Robotics.

7.3. **New Business Model**

The market research will be conducted using the frame of a CANVAS model. This business model is a well-defined concept that allows the company easily to describe and manipulate business models to create new strategic alternatives. The model is constituted by eleven elements (building blocks) that are:

- Value propositions
- Customer segments
- Key partners
- Key competitors
- Key activities
- Key resources
- Customer relationships
- Channels
- Cost structure
- Revenue streams
7.3.1. Value Proposition

Safe and secure systems in which their factories, robots and procedures can withstand possible external attacks, breaches and theft attempts.

The mobile robot is highly versatile, making it suitable for industrial plants, warehouses, healthcare, hospitals and labs, hotels and offices.

TIAGo Base is totally customizable according to the customers’ needs. We offer different models; the objective is to find the perfect match for every client in order to solve each problem they are facing. We design and manufacture with accessories to adapt to any specific need. Moreover, as each model is unique, we propose different quotes following the requirements.

Pal Robotics aims to resolve problems regarding information stealing, industrial espionage, system breaches and security problems. It also aims to develop optimisation strategies, planning and design for improved operations, systems and activities regarding Transportation, Manufacturing and Control for a wide variety of industries for the FoF.

Final output is going to be an Autonomous Robot equipped with CyberSecurity tools for logistics tasks in an industrial scenario.

Furthermore, the robot provides the option of collecting sensed data while moving in the environment which can be used for the optimization of the processes.

7.3.2. Customer Segments

Pal Robotics is creating value for companies aiming to automate intralogistics and optimize their processes through the use of robotics. Indeed, we create to facilitate deliveries in industrial settings, a robot with an autonomous behaviour, an easy control and a customized design.

It offers the opportunity to enhance logistics, cut down costs, and boost efficiency and productivity to manufacturing companies. At this point we are targeting factories and manufacturing plants, easily extendable to hospital, hotels and offices. Our most important customers are manufacturing and logistic plants and warehouses but we are developing new models and technologies to target more markets and uses.

7.3.3. Key Partners

Most of the partners are taking part on the project. The key resources used for this analysis have been code and cybersecurity measures and other industrial capabilities to develop tests and pilots. Key activities of the partners are the development of CyberSecurity packages targeted at logistics tasks in an industrial scenario, especially focused on multi_robot functionalities and security.
7.3.4. Key Competitors

With the entry of new industry players in the mobile robotics segment, a trend of solid, volume-driven growth has been observed in the market with the addition of new and advanced products. The market is developing fast and new competitors as well.

The main competitors in the industry are all small to medium sized players that have an established presence in the market. The major threat comes from the company MiR because they’re best positioned to compete and have the largest market share, selling 150 robots per month.

7.3.5. Key Activities

Key activities are programming and development of safer measures. Testing activities in simulation environment in order to increase the number of possible use cases and testing activities in real environment during the project. New actions will be needed to reach a TRL 9 product for the industrialization of the solution, besides the deployment of pilots in different real scenarios.

These activities combined with the collaboration of different partners will be scaling up the company in case of full commercialisation.

7.3.6. Key Resources

Our distribution channels are direct to the customer through contact, pilot tests and rehearsals.

We have customers all over the world, with a permanent contact. We also offer after sales service and we make sure to maintain contact with customers and provide training to our client according to each model of robots. We provide online tools for support and community building around our platforms to maintain a healthy relationship with our customers.

We also work alongside with universities, in this way we have the opportunity to improve our robots and provide a trusted business relationship with our customers.

7.3.7. Customer Relationships

Relationships with customers are based through the delivery of robotics and services around the automation of logistics, and processes. We establish a close relationship with customers to provide our services, our updates and offer customer support. To explain our customer relationship in greater detail, we offer an included technical online assistance with every robot we sell where the customer is having a twenty-four-seven support. In addition, we have several employees working on the customer relationship/service which enables a rapid and reliable collaboration.

7.3.8. Channels

Direct channels and contact with interested companies and clients. Mainly, business is done through three different channels: distributors, B2B and engagement in EU projects.
7.3.9. Cost Structure

The biggest costs are labour costs due to the highly skilled and specialised workforce and the costs involved in R&D for the development of new robots, models and updates as well as test. Then, for massive production, costs will scale up.

7.3.10. Revenue Streams

Revenue streams comes from the sale of robots to the final clients and customers and through the provision of additional services and optional add-ons to the customer.

We are also working on the development of new possible revenue streams for our robots regarding leasing/renting options and as a Service options. We plan on offering a wider variety of options to our customers to better adapt to their needs.

The customizability of the solution is one of the main selling points.

7.3.11. Promotion

In parallel to the channels, we are reaching our customers through fairs and congresses, through marketing from publications, and through integrators and consulting companies. By publishing posts on our website (blog) and social media regularly and creating a metrics accordingly, we are able to get a significant overview about our social media engagement. This allows us to react correspondingly and reach out to as many potential customers as possible.
8. IIoT & M2M

8.1. SWOT Analysis

Strengths
- Multicompetent consortium having players and research activities crossing IIoT and M2M capabilities
- Cross-country outreach (Europe + beyond, e.g. Canada)
- Sectorial diversity of users directly involved (Aeronautics, Automotive, Electronics, Automation)
- Good mix of SMEs, Research & Academics and Large enterprises
- Good mix of product vendors, system integrators & service providers

Weaknesses
- IIoT platforms adoption is growing but the installed base of complex IT/OT integration is small and focused on narrowly defined outcomes.
- Lack of involvement in standardization bodies except some of the major players like Airbus
- Common IIoT and M2M Security related reference architecture deployment level rather low, vendor-specific architectures available

Opportunities
- Emerging IIoT and M2M Security related reference architecture applications (Good draft example from Enisa³)
- Demand raising for secure IIoT and M2M applications due to increased needs for productivity raise
- Industrial IoT and smart sensing networks involved in shop floor optimization and factory supply chain management
- Focus on integration, and data and device management to ensure platforms scale with needs
- Strong supply push for digitization technology applied to industry
- Development of digital twin technology is also applicable for IIoT and M2M
- Development of secure IIoT and M2M solution applicable for the consortium scope
- Growing exposure of hyper-connected industry
- Trend towards more IT in OT and vice-versa (IoT & IIoT/M2M)

Threats
- Additional cost added to M2M & IIoT solution due hardened and layered security solutions (From components to data integration up to cloud)

- Difficult to explain the return on investment – compared to low cost solution available from the market
- Manufacturing sector is rather conservative, also for applying communication solutions like IIoT and M2M
- Applicable international security standards do not bring enough value due to added cost of implementation for security architectures
- Lack of support from European manufacturers towards scaled and secure industrial IIoT and M2M capacity building

8.2. Competition Analysis

IIoT / M2M solution competition is coming mainly from IIoT/M2M platform and solution providers as well as proprietary systems developed by OEMs. The IIoT platform differs from legacy OT used in industrial environments for its abilities based on following features as defined by Gartner\(^4\):

- The IIoT platform monitors IoT endpoints and event streams, and supports and/or translates a variety of manufacturer and industry proprietary protocols. The IIoT platform also analyses data at the IoT edge (near the asset) and in the cloud and data center.
- The IIoT platform integrates and engages IT and OT systems in data sharing and consumption, as well as enables application development and deployment. Increasingly, the IIoT platform is commonly used to enrich and supplement OT functions for improved asset management life cycle strategies and processes.
- The IIoT platform, in concert with the IoT edge, sensor and mesh networks and through enterprise IT and OT integration, prepares asset-intensive industries to become digital businesses. The transition is accomplished by enhancing data availability and access for production and business stakeholders.

The market for industrial Internet of Things (IIoT) platforms can be described as a set of integrated software capabilities (Gartner). These capabilities span efforts to improve asset management decision making, as well as operational visibility and control for plants, depots, infrastructure and equipment within asset-intensive industries. The IIoT platform may be consumed as a technology suite or as an open and general-purpose application platform, or both in combination. The platform is developed to support the requirements of safety, security and mission criticality associated with industrial assets and their operating environments.

The IIoT platform software in the devices — such as, controllers, routers, access points, gateways and edge computing systems — is considered part of a distributed IIoT platform. On the other hand managed M2M services may encompass integrated and managed IT infrastructure and systems, OT infrastructure and systems, software, network services (connectivity), and IT services Gartner\(^5\). Typical difference in comparison to managed M2M solutions and IoT solutions is the existence of broader platform capabilities on the part of the latter. An example includes the capability for IoT (and IIoT) endpoint and device management.

The following table represents the competition analysis based on the referenced IIoT and M2M platform studies.

\(^4\) Gartner: Magic Quadrant for Industrial IoT Platforms, May 2018 – IDG000337297\n\(^5\) Gartner: Magic Quadrant for Managed M2M Services, December 2018 – IDG00348379
<table>
<thead>
<tr>
<th>M2M/IoT</th>
<th>Our Solution</th>
<th>PTC ThingWorx</th>
<th>Accenture CPaaS</th>
<th>Vodafone Managed M2M Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile</td>
<td>• Secured IIoT / M2M solution</td>
<td>• IIoT platform</td>
<td>• IIoT platform</td>
<td>• Large operator offering managed M2M services</td>
</tr>
<tr>
<td>Key Competitive Advantage</td>
<td>• Layered security according to CyberFactory#1 X definitions applied in HW/SW/Data and sensor architectures</td>
<td>Wide range of users of PLM, CAD, SLM and ALM applications • Delivers connectors to legacy PTC applications.</td>
<td>• Preintegrated IoT services, managed delivery and deployment</td>
<td>Provides a wide range of value-added services to its customers beyond its core connectivity services. End-to-end services from the design of hardware through to providing help desk services through to a growing portfolio of operational services. • Operational services include provisioning and active administratio n of IoT edge device incidents</td>
</tr>
<tr>
<td>Target Market</td>
<td>• FoF adapters, e.g. Consortium member companies, in generic Industrial 4.0 adopters. • Transportation Solutions providers/user companies (e.g. railway (TGV/ICE)) • Automotive OEMs / 1st Tiers (Factory Solutions) • Companies in need for secure IIoT/M2M solutions</td>
<td>Industrial use cases include asset monitoring and predictive maintenance of multiple manufacturing styles and in-field assets</td>
<td>Off-the-shelf applications in transport, spaces, operations and commerce</td>
<td>Vodafone-staffed operating centers located in more than 50 countries. • M2M solutions requiring large fleets of connected devices across North America, Europe, Asia/Pacific and MEA, and for smaller fleets in Latin America</td>
</tr>
</tbody>
</table>
### M2M/IoT

<table>
<thead>
<tr>
<th>Our Solution</th>
<th>PTC ThingWorx</th>
<th>Accenture CPaaS</th>
<th>Vodafone Managed M2M Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>• At the moment small, however industrial customers e.g. for over 3000 devices using the approach</td>
<td>• The leader in “Ability to Execute” and “Visionary” in Magic Quadrant (2018) for IIoT platforms</td>
<td>• A #3 player leader in “Ability to Execute” in Magic Quadrant (2018) for IIoT platforms</td>
<td>• The leader in “Ability to Execute” and “Visionary” in Magic Quadrant (2018) for M2M managed services</td>
</tr>
</tbody>
</table>

### Marketing Strategy

| • Service providers: direct, | • Direct sales, manufacturers invested in PTC’s PLM, CAD, SLM and ALM applications | • Direct sales, internet website | • Multiple vertical markets, including automotive, energy and utilities, health, insurance, industry, public sector, transportation, and retail. |
| • Manufacturing services providers: direct, | • System integrators: direct, | • | |
| • System integrators: direct, | • Product & IIoT / M2M vendors: indirect, resellers & integrators | • | |

### Products & Services

<p>| • Crossed solution: Secured IIoT / M2M solution. | • ThingWorx is a complete end-to-end IIoT platform. | • Accenture’s Connected Platforms as a Service (CPaaS) is a hybrid, multicloud, stand-alone software platform | • End-to-end managed M2M solutions, leveraging its own edge devices, device management software, cloud services, analytics and application enablement assets |
| • CyberFactory#1 solution includes layers of security applied in HW/SW/Data architecture of IIoT / M2M platforms/solutions and physical products to ensure at the same time the actions of authentication | • Delivers connectors to legacy PTC applications. | • A full range of required IIoT platform components for this market. | |
| • The secured IIoT / M2M solution is able to provide seamless and secure communication with the data about individuals, computer related hardware, and software applications, | • PTC maintains a marketplace that offers developers access to connectors and extensions to popular IT and OT apps and hardware. | • Platform is extensible and configurable for specific customer needs. | |
| | • The platform is available as an on-premises deployment, and cloud and hybrid option | | |</p>
<table>
<thead>
<tr>
<th>M2M/IIoT</th>
<th>Our Solution</th>
<th>PTC ThingWorx</th>
<th>Accenture CPaaS</th>
<th>Vodafone Managed M2M Service</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>adapted to smart FoF environment.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Created solutions address the challenges of authentication and encryption of the solutions,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Chart e.g. the best practises for IIoT / M2M solution / network administration from security point of view.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pricing</td>
<td>• N/A</td>
<td>• N/A</td>
<td>• N/A</td>
<td>• N/A</td>
</tr>
<tr>
<td>Distribution Channels</td>
<td>• Service providers: direct,</td>
<td>• Direct sales, internet website</td>
<td>• Direct sales, internet website</td>
<td>• Direct sales to MNCs and small to midsize companies via its operating companies.</td>
</tr>
<tr>
<td></td>
<td>• Manufacturing services providers: direct,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• System integrators: direct,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Product &amp; IIoT / M2M vendors: indirect, resellers &amp; integrators</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Strengths</td>
<td>• Layered security architecture – not vendor specific solution</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Multicompetent consortium having players and research activities crossing IIoT and M2M capabilities</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Sectorial diversity of users directly involved (Aeronautics, Automotive, Electronics, Automation)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Ability to combine the approach with virtual</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manufacturers invested in PTC’s PLM, CAD, SLM and ALM applications -&gt;natural synergies of ThingWorx IIoT platform when creating connected products</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Offers a broad range of platform capabilities and flexible platform delivery options, and the customization capability meets specific customer use</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Vodafone manages the largest pool of cellular connections for M2M and IoT solutions.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Vodafone reported 67 million managed connections at the end of 2017. This reflects year-over-year growth of 23%.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2M/IoT</td>
<td>Our Solution</td>
<td>PTC ThingWorx</td>
<td>Accenture CPaaS</td>
<td>Vodafone Managed M2M Service</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>--------------</td>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td></td>
<td>manufacturing control and execution (ref. e.g. Bittium Prose system)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Weaknesses**

- IoT platforms adoption is growing but the installed base of complex IT/OT integration is small and focused on narrowly defined outcomes.
- Lack of involvement in standardization bodies except some of the major players like Airbus.
- Common IoT and M2M Security related reference architecture deployment level rather low, vendor-specific architectures available.
- Integration to enterprise systems is not native to the PTC ThingWorx IoT platform, although integration is enabled through other third party service providers, or through custom work.
- Lacks deep experience and capabilities in deploying CPaaS in mission-critical and regulated industrial settings.
- Ability to provide effective multisourcing service integration across large numbers of network and service delivery partners.
<table>
<thead>
<tr>
<th>M2M/IoT</th>
<th>Our Solution</th>
<th>PTC ThingWorx</th>
<th>Accenture CPaaS</th>
<th>Vodafone Managed M2M Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Opportunities</td>
<td>• Emerging IIoT and M2M Security related reference architecture applications (Good draft example from Enisa)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Industrial IoT and smart sensing networks involved in shop floor optimization and factory supply chain management</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Focus on integration, and data and device management to ensure platforms scale with needs</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Strong supply push for digitization technology applied to industry</td>
<td>• IIoT platform market size $1.6 billion by 2021 (IoT analytics), CAGR 33% (2015-2021)</td>
<td>• IIoT platform market size $1.6 billion by 2021 (IoT analytics), CAGR 33% (2015-2021)</td>
<td>• By 2023, 10% of managed M2M connectivity will be provided through hyperscale cloud providers</td>
</tr>
<tr>
<td>Threats</td>
<td>• Additional cost added to M2M &amp; IIoT solution due hardened and layered security solutions (From components to data integration up to cloud)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Difficult to explain the return on investment – compared to low cost solution available from the market</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manufacturing sector is rather conservative, also for applying communication solutions like IIoT and M2M</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Digital twin is designed for manufacturers of connected products, offers little support to operators to apply digital twins to environments based on complex, heterogeneous industrial assets and IoT devices</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Lacks of production customers integrating CPaaS into legacy OT technologies and systems in asset-intensive, regulated environments.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trends</td>
<td>• Demand raising for secure IIoT and</td>
<td>• Solution applicable for</td>
<td>• Lack of production</td>
<td>• Security and complexity</td>
</tr>
<tr>
<td></td>
<td>• Lack of production customers integrating CPaaS into legacy OT technologies and systems in asset-intensive, regulated environments.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
8.3. New Business Model

8.3.1. Value Proposition

Proposed solution:

Crossed solution: Secured IIoT / M2M solution.

Table 3: Business Model Overview

<table>
<thead>
<tr>
<th>Key Partners</th>
<th>Key Activities</th>
<th>Value Proposition</th>
<th>Customer Relationships</th>
<th>Customer Segments</th>
</tr>
</thead>
<tbody>
<tr>
<td>M2M/IoT</td>
<td>Our Solution</td>
<td>PTC ThingWorx</td>
<td>Accenture CPaaS</td>
<td>Vodafone Managed M2M Service</td>
</tr>
<tr>
<td>M2M applications due to increased needs for productivity raise</td>
<td>PTC clients</td>
<td>customers still creates a challenge</td>
<td>remain top considerations and challenges to the acquisition process of M2M services</td>
<td></td>
</tr>
</tbody>
</table>

CyberFactory#1 solution includes layers of security applied in HW/SW architecture of IIoT / M2M platforms/solutions and physical products to ensure at the same time the actions of authentication, authorization, roles, delegation, and interchange.

The secured IIoT / M2M solution is able to provide seamless and secure communication with the data about individuals, computer related hardware, and software applications, which are adapted to smart FoF environment.

Created solutions address the challenges of authentication and encryption of the solutions, as well as chart e.g. the best practises for IIoT / M2M solution / (mesh) network administration from security point of view.
These architectures enable seamless connectivity. In addition, reference security architectures like draft proposal of Enisa\(^6\) will be referred for the solution.

The features of the solution address, among others, the topics described in Table 4 (e.g. Enisa).

Table 4 - Topics

<table>
<thead>
<tr>
<th>Feature/Architecture Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data integration layer</td>
<td>Consisting of industrial IoT platform and data secured solution with seamless and secured connectivity from / to ERP/MES/SCADA and other factory systems.</td>
</tr>
<tr>
<td>Traceability and visibility layer</td>
<td>Data analytics, Artificial Intelligence/Machine Learning, M2M communication and prediction components</td>
</tr>
<tr>
<td>Effectiveness and Efficiency</td>
<td>Improved productivity of the solution enabled by predictive maintenance, traceability and accuracy for Operations.</td>
</tr>
<tr>
<td>Smart Work force</td>
<td>Improved HMI (HSE) including Augmented reality features with secured connectivity to / with sensoring devices/IIoT/M2M.</td>
</tr>
<tr>
<td>Cloud connectivity</td>
<td>Utilization of various Cloud solutions offering security is required by IIoT / M2M solutions. Digitized and secure communications with supply chain partners enabling “Digital Factory” and “Digital Delivery” with help of e.g. Digital Twin technologies.</td>
</tr>
<tr>
<td>Security solutions</td>
<td>Applicable and resilient technologies are required to enable cyber secure communication within IIoT/M2M solutions including mesh/sensoring networks. This includes secure connectivity to ERP/MES/SCADA and other factory systems.</td>
</tr>
</tbody>
</table>

The technical value chains addressed are described in Table 5.

Table 5 - Technical value chains addressed

<table>
<thead>
<tr>
<th>CyberFactory#1 Technical Value Chain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP 41</td>
<td>Tracking and geolocation of factory equipment: Connection to sensing data and mesh networks is required to support the phenomena.</td>
</tr>
<tr>
<td>CAP 42</td>
<td>Manufacturing data lake exploitation: Enables data collection and exploitation throughout the manufacturing cycle. IIoT systems are communication enablers for the data collection from sensing, data and mesh networks to support the phenomena.</td>
</tr>
<tr>
<td>CAP 44</td>
<td>Distributed manufacturing: The paradigm is changing from materials flows to digital information flows, and “stand-alone plants can also communicate with other factory sites, merging vast industrial infrastructures already in place with cloud computing and IoT and future with IIoT.</td>
</tr>
<tr>
<td>CAP 50</td>
<td>FoF Resilience: Addresses the Cybersecurity mechanisms for the IIoT/M2M including the</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CyberFactory#1 Technical Value Chain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>applicable sensing / mesh networks.</td>
<td></td>
</tr>
<tr>
<td>CAP 51</td>
<td>Human / Machine access &amp; trust management: Applicable IAM technologies are designed to manage the roles and privileges of (human) users on traditional IT networks. These include heavy management and administrative procedures that make them inappropriate to manage devices (IIoT) with autonomous enrolment and reconfiguration abilities.</td>
</tr>
</tbody>
</table>

Existing assets:

**Bittium SafeMove Mobile VPN** ([https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn](https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn)) - Bittium SafeMove Mobile VPN provides e.g. the following features; zero-click connectivity, seamless roaming, long session persistence, solid security with multifactor authentication, NSA suite B-level encryption, secure Hotspot login, high availability and load balancing, and integration to enterprise infrastructure. Bittium SafeMove Analytics ([https://www.bittium.com/secure-communications-connectivity/bittium-safemove-analytics](https://www.bittium.com/secure-communications-connectivity/bittium-safemove-analytics)) is an intelligent tool for monitoring and analysing device utilization and the performance of wireless networks. Bittium SafeMove® for Industrial IoT can be utilized in industrial internet solutions, mobile computing and multichannel routing products, as well as with wearable smart devices. These solutions provide secure collection, transfer and analysis of device and sensor based data.

**Rugged Tooling** ([www.ruggedtooling.com](http://www.ruggedtooling.com)) creates monitoring and testing tools for IP networks that can be utilized to monitor the IIoT / M2M networks. The high traffic processing capacity, accuracy and customizable product structure of the tools make them suitable for a variety of use cases.

- The PreScope sensor is capable of monitoring IP traffic and creating alerts based on detected anomalies.
- The Rude deviation emulator enables testing the robustness of network elements by creating highly controlled, repeatable deviations into the traffic.
- The Ruge traffic load generator enables testing a network or service capacity by emulating a high number of concurrent IP sessions.

8.3.2. **Customer Segments**

Identified customer segments are the following:

- FoF adapters, e.g. Consortium member companies, in generic Industrial 4.0 adopters.
- Transportation Solutions providers/user companies (e.g. railway (TGV/ICE)) - B2B market
- Automotive OEMs / 1st Tiers (Factory Solutions) - B2B market

8.3.3. **Key Partners**

The key partners include:
• Data integration layer: Providers for IIoT platform and data secured solutions with seamless and secured connectivity from / to ERP/MES/SCADA and other factory systems. (e.g. Sistrade, PTC ThingWorx ((outside consortium))
• Traceability and visibility layer: ML/AI solution providers (like ISEP, Houston Analytics in the consortium). Includes development of data analytics, artificial intelligence, M2M communication and prediction components applicable to IIoT environments
• Smart Work force: Innovative HMI solution providers to enable improved HMI (HSE) including Augmented reality features with secured connectivity to / with sensing devices/IIoT/M2M
• Cloud connectivity: Partners capable to support utilization of various type of Cloud solutions offering security required by IIoT / M2M solutions. Partners providing digitized and secure communications throughout supply chain enabling “Digital Factory” and “Digital Delivery” with help of e.g. Digital Twin technologies (e.g. VTT in the consortium)
• Security knowledge and know-how: Providers for Security Know-How (e.g. VTT, Innovalia, Airbus DS, Netox Solutions in the consortium)

8.3.4. Key Competitors

The identified key competitors are coming from IIoT platform and managed M2M service providers.

8.3.5. Key Activities

The key activities are described in Table 6.

Table 6 - Key activities of the IIOT & M2M Business Model

<table>
<thead>
<tr>
<th>CyberFactory#1 Technical Value Chain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP 41 Tracking and geolocation of factory equipment:</td>
<td>Builds connection to sensing data and mesh networks to support the phenomena.</td>
</tr>
<tr>
<td>CAP 42 Manufacturing data lake exploitation:</td>
<td>Enables data’s collection and exploitation throughout the manufacturing cycle. Potential ML / AI / traceability solutions related to IIoT / M2M solutions e.g. to trace seamless connectivity of these solutions to be studied</td>
</tr>
<tr>
<td>CAP 44 Distributed manufacturing:</td>
<td>Enables the need for scalability telecom and computing means involved in that multi-agent transaction to be able to generate huge amounts of data of different formats that to be processed in near real time for optimization purposes Connections to sensing data and mesh networks to support the phenomena to be built.</td>
</tr>
<tr>
<td>CAP 50 FoF Resilience:</td>
<td></td>
</tr>
</tbody>
</table>
## CyberFactory#1 Technical Value Chain

| CAP 51 | Human / Machine access & trust management: Enables identity and access management (IAM) for IIoT and M2M solutions |
| CAP 54 | Cyber-resilience mechanisms: Addresses the Cybersecurity mechanisms for the IIoT/M2M including the applicable sensing / mesh networks e.g. vulnerability management, incident response concepts and autonomous procedures developed wherever possible to protect from the new vulnerabilities. These activities include e.g. Regular monitoring and detection in case of malware infection. Better threat visibility and early detection of anomalies. Proactive prevention of threats and attacks between IT and OT. Secure data transfer. A next-generation IPS to prevent attacks from exploiting vulnerabilities. Server and application protection across the data center and the cloud. |

### 8.3.6. Key Resources

The key resources include e.g.

- Consortium safety security actors/providers: ADSC, Persistent, Lostar, Bittium, Netox Solutions
- Potential partners / competitors: PTC, Accenture, Vodafone
- Secure IIoT communications (IIoT platform, M2M sensoring, mesh network) providers
- Secure digital factory / related secure cloud expertise (CfMg, XaaS) providers

### 8.3.7. Customers

The customers include e.g.

- Service providers or Manufacturers: e.g. Transportation Solutions (e.g. railway (TGV/ICE), e.g. Bombardier in the consortium), Secure Communications Solutions (e.g. Communication system) or Automotive OEMs / 1st Tiers (Factory Solutions)
- System integrators / IIoT platform providers: prime contractor relation

### 8.3.8. Customer Relationships

The customer relationships include e.g.

- Service providers: Prime contract relations
- Manufacturing services providers: SLAs
- System integrators: prime contract relations
8.3.9. Channels

The following channels are identified similarly applicable to IIoT / M2M:

- Service providers: Direct,
- Operation services: Direct,
- System integrators: Direct,
- Product vendors: Indirect, resellers & integrators
- IIoT/M2M platform vendors: Through Cyberfactory #1 partners and direct

8.3.10. Cost Structure

The following cost structure elements are identified applicable to secure M2M/IIoT applications deployment:

- Service providers: PM + travel,
- System integrators: Risk + PM + Purchasing costs + Subcontracting + Indirect
- Product vendors: R&D + Maintenance + Branding & Marketing + Purchasing
- IIoT platform vendors: cost of cybersecurity development for all layers

8.3.11. Revenue Streams

The following revenue stream elements are identified areas applicable to M2M/IIoT:

- Service providers: time & materials,
- Manufacturing Service Providers: Cost + fees + upsell potential,
- System integrators: fixed price (incl. risk margin) for system / solution deployment and maintenance service
- Product vendors: market price
- IIoT platform vendors: product/solution market price, tailoring costs

8.3.12. Promotion

The promotion activities applicable to M2M/IIoT are:

- Business workshops, ITEA/H2020 events
- Collaboration/contribution to the reference cybersecurity architectures (e.g. M2M / IIoT).
9. ERP & SCADA

The ERP market is highly competitive, with well-established players and stable customers. The decision of implementing or changing ERP is not a trivial one. It usually follows an extensive period of internal evaluation, risk analysis and procurement. It is followed by a complex process of requirement elicitation, design of custom adaptations, migration of data structures, system interconnection, data transformation, integration and finally testing and operation. It implies long-term support contracts and a proximity relation. It is not, therefore, a market where rapid changes occur, which presents a barrier for disruptive and small players.

As part of structured process in the Cyberfactory#1 project which envisions the creation of new business models, the ERP & SCADA players developed a SWOT analysis in order to describe their current situation, including their strong and weak points and analysed the opportunities and threats. Then, that internal analysis was put in face with the competition profile, so finally, having in account the planned CyberFactory#1 developments, the ERP & SCADA Players were able to develop a new business model.

9.1. SWOT Analysis

As the first step, the SWOT analysis collected the conditions of the Sistrade value chain (ERP and SCADA) in the Cyberfactory#1 project.

Strengths

Sistrade, as a company, benefits from being part of a multidisciplinary team, with a diverse and complimentary set of competences. This is a fundamental condition for the successful development of management software for SoS systems, as it can have a comprehensive vision on the FoF challenges that goes beyond their traditional relation with their end user industries. Secondly, the consortium includes partners with strong security knowledge and experience, which is also an area of competences which is lacking in the ERP & SCADA sector. Cybersecurity is a growing concern in the industry as it gradually moves to the Industry 4.0 paradigm, and therefore the opportunity of gaining insights and experience in the field by the Suppliers partners.

Industry 4.0 brings other challenges, such as the use of the massive amounts of collected data. The SUPPLIERS group benefits from the possibility of offering increased value services to its customers by providing specialized data exploration services. It has also the ability to explore integrations with dedicated security solution partners as well as with dedicated data exploration partners.

The group features several industrial partners with distinct and often complimentary challenges which present a good source of experience and provides the base for the development and test if breakthrough features such as distributed manufacturing with dynamic reconfiguration.

Weaknesses

The new products and services planned in the CyberFactory#1 project are data driven, meaning that data is at its core. They depend on an extensive implementation of IIoT data collection infrastructure which is often still not available in many companies.
Opportunities

The fact that the ERP & SCADA market is already a consolidated market with big players, is both a barrier to the entrance of new players or new solutions, but it can also be seen as an opportunity to explore, as the existing players have less flexibility. They have usually well established and evolutive rather than radically innovative solutions, which can provide good opportunities for the marketization of the solutions developed throughout the CyberFactory#1 project.

The Cyberfactory#1 presents a clear opportunity for the suppliers’ group to improve its product compliance with the Industry 4.0, specifically in what concerns to the security of the IoT data flows coming from the shop floor and the intelligence of the solutions offered. This presents a great opportunity to improve the security awareness of its customers, and provide them more robust and efficient solutions.

Threats

Despite the opportunities open, the suppliers value chain is still affected by the fact that the changing or implementation of an ERP and SCADA systems do not occur often in a company lifetime, and therefore the margin for taking the innovations of this project to the market is also reduced. The suppliers’ group is made by medium/small players and big players, with more resources can make similar moves to implement innovations similar to the ones that Cyberfactory will bring and therefore close the gap and decreasing the competitive edge of the suppliers’ partner solutions. The increasing geopolitical and economic tensions may also lead to the rise of protectionism and fragment the markets or create barriers to the products of suppliers’ members.
9.2. Competition Analysis

If, regarding the national market, SISTRADE practices prices higher than some of its competitors, the truth is that it is a leader in the domestic market, which shows that the customers' decision is not made only considering the price, but also by the quality of the product that leads them to buy it in spite of competitor alternatives. Sistrade differentiates by quality, not by price, regarding the competition.

Regarding the international market, competition is greater, not only in relation to price, but also in relation to the quality of the product. The purchasing power of other developed countries is higher, and investment in research and development is far superior than in the national competition. There are two market segment fields where Sistrade solutions are present:

- Generic 1st tier ERPs, comprised by generic ERPs from big suppliers such as SAP, Oracle, Microsoft Dynamics NAV and Axapta, Sage X3 or EPICOR
- ERPs oriented to specific Industries (niche markets) in which Sistrade specializes and leads, such as: Printing; Printing & Packaging Industry; Labels & Flexible Packaging; Security Printing. Sistrade competes with players such as EFI Radius, CERM Software, THEURER or Gestión 21.

It is found that it is very important for the company to have its own brands, both in terms of presentation to the national market and in terms of the international market. Currently the company works with its own brand SISTRADE SOFTWARE which is a registered trademark of INPI (National Institute of Industrial Property).

The quality of the company's products and services is one of the critical success factors, particularly in the International market. Increasingly, the company is under pressure from the different market players, namely customers and partners, to improve the quality of the company's products. The company has invested heavily in this area in recent years, being currently an ISO 9001 certified company.

With an increasingly demanding national and international market with very active competitors, the company needs to keep a special attention to the process of innovation of its products and services in order to remain at the top in terms of international competitiveness. Consequently, innovation level of the company's products and services are decisive for the overall success. In the area where the company operates (the sale of software services to industries), the rhythm of obsolescence is very high, so it requires great focus on innovation. A software product can be innovative and competitive today and fail to be completely within a couple of years. The company uses the NP 4457 management of the innovation process, being currently certified, and then following the good practices of the Standard.

Considering that the company has its product implemented and sold in several countries, it also has local technical assistance facilities that provide local business awareness and allows it to understand and adapt to the reality of each market. Nevertheless, it is essential that the company can further strengthen its presence in markets where it already has clients and to expand its business to markets which the company believes has good chances of doing business.

With its participation in the Cyberfactory#1 project, Sistrade intends to complement its ERP and SCADA product line with data-driven functionalities, bases in a “as-a-service” paradigm, enhancing the key competitive advantages and further improving its market position in what concerns to the differentiation by quality. The fact that CyberFactory#1 also aims to enhance the distributed manufacturing is also a way of delivering increased value by enhancing productive efficiency. The main target market segments remain the same, but now with the possibility of
offering paid ERP connectors to security third party cybersecurity and Artificial Intelligence software.

Regarding the 1st Tier ERP providers, SAP is the largest and probably most widely known provider of ERP solutions for big industries, with a market share of 22%, although the recent years have seen it trying to enter the SME market with solutions such as the SAP Business one. It provides an all-round generic solution for the most common scenarios (usually fortune 500), which is usually heavily customized to meet its customer’s particular demands. SAP distributes its software through a certified network of providers. As strengths, SAP is a no-brainer for big companies (although some spectacular well know failures have also happened), and the solution is considered reliable and robust. As weaknesses, it is very expensive to customize and too complex, including many under the hood legacy parts. Usually SAP deployments imply a big effort in terms of time and money, some of them taking years. The company faces opportunities for expansion, specifically in the SME market, and threats coming from other well-known and resourceful companies such as Oracle. Oracle is also a big player in the field, having acquired smaller companies in several fields, from ERP to RDBMS development. Oracle has two main solutions: a top and a utility solution, both of them being available in the cloud. Its main customers are big/medium SME’s, also providing Industry-specific solutions. Oracle retains a 15% share in the global market, offering the Fusion ERP and Netsuite brands. The products are considered expensive, and its generic offering falls short in direct comparison with other competitors (such as SAP). Microsoft is still a big player, although it has divested from the ERP field, focusing specifically in the CRM solutions, with a market share of around 10%. It is not actively pursuing the ERP field. On the contrary, Sage is a very active player, offering both ERP and CRM solution and targeting smaller and medium companies, with roughly 6% of the market, with distribution through a network of certified providers. As strengths, it has strong global presence, including in the north American market. Its software has been praised recently by its visual fineness in comparison with other competitors. Is weaknesses being that they have had public security breaches. As opportunities, there are strategic acquisitions which can provide increased market share, and Sage has a history of successful acquisitions. Additionally, there is a growing interest in the SME field for business intelligence software. Sage also faces some threats, such as increasing competition pressure on their main market (SMEs) by bigger players which are trying to get a piece of their market. Epicor is also a big player with a global market share of 7.5%, mainly offering ERP, MES and CRM products, both directly and through its own network of providers. Its main strength is the capability of offering a solution with differentiating capabilities for companies with Make-to-Order and Engineer-to-Order requirements. On the weakness side, Epicor relies heavily on direct selling efforts in conjunction with its partner channel to deliver services. Often, this causes confusion about ownership of the implementation project deliverables and accountability. It faces threats from Open Source technologies. Financial obstacles and seemingly increasing debt may jeopardize the long-term strategy for the continued support and development of Epicor ERP products. Infor Systems has the same market share as Epicor, with about 68000 customers worldwide. It provides ERP, MES, SCM, WMS, Business Intelligence and Business Analytics solutions for Small and Midsized companies and large enterprises in diverse industries, such as health care, the public sector, distribution, food and beverage, aerospace, manufacturing and hospitality. Its distribution is based in its own network of distributors. As strengths, it has a strong customer base worldwide. It has opportunities in providing robust and scalable needs of larger organizations, in addition to those of small to mid-size companies. The ERPs Analysis has shown that Infor competes with its Tier I ERP system peers, especially in terms of average implementation duration and cost.
Regarding the ERPs oriented to specific Industries in which Sistrade currently competes, all of them distribute the software directly to their customers. EFI Software provides ERP for Packaging Industry, CRM, Business Intelligence and EDMS (Environment Data Management System). Its strength is its long experience in vertical business areas. Its weakness is that its software is installed on premise, so it is not for globalized industries. There is the opportunity of offering a cloud-based solution. Its main threats are the cloud-based solutions, more agile and capable of powering multi-site companies. CERM Software specifically targets the Web Printing Industry for the SME companies, offering Business Management and Automation Solutions such as Estimating, Job Management and Productions Scheduling. Its main strength is its strong experience in the printing industry, but as with Eurozone companies, it faces problems in export markets due to the high euro valuation. Theurer is also another competitor of Sistrade, offering an ERP|MIS solution with Business Intelligence and CRM functionalities. Its modular structure with limitless expandability, together with its “Best-Practice” processes via Business Templates are the biggest strengths of the product. Gestión 21 has lots of customers in the Spanish speaking countries, but reduced presence outside them. Although it is both considered a strength in Latin America markets, this presents an opportunity, to obtain a share in the other markets by competing with less qualified printing industry software providers.

The SCADA market has big players, such as ABB, Emerson Electric, Honeywell International and Schneider Electric & Siemens. All of these big players offer industrial automation solutions for electrification robotics, industrial automation and Process control systems. Sistrade SCADA is not its main product, being only a software solution (the data acquisition is made through 3rd party hardware), and being so it does not present a complete Scada solution, being a SCADA monitoring solution, and thus it does not directly compete on the same markets.
9.3. **New Business Model**

9.3.1. **Value Proposition**

The CyberFactory#1 aims to develop a new business model which can extract the full advantages of the new concepts researched and tested during the project. This translates into an enhanced value proposition in the ERP & SCADA field.

The ERP and SCADA group aims to provide an increased value proposition in what concerns the distributed manufacturing, by providing manufacturing management as-a-service, in the cloud, allowing dynamic reconfiguration of the industrial System of Systems, including distributed plant management as-a-service. The distributed manufacturing data flows should be secure, and the ERP and SCADA group aims to provide compliance with secure practices and protocols.

Delivering more useful and automated insights to managers and operators in the shop floor is also an objective: the ERP and SCADA group aims to include on-demand knowledge discovery services (such as useful patterns in environment conditions to improve product quality, for example) and include artificial intelligence to power the automated knowledge extraction on top of ERP data.

Another important part of the value proposition is the provision of an API to external Cybersecurity and AI solution vendors to integrate their solutions with the ERP, creating a network of certified providers.

Decision support as-a-service is also envisioned.

The technical value chains addressed are as described in Table 7.

**Table 7** – Technical Value chains addressed

<table>
<thead>
<tr>
<th>CyberFactory#1 Technical Value Chain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAP34  Factory SoS modelling</td>
<td></td>
</tr>
<tr>
<td>CAP41  Real time sensing, tracking &amp; supervision of tools, materials and humans in the supply chain</td>
<td></td>
</tr>
<tr>
<td>CAP42  Data-lake exploitation: enabling to build new business opportunities based on big data analytics over the manufacturing data thread</td>
<td></td>
</tr>
<tr>
<td>CAP43  Optimization of human / machine collaboration on the shop-floor</td>
<td></td>
</tr>
<tr>
<td>CAP44  Distributed manufacturing capability: enabling to optimize the distributing of production load over a network of factories or fab-labs in real time</td>
<td></td>
</tr>
<tr>
<td>CAP50  FoF Resilience</td>
<td></td>
</tr>
<tr>
<td>CAP51  Human / Machine access &amp; trust</td>
<td></td>
</tr>
</tbody>
</table>
9.3.2. Customer Segments

The main Customer segments are the services and industry players, with global production processes (with different production sites that need to be coordinated, optimized and secured).

Specialized Cybersecurity and AI vendors are also important segments as they provide specialized solutions which can be integrated with the ERP.

9.3.3. Key Partners

It is possible to group the key partners by areas:

- PLC Providers: Omron, Siemens, Mitsubishi, Beckoff, Allen Bradley, Rockwell
- Cloud Providers: Microsoft, Amazon, Google, Kamatera, Rackspace, Scaleway, Hetzner, OVH, ALIBABA
- SCADA providers: Arc Informatique, Sistrade, Houston Analytics
- Cyber Security providers: Consortium
- Resellers
- Integrators

9.3.4. Key Competitors

As previously mentioned in the competition analysis, the main competitors can be divided into three segments:

- Generic 1st tier ERPs: SAP, Oracle, Microsoft Dynamics, Sage, Epicor, Infor Systems.
- SCADA providers: ABB, Emerson Electric, Honeywell International and Schneider Electric & Siemens.

9.3.5. Key Activities

The key activities in the renewed business model are:

- Software development (Industry Solutions, particularly for value-added markets such as Printing; Printing & Packaging Industry; Labels & Flexible Packaging; Security Printing)
- Hardware installation and/or integration Specialized Vendor Pitching and Collaboration
- Modelling and Simulation

9.3.6. Key Resources

A data-driven and knowledge-intensive business model as the one currently being presented relies heavily on people:

- Brainware: Computer and Data science, Experienced Industry Consultants, Users involvement, Use Cases, Algorithms (AI, ML, Optimization, UX)
- Hardware: Computers / Servers
- Software: Development Tools, Libraries, Data Storage, Open Source
9.3.7. Customer Relationships

The relationships with customers will be created through on-site pitching and demonstrations, together with online marketing and presence in the relevant industry events. For the customers with established relationships, on-site training and continuous support (both on-site and remote) are fundamental.

9.3.8. Channels

Typically, the players in the ERP and SCADA field opt for one of two strategies: creating a network of certified providers or direct selling its solutions, with the big players usually opting for the first option and the smaller players often opting for the second one.

As the SUPPLIERS group players on the Cyberfactory#1 project belong to the small/medium players, direct sales are more adequate as a main channel. Nevertheless, resellers and country agents are important for penetrating and knowing new geographical markets. This strategy will be complemented through the presence in business fairs, personal contacts, digital and physical media and the presence on online sales platforms and marketplaces.

9.3.9. Cost Structure

The costs underlying this business model proposition include:

- Development
- Marketing
- Installation
- Training
- Operation
- Maintenance

9.3.10. Revenue Streams

As this is a business model based in as-a-service and data-driven paradigms, new revenue streams are envisioned:

- Distributed Manufacturing As-a-service billing: Per-mile / plafond billing (x production units per month), or per location (ex: production plant)
- Intelligence as-a-service billing: Pay-per-report, or Pay-per-Insight
- API-as-a-service for 3rd party integrations: Pay-per-API-call, flat rate
- Basic Cyber-security Module: sold as an additional cost as it may be more relevant for some industries, monthly pay

9.3.11. Promotion

This new business model will be promoted inside the relevant industry clusters and organizations, through the project website, promotion missions to current and potential customer and social media.
10. Security and Safety

10.1. SWOT – S4-Security & Safety

Strengths

Consortium mixing OT and IT security skills
Cross-country outreach (Europe + beyond, e.g. Canada, Turkey…)
Sectorial diversity of users directly involved (Aeronautics, Textile, Electronics, and Automation)
Noticeable advance in topics such as: anomaly/attack detection, identity & access control, authentication & encryption, data mining & machine learning.
Good mix of SMEs, Research & Academics and Large enterprises
Good mix of product vendors, system integrators & service providers
Airbus CyberRange
Including change management skills

Weaknesses

Lack of involvement in standardization bodies
Few experts with both IT and OT security competencies
Inertia due to the misalignments between national funding authorities
Technical issues overestimated

Opportunities

Cyber-attacks in constant progression, targeting both SMEs and large industries
The average global cost of cyber-crime increased by over 27% in 2017 (Accenture)
60% of cyber-breaches or attacks are attributed to insiders* > need for human behaviour watch (*IBM Cyber Security Intelligence Index)
Strong demand pulls for advanced manufacturing capabilities
Strong supply push for digitization technology applied to industry
Development of digital twin technology
Development / existence of cyber-range technology
Development of AI-based detection capabilities
Advent of Industry 4.0 in all sectors of activity, increasing the attack surface
Growing exposure of hyper-connected industry > security needs
Trend towards more IT in OT and vice-versa (IoT & IIOT)
Development of systems and jobs interconnections with necessary cooperation

Threats

Difficult to “sell” security (quantify losses and demonstrate added value)
Perception of cyber-security as an additional constraint and cost factor instead of a business enabler
Difficult to explain the return on investment – particularly towards predictive / preventive security
Manufacturing sector is rather conservative
OT people mindset is not that much into digital security
Remaining cleavage between security and safety people
Lack of open applicable international security standards
Lack of scaled support from European MS to industrial capacity building
Psychological break towards intrusive techno (human behaviour watch) + GDPR
Conflicting requirements between security and privacy
Scarcity of Cyber-skilled profiles for modelling industrial environments
Presence of legacy systems and mismatching life cycle between IT & OT
Reluctance to invest in CPS modelling and digital twins
Aeronautics installations tend to be highly specific and would not easily make a business rationale for
digital twinning

10.2. CAP51-H/M Access & Trust

Strengths

Existing assets:

- CymID (Airbus Identity & Access Management solution)
- Accelerite Trust Management Software: It provides flexible software solutions to manage and secure complex infrastructure for enterprises (mobile devices, PCs, tablets, servers, clouds, legacy and next generation machinery assets, ERP, CRM systems and an increasingly array of connected tooling systems). Accelerite has worked extensively on digital transformation projects for its customers, developing solutions that encompass several combined technologies and capabilities (e.g. IoT, Analytics, Big Data, Machine Learning, Cloud Computing, End Point Management, Security and Threat Prevention, Mobility and Collaborative Lifecycle Management etc.).
- Bittium SafeMove Mobile VPN Secure and Seamless Connectivity: Bittium SafeMove Mobile VPN remote access solution provides always-on, secure and seamless connectivity for mobile workers. By simplifying and improving the reliability of wireless networks, Bittium’s SafeMove solutions address the common connectivity, security and productivity challenges facing today’s mobile workers. Bittium SafeMove Mobile VPN provides e.g. the following features; zero-click connectivity, seamless roaming, long session persistence, solid security with multifactor authentication, NSA suite B-level encryption, secure Hotspot login, high availability and load balancing, and integration to enterprise infrastructure.
- Bittium SafeMove Analytics is an intelligent tool for monitoring and analyzing device utilization and the performance of wireless networks.

Weaknesses

- IAM techniques involve heavy management and administrative procedures that make them inappropriate to the management of identities in cloud environments.
- Management of the booming numbers of IIoT devices and the maintenance & management of roles over time in fast changing organizations.

Opportunities

Biometric authentication:

- Market size $16.8 billion (2018)
- CAGR 20% (2023)

IAM:

- Market size $9.5 billion (2017)

---

7 https://www.bittium.com/secure-communications-connectivity/bittium-safemove-mobile-vpn
8 https://www.bittium.com/secure-communications-connectivity/bittium-safemove-analytics
• CAGR 10.4% (2024)
Automated security e-gate:
• Market size $1 billion (2021)
• CAGR 10% (2017-2021)
• Increasing SaaS demand
• over 20 billion connected objects expected in 2025

Threats
• Hackers will adapt to biometric technology
• Invasive feeling for humans
• Hard competition in biometric authentication with niche/big players well established (e.g. Morpho, Gemalto)
• Changing IAG market → Needs of constant technological adaptation to: cloud expansion + strengthening of legislation and industry standards

10.2.1. Competition analysis

<table>
<thead>
<tr>
<th>Profile</th>
<th>OT-Morpho (Idemia)</th>
<th>Gemalto</th>
<th>Evidian (Atos)</th>
<th>Gunnebo</th>
</tr>
</thead>
<tbody>
<tr>
<td>Market Share</td>
<td>Leader in biometric solutions</td>
<td>Leader in Gartner Magic Quadrant (2014) for “User authentication”</td>
<td>NIA</td>
<td>NIA</td>
</tr>
<tr>
<td>Products &amp; Services</td>
<td>Physiological, morphological and behavioral biometric solutions</td>
<td>Authentication and digital signing products (e.g. ID badges) -Biometric auth. (scanning devices for fingerprint, palm print, face,</td>
<td>Identify and Access Management (IAM) software: Web access manager, single auth., Self Service Software Reset,</td>
<td>Security gates (tripod, airport, metro, etc.) -Security doors -Anti-theft gateways</td>
</tr>
<tr>
<td>OT-Morpho (Idemia)</td>
<td>Gemalto</td>
<td>Evidian (Atos)</td>
<td>Gunnebo</td>
<td></td>
</tr>
<tr>
<td>--------------------</td>
<td>---------</td>
<td>----------------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>and iris capture)</td>
<td>Cloud solutions</td>
<td>-Identity Governance &amp; Administration (IGA)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Pricing**
- 1500 € for a simple biometric reader gate
- NIA
- NIA
- NIA

**Distribution Channels**
- Website, direct sales, tender submission
- Direct sales, internet website / catalogue
- Website
- Direct sales, internet website / catalogue

**Strengths**
- Proven technology + FBI, Interpol, NYPD & Apple provider + International network (all continents) + IPO (Stock Exchange Introduction) in 2020/2021
- Strong establishment and reputation in IAM & ID-cards for governments (40 countries)
- 2017: acquisition of 3M Cogent (biometric auth.)
- 2019: Merger with THALES
- Does not require any modification of existing applications + get the 'France Cybersecurity' label + adapted to GDPR requirements + Quoted as a niche player in the 'Magic Quadrant for (IGA) for its IAM solution’ (2013, Gartner)
- Niche player in the entrance control market (access to buildings & critical infrastructures)
- Subsidiaries in 25 countries and 5 continents

**Weaknesses**
- Can be usurped Phys & Cyber
- Can be stolen Phys & Cyber
- 1-factor authentication Digital only
- Proprietary Phys. only

**Trends**
- Focus on augmented Identity + expand to connected objects
- Apply biometric auth. to IOT applications.
- Extension to personal devices (smartphones...)
- Facial recognition capabilities incorporated into control gates > fast & contactless authentication
10.2.2.  New Business Model

10.2.2.1.  Value Proposition

Authorization, authentication, and continuous trust level management for humans and machines in FoF environments

Crossed solution: Physical and biometric solutions combined with an identity and access management (IAM) Software. CyberFactory#1 solution should include identity-management systems and physical products to ensure at the same time the actions of authentication, authorization, roles, delegation, and interchange. It should be able to manage data about individuals, computer related hardware, and software applications, adapted to FoF environment. The solution should also include granular trust management and behaviour-based identity verification, enabling systems to detect and protect themselves when a user's behaviour is abnormal.

Differentiation factors:

- Improved management of insider threats
- Holistic shop floor access management (cyber & physical)

The IAM market is already very dense. Competition will not be direct because currently none of the actors is exclusively centred on the factory sector. Most of them are focused on banking, governments, e-commerce or generic enterprise markets. A strategy of differentiation by the offer to position CyberFactory#1 as a niche player on hybrid solutions (physical & cyber) for FoF environments seems the best option.

10.2.2.2.  Customer Segments

FoF / Industry4.0

- Automotive
- Aerospace
- Electronics
- Machine Industry

10.2.2.3.  Key Players

- Partners: Consortium safety security actors: ADSC, Accelerite, Lostar, Bittium
- Competitors: OT-Morpho, Evidian, Gemalto
- Key Activities
- Deployment of authentication means
- Access control services

10.2.2.4.  Key Resources

- IT: modelling and dev. skills & tools
• Cloud storage and services
• Cyber-range platform / services
• IP rights
• Test & demo platforms
• Supports for communication, dissemination and exploitation.

10.2.2.5. Customer Relationships
• Service providers: *intuitu personae*
• MSSP: SLAs
• System integrators: prime contractor relation
• Product vendors: branding

10.2.2.6. Channels
• Service providers: direct;
• Operation services: direct;
• System integrators: direct;
• Product vendors: indirect;
• Resellers & integrators: indirect;
• User IAM: direct or indirect – license sales;
• Asset authentication - Indirect Sales (to be integrated in manufacturing equipment, machines and software).

10.2.2.7. Cost Structure
• Service providers: PM + travel,
• MSSP: PM + SOC Infra + IDS + SIEMS,
• System integrators: Risk + PM + Purchasing costs + Subcontracting + Indirect,
• Product vendors: R&D + Maintenance+ Branding & Marketing + Purchasing.

10.2.2.8. Revenue Streams
Prices of some IAM solutions on the market:
• Centrify: Apps is $4 per user per month and App+ is $8 per user per month
• Oracle Identity Cloud Service: Basic - Enterprise User, $1 per hosted named user (100 user minimum); Standard - Enterprise User, $4 per hosted named user (100 user minimum); Standard - Non-Enterprise User $0.02 per hosted named use (1,000 user minimum).
• RSA SecurID Access: Base ($1-3 per user per month), Enterprise ($1-4 per user per month) and Premium ($2-6 per user per month).

• OneLogin: Free SSO for employees for up to three apps and five personal apps; $2 per user per month for SSO and multi-factor authentication for all apps (minimum of 25 users); $4 per user per month for policy-driven security, MFA and end-to-end user management (minimum of 10 users); $8 per user per month for total identity management for the complex enterprise (minimum of five users).

Because of the strong competition in this market and the variety of actors already implanted, CyberFactory#1 should not be too expensive to expect finding a place in the market landscape, despite the strong forecasts of growth of the IAM market. Therefore, the basic license should not be higher than 2$ per user per month.

The revenue stream integrates the following:
• Service providers: time & materials,
• MSSP: Cost + fees + upsells,
• System integrators: Firm fixed price (incl. risk margin),
• Product vendors: market price.

10.2.2.9. Promotion

Use the lobbying power of the consortium partners and take advantage of all the events, conferences and publications to be realized in the frame of CyberFactory#1 dissemination plan to hit the targeted market.

• Targets: Factory owners, IoT & automation vendors
• Media: Usine Nouvelle, Usine Digitale, LeMagIT, European Utility Week, International Cybersecurity Forum, etc...
10.3. CAP52-Robust ML

Strengths

**Existing assets:**

Work from Fraunhofer AISEC in adversarial ML

Weaknesses

None of the consortium partners have competencies and developments on this particular aspect.

Opportunities

New field for opportunities, very few works done yet on the topic

Cobot industry:

- Market size $0.7B (2018) → $12B (2025)
- CAGR 50% (2018-2025)

Proliferation of large and multidimensional data sets

Machine Learning:

- global market will grow from $1.4B (2017) to $8.8B (2022)
- CAGR 44%-2022

Threats

Cobot industry: Closed market + arrival of many new players (including Chinese)

API: Harsh competition, aggressive pricing strategies (e.g. Amazon)
## 10.3.1. Competition Analysis

<table>
<thead>
<tr>
<th></th>
<th>Universal Robots</th>
<th>IBM Watson</th>
<th>Amazon ML</th>
<th>TensorFlow (Google)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>Point solution</td>
<td>Pre-trained model &amp; API Services</td>
<td>Development platforms</td>
<td>Development libraries</td>
</tr>
<tr>
<td><strong>Key Competitive Advantage</strong></td>
<td>Fast set-up, easy programming, flexible deployment and safe use.</td>
<td>Pre-trained</td>
<td>Flexible</td>
<td>Open Source</td>
</tr>
<tr>
<td><strong>Target Market</strong></td>
<td>All industrial segments</td>
<td>All markets (wide range of industries &amp; org.) B2B</td>
<td>All markets</td>
<td>All markets (users from a very wide range of sectors)</td>
</tr>
<tr>
<td><strong>Market Share</strong></td>
<td>More than 55% in 2016 to 46% in 2017 (cobots industry)</td>
<td>Ranked in the Top 4 ML-players by Gartner (w/ Amazon ML, Google Cloud AI, Microsoft Azur)</td>
<td>Ranked in the Top 4 ML-players by Gartner (w/ IBM Watson, Google Cloud AI, Microsoft Azur)</td>
<td>47.74% market share (*Datanyze Universe). Main competitors: Scikit-learn, MLib, Weka, Microsoft Azur ML.</td>
</tr>
<tr>
<td><strong>Products &amp; Services</strong></td>
<td>Collaborative robots (6 degrees of freedom robots)</td>
<td>API services (integrated to work with IMB Watson Studio)</td>
<td>API combining powerful machine learning algorithms with interactive visual tools (in the cloud and at the edge)</td>
<td>Open source software library for ML &amp; high perf. numerical computation</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>30 to 60 k€ / robot</td>
<td>$0.40 / 1,000 predictions $0.40 / capacity unit-hour</td>
<td>Pay par use $0.10 / 1,000 predictions $0.42 / capacity unit-hour</td>
<td>NA</td>
</tr>
<tr>
<td><strong>Distribution Channels</strong></td>
<td>Large distribution network (reselling partnerships)</td>
<td>Large distribution network</td>
<td>Amazon AWS</td>
<td>Open Source</td>
</tr>
<tr>
<td><strong>Strengths</strong></td>
<td>Ubiquitous fully integrated</td>
<td>Easy to integrate IBM community</td>
<td>Highly customizable</td>
<td>Ergonomic UI Fully customizable</td>
</tr>
<tr>
<td></td>
<td>Universal Robots</td>
<td>IBM Watson</td>
<td>Amazon ML</td>
<td>TensorFlow (Google)</td>
</tr>
<tr>
<td>---------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-----------------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>robotic solution</td>
<td>Github repository</td>
<td>machine learning models including automatic data labeling and reinforcement learning</td>
<td>Flexible archi: easy deployment of computation across various platforms (CPUs, GPUs, TPU), and from desktops to clusters of servers to mobile and edge devices.</td>
</tr>
<tr>
<td></td>
<td>Variety of applications (adapted to every industrial sectors)</td>
<td></td>
<td></td>
<td>Google has the potential to attract a significant share of ML workloads. With their advantages in AI, they have an opportunity to become the cloud of choice for not just ML and AI focused startups but also bigger customers.</td>
</tr>
<tr>
<td></td>
<td>Fast set-up, easy programming, flexible deployment and safe use</td>
<td></td>
<td></td>
<td>▸ Google has the potential to attract a significant share of ML workloads. With their advantages in AI, they have an opportunity to become the cloud of choice for not just ML and AI focused startups but also bigger customers.</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>Faces security flaws (on models UR3, UR5 and</td>
<td>Requires cloud resident data</td>
<td>High skills requirements</td>
<td>Very high skills requirements No support</td>
</tr>
<tr>
<td></td>
<td>Universal Robots</td>
<td>IBM Watson</td>
<td>Amazon ML</td>
<td>TensorFlow (Google)</td>
</tr>
<tr>
<td>---------------------</td>
<td>------------------</td>
<td>------------</td>
<td>-----------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Trends</td>
<td>UR10)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>for “inline operations” → slow</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No Scala or Java integration</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>No commercial support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Deep Learning</td>
</tr>
</tbody>
</table>
10.3.2. New Business Model

10.3.2.1. Value Proposition

Techniques to prevent, detect, respond and investigate on adversarial machine learning attempts affecting FoF AI modules

Proposed solution: Robust learning algorithms enabling manufacturers to leverage machine learning and AI for their operational activities, preventing adversarial manipulation of data from malicious actors. It includes techniques to prevent, detect, respond and investigate on adversarial machine learning attempts affecting FoF AI modules.

To contrast with the already existing solutions on the market, the technology developed shall be accessible to “production people” for modifications (flexibility to better fit their operational needs) without requiring high IT-skills.

Differentiation factors: Algorithms resilient to adversarial learning attacks

10.3.2.2. Customer Segments

FoF / Industry4.0
- Automotive
- Aerospace
- Electronics
- Machine Industry

10.3.2.3. Key Players

- Partners: Consortium safety security actors: ADSC, Accelerite, Lostar, Bittium
- Competitors: Universal Robots, Amazon ML, TensorFlow (Google)

10.3.2.4. Key Activities

Software development, algorithm training & testing in industrial environment

10.3.2.5. Key Resources

- IT: modelling and dev. skills & tools
- Cloud storage and services
- Cyber-range platform / services
- IP rights
- Test & demo platforms
- Supports for communication, dissemination and exploitation.
10.3.2.6. **Customer Relationships**

- Service providers: *intuitu personae*
- MSSP: SLAs
- System integrators: prime contractor relation
- Product vendors: branding

10.3.2.7. **Channels**

- Service providers: direct,
- Operation services: direct,
- System integrators: direct,
- Product vendors: indirect, resellers & integrators,
- Indirect: from data scientists to factories through robotics players,
- Indirect: from data scientists to factories through ERP provider for generic process optimization & control,
- Direct: from data scientists to factories for specific process optimisation and control.

10.3.2.8. **Cost Structure**

- Service providers: PM + travel,
- MSSP: PM + SOC Infra + IDS + SIEMS,
- System integrators: Risk + PM + Purchasing costs + Subcontracting + Indirect,
- Product vendors: R&D + Maintenance + Branding & Marketing + Purchasing

10.3.2.9. **Revenue Streams**

- Service providers: time & materials,
- MSSP: Cost + fees + upsells,
- System integrators: Firm fixed price (incl. risk margin),
- Product vendors: market price

10.3.2.10. **Promotion**

Take advantage of all the events, conferences and publications to be realized in the frame of CyberFactory#1 dissemination plan to hit the targeted market. Use the lobbying power of the consortium partners to promote the solution as the unique comprehensive and European solution enabling secure ML and AI in industrial environments.

- Targets: Factory owners, developers & programmers, automation vendors.
10.3.2.11. Positioning

ML is a red market. Competitors are already settled with aggressive pricing strategies (e.g. Amazon) and propose generic solutions for all market segments. In this context, it is not recommended to focus on having the lowest price, but rather focus on the quality of service and safety and security levels delivered to ensure the close correspondence to customer’s needs (manufacturing facilities, production lines, FAL, etc.). In that sense, the main strength of the consortium is its knowledge of the manufacturing environment, its constraints and challenges.

The idea is not to target the lead in the very competitive ML field, nor to compete with big layers (Amazon, IBM, Google), but to propose a solution specific to manufacturing facilities, close to its needs and considering its constraints (e.g. continuity of process). Therefore, a position of integrator and possibly consultant would be recommended to gain in credibility in the manufacturing industry segment.

10.3.2.12. Price

Price of consulting mission, according to the consultancy price market (vary from country to country).

10.4. CAP53-H/M Behavior Watch

Strengths

Existing assets:
Airbus: MMDG traffic generator for ML: Generic component for artificial intelligence learning, generating massive quantity of events and metrics multi-int, multi-source, multi-temporal, multi-variable, implicitly or explicitly labeled. The component lies on an accelerated simulation of scripted behaviors, on a parametric multiplier of time cycles, on a modeling of random variables (possibly linked from predefined or specific parametric laws in the form of dedicated code executed in secured compartment.

- Airbus: Research work on UEBA (Alexandre Dey)
- Airbus: Partnership with ShieldIoT
- Airbus: operates sensors from Forescout (Security Matters), Nozomi, Claroty and Sentryo.

Weaknesses

No own OT sensor in the consortium, needs to be found externally.

Opportunities

Over 20 billion connected objects expected in 2025

Threats

Mass market: compatible business model required
OT service market becomes overcrowded
### 10.4.1. Competition Analysis

<table>
<thead>
<tr>
<th></th>
<th>ShieldIOT</th>
<th>Claroty</th>
<th>Indegy</th>
<th>Sentryo</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>IoT IDS IA based</td>
<td>Active OT IDS Hybrid IDS</td>
<td>Rule-based OT IDS Deterministic IDS</td>
<td>Protocol-based IDS Machine Learning based IDS</td>
</tr>
<tr>
<td><strong>Key Competitive Advantage</strong></td>
<td>Targeted to IoT Scaling up</td>
<td>High detection rate</td>
<td>Low false positive rate</td>
<td>Effective on legacy ICS</td>
</tr>
<tr>
<td><strong>Target Market</strong></td>
<td>IoT and Industrial IoT 4.0 industry, smart cities, connected transport, smart meters, connected buildings, supply chain logistics</td>
<td>Connected Factory (critical industries, energy, nuclear, water, aviation and critical manufacture)</td>
<td>Connected Factory</td>
<td>Connected Factory (energy, oil&amp;gas, utilities, automotive, manufacturing, ...)</td>
</tr>
<tr>
<td><strong>Market Share</strong></td>
<td>New entrant</td>
<td>NIA. Expanded its bookings by &gt;300% (in 2018)</td>
<td>NIA.</td>
<td>NIA.</td>
</tr>
<tr>
<td><strong>Products &amp; Services</strong></td>
<td>ShieldEdge (at the device level) ShieldCloud (a centralized security management module) Focused on IoT environments – scaling up to big data with low false positives</td>
<td>Platform providing IT security and control room engineers with full visibility, continuous threat detection, secure remote access and ongoing risk assessments for ICS, SCADA and OT networks A centralized management console provides a unified view of assets, activities, alerts and access requests.</td>
<td>Platform for industrial automation and control asset tracking, real-time activity monitoring, policy enforcement, and configuration control for OT environments.</td>
<td>ICS CyberVision is a platform designed to secure industrial control systems (ICS) and SCADA networks. ICS CyberVision includes Equipment inventory, Network monitoring and Threat intelligence.</td>
</tr>
<tr>
<td></td>
<td>ShieldIoT</td>
<td>Claroty</td>
<td>Indegy</td>
<td>Sentryo</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------</td>
<td>-------------------------</td>
<td>------------------------------------</td>
<td>--------------------------------------</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>NA (depends on the IOT network)</td>
<td>NA (depends on the IOT network)</td>
<td>NA (depends on the IOT network)</td>
<td>NA (depends on the IOT network)</td>
</tr>
<tr>
<td><strong>Distribution Channels</strong></td>
<td>Direct sales</td>
<td>Direct sales, internet website (demo/quote request)</td>
<td>Direct sales</td>
<td>Network of reselling partners + Direct sales, internet website</td>
</tr>
<tr>
<td><strong>Strengths</strong></td>
<td>No code changes needed + continuity of services even when compromised by attack</td>
<td>No active scanning required (\rightarrow) zero impact on the OT network</td>
<td>Not passive: it can map the network without having to wait for traffic.</td>
<td>Provides control engineers with a detailed view of all equipment in their industrial infrastructures and their vulnerabilities, records each equipment modification in order to identify the source of an attack and detects behaviour anomalies in real time to raise the alarm and collaborate with IT to fight against cyber attacks</td>
</tr>
<tr>
<td>ShieldIoT</td>
<td>ClaroTy</td>
<td>Indegy</td>
<td>Sentryo</td>
<td></td>
</tr>
<tr>
<td>----------</td>
<td>---------</td>
<td>--------</td>
<td>---------</td>
<td></td>
</tr>
<tr>
<td>Security Awards program. - June 2018: raised $60m from investors including equipment manufacturers (Rockwell, Siemens and Schneider-Elec.)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Weaknesses**

- Could be exposed to adversarial machine learning techniques aiming to wrong their training
- Shield IoT: Is potentially not able to connect to all type of IoT Devices – (latency, required bandwidth for communications)
- No network segmentation
- Deterministic IDS not adapted to AI in manufacturing systems
- High rate of false positive
- Could be exposed to adversarial machine learning techniques aiming to wrong their training
- Require long training periods

**Trends**

- Try to develop its activity on the European and French market
- International expansion in Europe & North America

### 10.4.2. Business Model Canvas

**Value Proposition**

Mutual surveillance of humans and machines on shop floor environments, anomaly / misbehaviour / attack detection.

**Proposed solution:**

Combined physical and cyber threats detection: Hybrid IDS which combine signature-based and Machine Learning (ML) based techniques, attempting to benefit of advantages of both approaches, adapted to FoF networks. Propose edge-based IDS for time critical anomaly detection & scalable to big data (for IoT enhanced shop floor).
It should federate IT and OT oriented detection techniques to properly secure cyber-physical systems such as collaborative robots and anticipate shifts of personnel behaviour (ex: reduction of vigilance).

Differentiation factors:
- Adapted to 4.0 industrial environment
- Hybrid
- Scalable with low false positives

**Customer Segments**
FoF / Industry 4.0: Automotive, Aerospace, Electronics, Machine Industry

**Key Players**
- Partners: Consortium safety security actors: ADSC, Accelerite, Lostar, Bittium
- Competitors: see listed in competition analysis: ShieldIOT, clarity, Indegy, Sentryo

**Key Activities**
Software development, machine learning model implementation and training, definition of behaviour rules, deployment on network

**Key Resources**
- IT: modelling and dev. skills & tools
- Cloud storage and services
- Cyber-range platform / services
- IP rights
- Test & demo platforms
- Supports for communication, dissemination and exploitation.

**Customer Relationships**
- Service providers: *intuitu personae*
- MSSP: contracts with SLAs
- System integrators: prime contractor relation
- Product vendors: branding

**Channels**
- Service providers: direct, Operation services: direct,
- System integrators: direct,
- Product vendors: indirect, resellers & integrators
Cost Structure

- Service providers: PM + travel,
- MSSP: PM + SOC Infra + IDS + SIEMS,
- System integrators: Risk + PM + Purchasing costs + Subcontracting + Indirect,
- Product vendors: R&D + Maintenance + Branding & Marketing + Purchasing

Revenue Streams

- Service providers: time & materials,
- MSSP: Cost + fees + upsells,
- System integrators: Firm fixed price (incl. risk margin),
- Product vendors: market price

Promotion

Use the lobbying power of the consortium partners and take advantage of all the events, conferences and publications to be realized in the frame of CyberFactory#1 dissemination plan to hit the targeted market.

- Targets: Chief Information Security Officer (CISO), Chief Information Officer (CIO), Factory owners,
- Channels: Usine Nouvelle, Usine Digitale, LeMagIT, European Utility Week, International Cybersecurity Forum, etc.

Positioning

Hybrid competitors are rare so CyberFactory#1 can enter in the visionary Gartner quadrant in this market, and propose a solution specialized for industry 4.0 (differentiation by the offer). The competitive advantage is played out on the performances of the IDS (number of false positive, real-time detection, reactivity time, capacity of resilience, ensuring the continuity of factory activity, adaptation to existing networks without need of changes in network architectures, security expertise requirement, adapting to a specific 4.0 industrial environment).

Price

Mature market: Several competitors established through strategic alliance and partnership with big industrial players. But there are also new entrants, meaning that the market is not saturated yet. The strong forecasts of growth of the IDS market is positive.

80 k€ per IDS unit / Year

10.5. CAP54-Cyber-Resilience

Strengths

Existing assets:
- StormShield SNi40
- CyberRange
- testing of firewall tech
- impact-based countermeasure assessment and decision support
- IoT secure authentication & encryption

Weaknesses
Lack of adapted methods to validate non-deterministic systems.

Opportunities
Next generation firewall:
- CAGR of 13.7% (2017 to 2024)

Threats
Aggressive pricing strategies from US vendors

10.5.1. Competition Analysis

<table>
<thead>
<tr>
<th></th>
<th>Tofino FW</th>
<th>Stormshield SNi40 (Airbus DS)</th>
<th>Cisco NGFWs</th>
<th>Symantec</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Profile</strong></td>
<td>Industrial Firewall</td>
<td>Industrial Firewall</td>
<td>Next Generation Firewall</td>
<td>Endpoint Detection and Response (EDR)</td>
</tr>
<tr>
<td><strong>Key Competitive Advantage</strong></td>
<td>Maturity Tailored</td>
<td>Trusted EU certifications: ANSSI, OTAN, EAL4+, EU-RESTRICTED</td>
<td>Continuous file trajectory</td>
<td></td>
</tr>
<tr>
<td><strong>Target Market</strong></td>
<td>Industry</td>
<td>Critical industries Manufacturing</td>
<td>Best suitable for large enterprises with complex networking infrastructure</td>
<td>All industries</td>
</tr>
<tr>
<td><strong>Market Share</strong></td>
<td>NIA</td>
<td>NIA</td>
<td>“Leader” in the Gartner 2018 Magic Quadrant</td>
<td>-Leader in Gartner Magic Quadrant (2018) for “Endpoint Protection Platforms” - Boasts 25% of all deployments worldwide and</td>
</tr>
<tr>
<td>Tofino FW</td>
<td>Stormshield Sni40 (Airbus DS)</td>
<td>Cisco NGFWs</td>
<td>Symantec</td>
<td></td>
</tr>
<tr>
<td>-----------</td>
<td>-----------------------------</td>
<td>-------------</td>
<td>----------</td>
<td></td>
</tr>
<tr>
<td><strong>Products &amp; Services</strong></td>
<td>Pre-emptive threat detection + Threat termination + Threat reporting</td>
<td>Firewall protecting industrial networks from other networks (external / unreliable) and from physical aggressions specific to industri. environments (impacts, dust, extreme T°, electromagnetic interferences, ...)</td>
<td>Firewall providing deep visibility into telemetry and any potentially malicious file activity across users, hosts, networks and infrastructure, all in a single view via the Firepower Management Center</td>
<td>EDR using behavioral analysis at the endpoint and AI-based analytics in the cloud to detect advanced attacks.</td>
</tr>
<tr>
<td><strong>Pricing</strong></td>
<td>1,000$</td>
<td>$2,000€</td>
<td>$(10,000-$-100,000$ depends on version)</td>
<td>Starts at 40$ per endpoint per year</td>
</tr>
<tr>
<td><strong>Distribution Channels</strong></td>
<td>Direct Sales (Tofino Security) + as part of systems offered by Hirschmann, Honeywell, Invensys and</td>
<td>Network of reselling partners + Direct sales, internet website</td>
<td>Direct sales &amp; retail (aws Marketplace, ...)</td>
<td>Reselling partnerships</td>
</tr>
<tr>
<td>Strengths</td>
<td>Tofino FW</td>
<td>Stormshield Sni40 (Airbus DS)</td>
<td>Cisco NGFWs</td>
<td>Symantec</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------------------------------------------</td>
<td>------------------------------</td>
<td>----------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>MTL Instruments</td>
<td>detected without plant downtime + no network changes needed + certified to numerous standards + lower maintenance costs</td>
<td>Detect and protect without impacting the industrial activity. Can be installed easily in industrial environments thanks to a simple setup procedure. SNI40 is the only product on the market to have received the First Level Security Certification (CSPN) from ANSSI Got various certifications</td>
<td>Prevents breaches, get fast visibility to detect and stop threats, and automate network and security « 2017 Price » of Global Network Market Leadership (Frost &amp; Sullivan)</td>
<td>123 million sensors record thousands of threat events per second from 157 countries and block 142 million threats daily</td>
</tr>
<tr>
<td>Weaknesses</td>
<td>No defense against 0-days</td>
<td>Absence of reselling partners on the American markets (North / South)</td>
<td>Not dedicated to OT Complex and confusing licensing. 2018 NSS Labs report: “only 70% efficiency against exploits, less than its competitors (~ 95%)”</td>
<td>According to Forrester report, the performance and detection and response capabilities rate pretty low compared to competition.</td>
</tr>
<tr>
<td>Trends</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

10.5.2. New Business Model

Value Proposition

Decision support for incident response and autonomous reconfiguration / remediation management capabilities.

Proposed solution:

Cyber-resilience mechanisms to ensure continuity of processes and maximum availability of the production assets in crisis situations.

Differentiation factors:

- Holistic approach that goes far beyond the only network protection which is provided by industrial firewalls. The envisioned solution encompasses decision support for incident management, as well as autonomous reconfiguration and remediation functionalities.
- OT-IT modelling supporting autonomous / semi-autonomous remediation.

Customer Segments

FoF / Industry4.0: Automotive, Aerospace, Electronics, Machine Industry

Key Players

- Partners: Consortium safety security actors: ADSC, Accelerite, Lostar, Bittium
- Competitors: Tofino, Cisco, Symantec, Stormshield (Airbus DS).

Key Activities

- Software development and deployment on network
- Econometric quantification of company’s processes and tools

Key Resources

- IT: modelling and dev. skills & tools
- Cloud storage and services
- Cyber-range platform / services
- IP rights
- Test & demo platforms
- Supports for communication, dissemination and exploitation.

Customer Relationships

- Service providers: intuitu personae
- MSSP: SLAs
- System integrators: prime contractor relation
• Product vendors: branding

Channels
• Service providers: direct, Operation services: direct,
• System integrators: direct,
• Product vendors: indirect, resellers & integrators

Cost Structure
• Service providers: PM + travel,
• MSSP: PM + SOC Infra + IDS + SIEMS,
• System integrators: Risk+ PM + Purchasing costs + Subcontracting + Indirect,
• Product vendors: R&D + Maintenance+ Branding & Marketing + Purchasing

Revenue Streams
• Service providers: time & materials,
• MSSP: Cost + fees + upsells,
• System integrators: Firm fixed price (incl. risk margin),
• Product vendors: market price

Promotion
Use the lobbying power of the consortium partners and take advantage of all the events, conferences and publications to be realized in the frame of CyberFactory#1 dissemination plan to hit the targeted market.

• Targets: Chief Information Security Officer, Chief Information Officer, Factory owners, System Network Architect, OT/IT modelling.
• Channels: Usine Nouvelle, Usine Digitale, LeMagIT, European Utility Week, International Cybersecurity Forum, etc.

Positioning
Since no competitors seem to address the cyber-resilience issue of the industry 4.0 with such a global approach, CyberFactory#1 could legitimately claim for a position of visionary with its innovative and comprehensive solution.

Price
Compare with the cost of a CSIRT (cost of one intervention / annual cost)
### 10.6. Conclusion

<table>
<thead>
<tr>
<th>CAP51</th>
<th>CAP52</th>
<th>CAP53</th>
<th>CAP54</th>
</tr>
</thead>
<tbody>
<tr>
<td>OT-Morpho</td>
<td>Universal Robotics</td>
<td>Shield IoT</td>
<td>Tofino</td>
</tr>
<tr>
<td>Gemalto</td>
<td>IBM Watson</td>
<td>Claroty</td>
<td>StormShield</td>
</tr>
<tr>
<td>Evidian</td>
<td>Amazon ML</td>
<td>Indegy</td>
<td>Cisco</td>
</tr>
<tr>
<td>Gunnebo</td>
<td>TensorFlow (Google)</td>
<td>Sentryo</td>
<td>Symentec</td>
</tr>
</tbody>
</table>
11. Conclusions

As the European industry makes its transition to the Industry 4.0 paradigm, new challenges and opportunities arise from the increased data interconnections. The opportunities reflect the increased possibility of exploiting the increasing data flows to optimize the production and gain competitive advantages over the competitors: the ability to adequately generate, obtain and treat data to obtain insights and optimize the productive processes is crucial. Additionally, a new world of possibilities is open, as the interconnection of the business players with other actors in their value chains (customers, suppliers, etc) unleashes new heights of operational efficiency across the whole value chain with shared benefits.

On the other hand, the challenges reflect security issues that companies are increasingly exposed to, as the surface-of-attack increases with the diversification of the data sources, data flows, the increased reliance on digital information to get the business running efficiently. These are the challenges of the factory of the future that CyberFactory#1 strives to tackle.

To seize the opportunities and tackle the challenges, CyberFactory#1 partners developed 8 new business models. These new business models, described in this document, present the point of view of each of the Business Model leader on the best business model in their sector to fully extract the advantages of the Factory of the Future. These business models are also a starting point for the development of commercial synergies with external partners in order to leverage and exploit the technical developments of Cyberfactory#1.