Cognitive Heterogeneous Architecture for Industrial IoT

D1.4 CHARIOT Design Method and Support Tools (ver.1)

Document Summary Information

<table>
<thead>
<tr>
<th>Grant Agreement No</th>
<th>780075</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acronym</td>
<td>CHARIOT</td>
</tr>
<tr>
<td>Full Title</td>
<td>Cognitive Heterogeneous Architecture for Industrial IoT</td>
</tr>
<tr>
<td>Start Date</td>
<td>01/01/2018</td>
</tr>
<tr>
<td>Duration</td>
<td>36 months</td>
</tr>
<tr>
<td>Project URL</td>
<td><a href="http://www.chariotproject.eu">www.chariotproject.eu</a></td>
</tr>
<tr>
<td>Deliverable</td>
<td>D1.4 CHARIOT Design Method and Support Tools (ver.1)</td>
</tr>
<tr>
<td>Work Package</td>
<td>WP1</td>
</tr>
<tr>
<td>Contractual due date</td>
<td>M15 31/03/2019</td>
</tr>
<tr>
<td>Actual submission date</td>
<td>M15 29/03/2019</td>
</tr>
<tr>
<td>Nature</td>
<td>R</td>
</tr>
<tr>
<td>Dissemination Level</td>
<td>PU</td>
</tr>
<tr>
<td>Lead Beneficiary</td>
<td>EBOS</td>
</tr>
<tr>
<td>Responsible Author</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>Contributions from</td>
<td>ASP, VLTN, CEA, ILS</td>
</tr>
</tbody>
</table>
### Revision history (including peer reviewing & quality control)

<table>
<thead>
<tr>
<th>Version</th>
<th>Issue Date</th>
<th>% Complete</th>
<th>Changes</th>
<th>Contributor(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>29/03/2018</td>
<td>5%</td>
<td>Initial Deliverable structure</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>V0.2</td>
<td>08/08/2018</td>
<td>10%</td>
<td>Integration of Survey of Industrial IoT threats</td>
<td>Andrea Battaglia (ASP)</td>
</tr>
<tr>
<td>V0.3</td>
<td>08/09/2018</td>
<td>30%</td>
<td>IoT threats initial input</td>
<td>Andrea Chiappetta (ASP)</td>
</tr>
<tr>
<td>V0.4</td>
<td>01/10/2018</td>
<td>40%</td>
<td>IoT threats updates</td>
<td>Andrea Chiappetta (ASP)</td>
</tr>
<tr>
<td>V0.5</td>
<td>15/10/2018</td>
<td>60%</td>
<td>Consolidated design method input</td>
<td>Bill Karakostas (VLTN)</td>
</tr>
<tr>
<td>V0.6</td>
<td>01/11/2018</td>
<td>60%</td>
<td>Restructure and consolidate input</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>V0.7</td>
<td>26/11/2018</td>
<td>80%</td>
<td>IoT Search Index input</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>V0.8</td>
<td>20/12/2018</td>
<td>85%</td>
<td>IoT threats updates</td>
<td>Andrea Chiappetta (ASP)</td>
</tr>
<tr>
<td>V0.9</td>
<td>16/01/2019</td>
<td>95%</td>
<td>Simulation tools input</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>V0.9</td>
<td>21/01/2019</td>
<td>95%</td>
<td>Internal quality assurance process</td>
<td>Stelios Christofi (EBOS) Frini Lazarou (EBOS)</td>
</tr>
<tr>
<td>V1.0</td>
<td>15/02/2019</td>
<td>100%</td>
<td>Final adjustments</td>
<td>Christos Skoufis (EBOS) Andrea Battaglia (ASP) Bill Karakostas (VLTN)</td>
</tr>
<tr>
<td>V1.0</td>
<td>05/03/2019</td>
<td>100%</td>
<td>Internal quality assurance and peer review process</td>
<td>Stelios Christofi (EBOS) Frini Lazarou (EBOS) Bill Karakostas (VLTN) Florent Kirchner (CEA)</td>
</tr>
<tr>
<td>V1.1</td>
<td>13/03/2019</td>
<td>100%</td>
<td>Adjustments on content</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
<tr>
<td>V1.1</td>
<td>18/03/2019</td>
<td>100%</td>
<td>Quality check</td>
<td>Konstantinos Loupos (ILS)</td>
</tr>
<tr>
<td>V1.2</td>
<td>26/03/2019</td>
<td>100%</td>
<td>Final Version</td>
<td>Christos Skoufis (EBOS)</td>
</tr>
</tbody>
</table>

---

1. According to CHARIOT’s Quality Assurance Process:
   - 4 months before Deliverable’s Due Date: 70% should be complete
   - 3 months before Deliverable’s Due Date: 90% should be complete
   - 2 months before Deliverable’s Due Date: close to 100%. At this stage it sent for review by 2 peer reviewers
   - 1 month before Deliverables Due Date Month-1: All required changes by Peer Reviewers have been applied, and goes for review by the Quality Manager
### Disclaimer

The content of the publication herein is the sole responsibility of the publishers and it does not necessarily represent the views expressed by the European Commission or its services.

While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the CHARIOT consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose.

Neither the CHARIOT Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein.

Without derogating from the generality of the foregoing neither the CHARIOT Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

### Copyright message

© CHARIOT Consortium, 2018-2020. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.
# Table of Contents

1 Executive Summary .................................................................................................................. 10
2 Introduction ............................................................................................................................ 11
  2.1 Mapping CHARIOT Outputs ............................................................................................ 11
  2.2 Deliverable Overview and Report Structure ...................................................................... 13
3 Survey of Industrial IoT Threats ............................................................................................ 14
  3.1 Network architectures and technologies of IoT systems .................................................. 15
  3.2 Future evolution of the IoT ............................................................................................... 17
    3.2.1 Evolution and Trends in IoT Security ........................................................................... 17
    3.2.2 A Framework for Threat-driven Cyber Security Verification of IoT Systems .............. 19
    3.2.3 Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking ........................................................................................................... 20
    3.2.4 IoT security tools as recommended by ENISA ................................................................ 20
    3.2.5 Alliance for the Internet of Things Innovation (AIOTI) .................................................. 20
  3.3 IoT in compliance with the GDPR and the NIS ................................................................. 21
    3.3.1 Detecting Privacy Threats in IoT Neighborhoods ......................................................... 21
  3.4 IoT security ........................................................................................................................ 22
  3.5 IoT threats .......................................................................................................................... 24
    3.5.1 Threats on the perception layer .................................................................................... 24
  3.6 Network layer threats ......................................................................................................... 25
    3.6.1 Attacks on the adaptation layer .................................................................................... 25
  3.7 IoT security ........................................................................................................................ 26
    3.7.1 General threats ............................................................................................................. 26
    3.7.2 A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting .................................................................................................................................. 31
    3.7.3 Hardware and software limits of IoT objects ................................................................ 32
    3.7.4 The weak link of IoT devices: "the Firmware" .............................................................. 32
    3.7.5 Taxonomy of Firmware Trojans in Smart Grid Device as examples ............................ 34
    3.7.6 Impact of Firmware Modification Attacks on Power Systems Field Devices ............... 35
    3.7.7 Critical infrastructure protection ................................................................................... 35
    3.7.8 Classification and comparison of critical infrastructure protection tools .......................... 37
    3.7.9 A process-based dependency risk analysis methodology for critical infrastructures ........ 37
    3.7.10 Standards .................................................................................................................... 37
    3.7.11 From SCADA to cloud computing and IoT in the supply chains ................................. 39
  3.8 Cybersecurity in a Transportation Sector & Airports ......................................................... 42
    3.8.1 Rail sector .................................................................................................................... 43
    3.8.2 European Integrated Radio Enhanced Network (EIRENE) ............................................. 45
    3.8.3 European Rail Traffic Management System (ERTMS) ................................................. 45
    3.8.4 Airports Sector ............................................................................................................ 46
  3.9 Smart building ..................................................................................................................... 54
    3.9.1 Integrated building networks ........................................................................................ 54
    3.9.2 The most famous smart building attacks ....................................................................... 55
    3.9.3 Possible solutions to Protecting Smart Buildings from attacks .................................. 55
    3.9.4 Smart Building design and related components .......................................................... 56
    3.9.5 Cyber-threats to smart buildings ................................................................................. 56
4 Consolidated CHARIOT Design Method ............................................................................. 60
  4.1 Overview ............................................................................................................................ 60
    4.1.1 CHARIOT Methodology Stakeholders ......................................................................... 60
    4.2 System engineering ......................................................................................................... 63
D1.4 CHARIOT Design Method and Support Tools (ver.1)

4.2.1 System and context modelling ................................................................. 63
4.2.2 Collecting, analysing and specifying Industrial System requirements ............. 63

4.3 IoT system engineering ............................................................................. 65

4.3.1 IoT system and context modelling ........................................................... 65
4.3.2 IoT Requirements specification ............................................................... 65
4.3.3 IoT component testing and configuration ................................................. 66
4.3.4 CHARIOT platform configuration, deployment and continuous delivery ......... 66

4.4 Continuous engineering ............................................................................ 68

5 Simulation Tools .......................................................................................... 69

5.1 Project requirements .................................................................................. 69

5.2 Market research ......................................................................................... 69

5.2.1 Market research conclusion ....................................................................... 72

5.3 Scenarios utilising Simulation Tool ............................................................. 72
5.3.1 Building Management Scenario .................................................................. 72
5.3.2 Rail Management Scenario ......................................................................... 73

5.4 Development .............................................................................................. 74

5.4.1 Functionalities, technology used and screenshots ........................................ 74
5.4.2 Key benefits and future work ..................................................................... 78

6 IoT search index ............................................................................................ 80

6.1 Search index development .......................................................................... 80

6.1.1 Methodology and development technology .............................................. 81
6.1.2 Market research and desired features ....................................................... 81

6.1.3 Categorization ......................................................................................... 82

6.1.4 Front-end initial designs ........................................................................... 83
6.1.5 Front-end implementation ......................................................................... 83

6.2 Continuous update, Maintenance and Impact Maximization ......................... 88

6.2.1 Administration ......................................................................................... 88
6.2.2 Content structure ..................................................................................... 89

6.2.3 Impact Maximization ................................................................................ 90

7 Conclusions .................................................................................................. 91

8 References .................................................................................................... 94

9 Bibliography .................................................................................................. 97

Annex 1: Search index research ....................................................................... 98
Annex 2: IoT search index categorization .......................................................... 100
Annex 3: IoT search index mockup designs ......................................................... 103
Annex 4: Welcome page screenshots ................................................................. 104
Annex 5: Category page screenshots .................................................................. 105
Annex 6: Sub-category page screenshots ............................................................ 107
Annex 7: Article page screenshots ..................................................................... 109
Annex 8: Search index administration platform ................................................. 111
List of Figures

Figure 1 - The fourth industrial revolution: "Industry 4.0" ................................................................. 15
Figure 2 – The market IoT – Source: A.T. Kearney analysis [10] ............................................................ 17
Figure 3 - IoT installed base, Forbes ....................................................................................................... 18
Figure 4 - Representation of the Internet of Things ecosystem .............................................................. 23
Figure 5 - Representation of the Internet of Things ecosystem .............................................................. 27
Figure 6 - General threats that could affect an IT infrastructure ........................................................... 29
Figure 7 - The taxonomy of firmware Trojans in smart grid gadgets ..................................................... 34
Figure 8 - Modern firmware-controlled devices integrated in every layer of smart grid infrastructure. [53] .... 35
Figure 9 - Critical infrastructure characteristic tree .................................................................................. 36
Figure 10 - The framework of the three major areas of concern ............................................................... 48
Figure 11 - Airport High-Level Representation ....................................................................................... 49
Figure 12 - The landscape of smart building service providers ............................................................... 54
Figure 13 - Exhibit: security threats of an integrated network in a smart building ................................... 55
Figure 14 - Heating, Ventilation and Air Conditioning Control ................................................................. 57
Figure 15 - An ‘onion’ view of systems in the context of CHARIOT ....................................................... 61
Figure 16 - Orthogonal concerns addressed by the CHARIOT method ................................................... 61
Figure 17 - Simulation Tool – User Interface (UI) ................................................................................... 75
Figure 18 - Simulation Tool – IoT Device Parameters ............................................................................. 76
Figure 19 - Simulation Tool – Runtime Execution (Console) and Sample Data Generation .................. 76
Figure 20 - Simulation Tool – Generate Data – Generate Data ................................................................. 77
Figure 21 – Simulation Tool - Temperature, CO2 Sensors, Ventilation Unit Statistical and Other Sensors’ Values .......................................................................................................................... 78
Figure 22 - Accessing the IoT Search Index .............................................................................................. 80
Figure 23 - IoT Search Index – Pages Structure ....................................................................................... 83
Figure 24 - IoT Search Index – Tablet & Smartphone UI .......................................................................... 84
Figure 25 - IoT Search Index - Search ...................................................................................................... 84
Figure 26 - IoT Search Index – Search Results ........................................................................................ 85
Figure 27 – IoT Search Index – Settings ................................................................................................. 85
Figure 28 - IoT Search Index – Latest Articles ......................................................................................... 86
Figure 29 - IoT Search Index – Most Popular & Sticky Articles ............................................................... 86
Figure 30 – IoT Search Index - Administration - Main Page .................................................................... 88
List of Tables
Table 1 - Adherence to CHARIOT’s GA Deliverable & Tasks Descriptions .......................................................... 11
Table 2 - General Threats ....................................................................................................................................... 29
Table 3 - Regulations Overview .......................................................................................................................... 36
Table 4 - Historical cyber-attacks in transport sector until 2018 .............................................................................. 39
Table 5 - The main transportation threats ............................................................................................................ 42
Table 6 - Cybersecurity and Privacy Technologies with respective Cybersecurity and Privacy Engineering Process .......................................................................................................................... 44
Table 7 - The costs of a cyber-security breach can................................................................................................. 47
Table 8 - Functions and Assets ............................................................................................................................... 49
Table 9 - The vulnerabilities identified that can allow the attacks ............................................................................ 53
Table 10 - Most common BAS protocols ................................................................................................................ 58
Table 11 – Simulation Tool - Building Management Scenario ..................................................................................... 73
Table 12– Simulation Tool - Rail Management Scenario .......................................................................................... 73
Table 13 - Simulation Tool - IoT and Other Devices Supported ............................................................................... 75
Table 14 - IoT Search Index – Administration - Content Structure – Article Fields ..................................................... 89
## Glossary of terms and abbreviations used

<table>
<thead>
<tr>
<th>Abbreviation / Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>6LOWPAN</td>
<td>Internet Protocol v 6 Over low power wireless personal area network</td>
</tr>
<tr>
<td>ACI</td>
<td>Airport Council International</td>
</tr>
<tr>
<td>ACRIS</td>
<td>Aviation Community Recommended Information Services</td>
</tr>
<tr>
<td>ACSEC</td>
<td>Advisory committee on information security and data privacy</td>
</tr>
<tr>
<td>AIOTI</td>
<td>Alliance for the Internet of Things Innovation</td>
</tr>
<tr>
<td>ANSP</td>
<td>Air navigation service provider</td>
</tr>
<tr>
<td>AOP</td>
<td>Airport Operation Plan</td>
</tr>
<tr>
<td>APOC</td>
<td>Airport Operations Centre</td>
</tr>
<tr>
<td>APT</td>
<td>Advanced Persistent Threat</td>
</tr>
<tr>
<td>ATO</td>
<td>Automatic Train Operations</td>
</tr>
<tr>
<td>AWS</td>
<td>Amazon Web Services</td>
</tr>
<tr>
<td>BAS</td>
<td>Building automation system</td>
</tr>
<tr>
<td>BOS</td>
<td>Building operating system</td>
</tr>
<tr>
<td>BYOD</td>
<td>Bring your own device</td>
</tr>
<tr>
<td>CANSO</td>
<td>Civil air navigation services organization</td>
</tr>
<tr>
<td>CAPA</td>
<td>Supply Chain Corrective and Preventive actions</td>
</tr>
<tr>
<td>CBI</td>
<td>Computer based Interlocking</td>
</tr>
<tr>
<td>CBTC</td>
<td>Communications-based train control</td>
</tr>
<tr>
<td>CDC</td>
<td>Cloud Data Centre</td>
</tr>
<tr>
<td>CENELEC</td>
<td>European Committee for Electrotechnical standardization</td>
</tr>
<tr>
<td>CI</td>
<td>Critical Infrastructure</td>
</tr>
<tr>
<td>CIA</td>
<td>Confidentiality Availability Integrity</td>
</tr>
<tr>
<td>CIP</td>
<td>Critical Infrastructure Protection</td>
</tr>
<tr>
<td>CoAP</td>
<td>Constrained Application Protocol</td>
</tr>
<tr>
<td>DCS</td>
<td>Distributed Control System</td>
</tr>
<tr>
<td>DDoS</td>
<td>Distributed Denial of Service</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EDC</td>
<td>Edge Data Center</td>
</tr>
<tr>
<td>EIRENE</td>
<td>European Integrated Radio Enhanced Network</td>
</tr>
<tr>
<td>ERMTS</td>
<td>European Railway Traffic Management</td>
</tr>
<tr>
<td>GA</td>
<td>General Assembly</td>
</tr>
<tr>
<td>GAO</td>
<td>Government Accountability Office</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>HTTPS</td>
<td>Hyper Text Transfer Protocol Secure</td>
</tr>
<tr>
<td>HVAC</td>
<td>Heating Ventilation &amp; Air Conditioning</td>
</tr>
<tr>
<td>IACS</td>
<td>Industrial Automated Control System</td>
</tr>
<tr>
<td>ICAO</td>
<td>International civil aviation organization</td>
</tr>
<tr>
<td>ICS</td>
<td>Industrial Control System</td>
</tr>
<tr>
<td>ID</td>
<td>Identification code</td>
</tr>
<tr>
<td>IEC</td>
<td>International Electrotechnical Commission</td>
</tr>
<tr>
<td>Abbreviation</td>
<td>Description</td>
</tr>
<tr>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>IERC</td>
<td>IoT European Research Cluster</td>
</tr>
<tr>
<td>IoT</td>
<td>Internet of Things</td>
</tr>
<tr>
<td>IoT-DAP</td>
<td>Internet of Things Data Analytics Platform</td>
</tr>
<tr>
<td>IPV6</td>
<td>Internet Protocol V 6</td>
</tr>
<tr>
<td>ISA</td>
<td>International Society for Standards</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ISO</td>
<td>International Organization for Standardization</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transport System</td>
</tr>
<tr>
<td>KPI</td>
<td>Key Performance Indicator</td>
</tr>
<tr>
<td>LAN</td>
<td>Local area network</td>
</tr>
<tr>
<td>M2H</td>
<td>Machine to Human</td>
</tr>
<tr>
<td>M2M</td>
<td>Machine to Machine</td>
</tr>
<tr>
<td>MB</td>
<td>Management Board</td>
</tr>
<tr>
<td>MITM</td>
<td>Man in the middle</td>
</tr>
<tr>
<td>MMI</td>
<td>Man machine interfaces</td>
</tr>
<tr>
<td>MQTT</td>
<td>Message Queuing Telemetry Transport</td>
</tr>
<tr>
<td>MR</td>
<td>MapReduce</td>
</tr>
<tr>
<td>NIS</td>
<td>Network and Information Security</td>
</tr>
<tr>
<td>NIST</td>
<td>National Institute of Standards and Technology</td>
</tr>
<tr>
<td>NOP</td>
<td>Network Operation Plan</td>
</tr>
<tr>
<td>OT</td>
<td>Operational Technology</td>
</tr>
<tr>
<td>PCS</td>
<td>Process Control System</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PLC</td>
<td>Programmable Logic Controller</td>
</tr>
<tr>
<td>PNR</td>
<td>Passenger Name Record</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio Frequency Identification</td>
</tr>
<tr>
<td>RFID</td>
<td>Radio-frequency identification</td>
</tr>
<tr>
<td>S2R</td>
<td>Shift2Rail</td>
</tr>
<tr>
<td>SCADA</td>
<td>Supervisory control and data acquisition</td>
</tr>
<tr>
<td>SEO</td>
<td>Search Engine Optimization</td>
</tr>
<tr>
<td>SESAR</td>
<td>Single European Sky ATM research</td>
</tr>
<tr>
<td>SG</td>
<td>Steering Groups</td>
</tr>
<tr>
<td>SPS</td>
<td>Security, Privacy and Safety</td>
</tr>
<tr>
<td>SWIM</td>
<td>System Wide Information Management</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TTM</td>
<td>Time to Market</td>
</tr>
<tr>
<td>UN/CEFACT</td>
<td>United Nations Centre for Trade Facilitation and Electronic Business</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>WCO</td>
<td>World Customs Organization</td>
</tr>
<tr>
<td>WG</td>
<td>Working Groups</td>
</tr>
<tr>
<td>WSN</td>
<td>Wireless Sensor Network</td>
</tr>
</tbody>
</table>
1 Executive Summary

This is the initial version of the Project’s D1.4 Deliverable addressing the Task 1.4 “CHARIOT Design Method and Supporting Tools” along with the work has been performed under this Task.

The deliverable starts with an extensive survey that has been performed by ASP in the Industrial IoT security threats in the sectors of for rail, airports and smart buildings which are relevant to the Project’s LLs. Among others, this survey includes information about the cybersecurity in industrial environments, the network architectures and latest trends in IoT systems technologies, the evolution of the IoT, an IoT compliance with different regulations, such as the General Data Protection Regulation (GDPR), and the Network and Information Systems (NIS). As has been identified, with the new technology trends, security (and privacy) issues, including cyber threats, have been came up in different industrial sectors (i.e. airports, railways and smart buildings). In addition, the increasing number of devices connected via the Internet creates new opportunities but also additional vulnerabilities to attacks due to the potential for more rapid spread of security incidents. The success of having a fully deployed secured IoT environment is strongly dependent on standardization and depth elaboration of various security protocols and in the different ways of developing and designing a privacy-friendly and secure IoT system, such as taking extra measures and precautions while performing sensitive operations.

Information about the CHARIOT design method is also included in this deliverable where in align with the architecture (defined under T2.1), it consolidates the outputs from T1.1 (Classification and use guidelines of relevant standards and platforms), T1.2 (Method for coupling pre-programmed private keys on IoT devices with a block-chain system) and T1.3 (Specialized Static Analysis tools for secure and safe IoT software development) to capture the ‘system of systems’ aspects, encapsulating the vision, actors, objectives and drivers, principles and constraints to business functions, services, processes, data and their relationships and covering all stages of risk and resilience management.

This deliverable version also presents the initial version of simulation tool. This version of the web-based tool (part of the Dashboard solution implemented under T3.5) has been developed to support IoT applications modelling and scenarios for Privacy, Security, Safety along with the generation of simulated IoT data for each LL topology and showcase the usability of different IPSE components. As a next step, a Threat Vulnerability Analysis using multiple methods of assessment will also be implemented, in order to support the scenarios of each LL.

Concluding, this deliverable presents the first version of the web-based Search Index tool, which has been developed to include an index of IoT Threats, Protection Technologies and Governance Models. This tool provides a web environment where a wide range of users (not only within the Consortium) can easily access centralized (and well-organized) hosted publications, articles, and other relevant documents. The threats defined in the above-mentioned survey have been used as the backbone of structuring this Search Index Tool. Throughout and beyond the lifecycle of the project, this tool will continuously be enriched with contents via Rich Site Summary (RSS) feeds and be used for subsequent architectural and design tasks in WP2 and WP3, but also in the capacity building planning in WP5.
2 Introduction

2.1 Mapping CHARIOT Outputs

The purpose of this section, is to map CHARIOT’s Grant Agreement commitments, both within the formal Deliverable and Task description, against the project’s respective outputs and work performed.

<table>
<thead>
<tr>
<th>CHARIOT GA Component Title</th>
<th>CHARIOT GA Component Outline</th>
<th>Respective Document Chapter(s)</th>
<th>Justification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DELIVERABLE</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D1.4 CHARIOT Design Method and Support Tools (V1)</td>
<td>This deliverable will include a report with the Design Method, a Search Index of IoT Threats, Protection Technologies and Governance Models and simulation tools to show application in the Living Labs. An initial version (v1) will be created in M15 and a revised version (v2) with experience gained throughout the CHARIOT project in M33.</td>
<td>Chapters 3-6, and Annexes</td>
<td>These chapters describe the Survey performed in the Industrial IoT threats for rail, airports and smart buildings along with the consolidated Chariot design method. Moreover, the main functionality of the online simulation tool and search index along with screenshots is presented.</td>
</tr>
<tr>
<td><strong>TASKS</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ST1.4.1 Survey of Industrial IoT threats for rail, airports and smart buildings</td>
<td>Under this subtask, a comprehensive survey of threats, relevant protection technologies and governance models for the IoT ecosystem in the transport (e.g. rail, airports) and smart buildings industry will be carried out. The data obtained will be categorized and grouped in such a way as to ease their insertion in the Search Index.</td>
<td>Chapter 3</td>
<td>Description and analysis of the Survey performed in the Industrial IoT threats for rail, airports and smart buildings</td>
</tr>
<tr>
<td>ST1.4.2 Consolidated Chariot Design Method</td>
<td>Consolidate outputs from T1.1 to T1.3 in the CHARIOT Design method to capture the ‘system of systems’ aspects, encapsulating the vision, actors, objectives and drivers, principles and constraints to business functions, services, processes, data and their relationships and covering all stages of risk</td>
<td>Chapter 4</td>
<td>Description of the design method as has been consolidated and satisfy the needs of Chariot</td>
</tr>
</tbody>
</table>
and resilience management. Also, dealing with capability maturity assessment, cost benefit analysis, change management, impact strategies, benchmarking qualification and certification.

<table>
<thead>
<tr>
<th>D1.4 CHARIOT Design Method and Support Tools (ver.1)</th>
<th></th>
</tr>
</thead>
</table>
| **ST1.4.3 Simulation tools**  
Provide tools to support IoT applications modelling and Privacy, Security, Safety Threat Vulnerability Analysis using multiple methods of assessment such as agent and network-based methods utilizing existing tools from CORE. Create a ‘Competence Centre’ within CHARIOT for simulation-based analysis. | Chapter 5  
Analysis, description, and functionalities of the initial version of the simulation tool along with screenshots and research on existing solutions in the market. |
| **ST1.4.4 Development of an interactive web-based IoT Search Index**  
Under this subtask, an interactive web-based. Search Index will be developed that will contain an index of IoT Threats, Protection Technologies and Governance Models. The software tool will also be used for subsequent architectural and design tasks in WP2 and WP3 and capacity building planning in WP5. | Chapter 6.1  
Research on existing solutions in the market along with description and functionalities of the implemented search index tool. |
| **ST1.4.5 Continuous update of the Search Index**  
Under this subtask throughout and beyond the lifecycle of the CHARIOT project users will have the ability to continuously enrich the contents of the search index to provide a one-stop info source for all players in the industrial IoT ecosystem. Connection to Rich Site Summary (RSS) feeds for automatic content updating upon administrator’s reviewing and approval. | Chapter 6.2  
Description of the administration part of the search index tool and the way continuously enrich it with contents, throughout and beyond the lifecycle of the CHARIOT project. |
2.2 Deliverable Overview and Report Structure

The following section provides an overview of the Deliverable’s structure as well as a detailed description of the plan of action in compliance with the expected outcomes of Task 1.4. Special attention is placed on the five Subtasks (listed below) presented in this task and the purpose of the following Sections is to describe in deep each of them.

- Survey of Industrial IoT threats for rail, airports and smart buildings
- Consolidated Chariot Design Method
- Simulation tools
- Development of an interactive web-based IoT Search Index
- Continuous update of the Search Index

A summary of the chapters of this report is included below.

**Section 3** describes and analyses of the Survey that has been performed in the Industrial IoT security threats for rail, airports and smart buildings area.

**Section 4**, describes the design method as has been consolidated and satisfy the needs of Chariot

**Section 5**, analyses, and describes the functionalities of the initial version of the simulation tool that has been implemented along with screenshots and research on existing solutions in the market.

**Section 6**, presents the research on existing indexing solutions in the market and describes the functionalities of the implemented search index tool. All available market solutions are listed in Annex 1. Description of the administration part of the search index tool and the way continuously enrich it with contents, throughout and beyond the lifecycle of the CHARIOT project, it is also described in this section. The appropriate mockup designs along with screenshots from the actual solution are also included in Annexes as listed below:

- Annex 2: IoT Search Index Mockup Designs
- Annex 3: Welcome Page Screenshots
- Annex 4: Category Page Screenshots
- Annex 5: Sub-Category Page Screenshots
- Annex 6: Article Page Screenshots
- Annex 7: Search Index Administration Platform
3 Survey of Industrial IoT Threats

This document focuses on the issues set out in the European Commission’s "Horizon 2020" program and takes into consideration aspects concerning IoT devices as foreseen in the "Chariot" project.

The new generation peripherals and their constant evolution, clearly show that the next decade will be characterized by the connected "objects" constantly interconnected to the Internet leading to the affirmation of the paradigm "Internet of Things (IoT)" that already started to impact in our life all around the world.

The IoT paradigm is already in our daily life, it is growing systematically and with the adoption of 5G technologies, a real disruption will change further our capacity to connect and interconnect objects.

The 5G will provide tailored connectivity meeting demands of different user groups developing infrastructure able to deliver a wide range of innovative services for enterprises, including IoT applications and deep integration of connectivity (e.g. transport telematics).

Speed or easy plug and play don't mean secure, or cyber secure, it is necessary to manage the threats, the quality of the components and in particular, the firmware embedded able to provide an adequate and sufficient level of protection against the new threats "inherent" the cyberspace.

At EU level, recently adopted by the whole Europe the directives aimed to guarantee the protection and the integrity of data Privacy and Critical Infrastructures, as defined in the Critical Infrastructure Protection Directive (2008/114/EC) and in the new European Data Protection Regulation (GDPR 679/2016) and explicated in the European Network and Information Security Directive (NIS 1148/2016) performed on 9 May 2018.

The Internet of Things (IoT) will contribute to improve the opportunity for private (consumer and companies) and public bodies but will be fundamental be able to manage the risks to which they might are exposed. As all new opportunities require a severe analysis of cyber security issues and how to manage this new connected hera.

As for the private sector also for the industry, the Internet of Things (IoT) is seen as a valuable tool to offer opportunities, but often they do not appropriately evaluate the risks to which they might exhibit. This aspect, on the one hand, provides excellent opportunities deriving from having a great variety of apparat/systems always connected, on the other, it exposes to security breaches as the equipment is not always designed taking this aspect into account.

As previously stated, not all IoT devices are used in the same way. Some devices are used by industrial organizations in the energy, finance, public services, transport, construction and health sectors. These settings integrate the so-called Industrial Internet of Things (IIoT) devices into complex IT and OT environments that are subject to specific digital threats that could have severe and impactful consequences.

The central aspect that must be considered concerns the fact that modern cyber threats are dynamic, so we cannot think that the best answer lies in an all-encompassing security check. The right approach should consider the application of security controls for new environments, best practice, and respect for the standard. Also, customers should be an active part in sensitizing manufacturers to incorporate security into IoT devices, protect hardware and software configurations, and set up a specific control to use administrative privileges.

To explain a severe firmware exposure, we take as an example Equation Group², a sophisticated cyber-attack group that developed a module that allows them to install malicious data in the firmware of hard disk making it more difficult to detect and repair.

From the previous definition, it is possible to understand how the Internet of Things will be more and more present in the current and future technological evolution. The potentials that emerged from the paradigm are

---

considerable and stimulate the research and development of new solutions to be offered on the market both in
the business and in the consumer sector.

It is precisely this tremendous concrete opportunity for IoT technological growth that is the fundamental pillar
for the development of the so-called "Fourth Industrial Revolution" known by the term Industry 4.0, as shown in
Figure 1 below.

![Figure 1 - The fourth industrial revolution: "Industry 4.0"](https://en.wikipedia.org/wiki/Industry_4.0)

3.1 Network architectures and technologies of IoT systems

The network architecture typically used by IoT systems has 3 distinct levels:

- Interface with the physical world;
- Mediation;
- Control Center.

At the first level belong all the "objects" that can:

- interact with the surrounding environment;
- provide your identification code (ID);
- acquire specific information;
- execute certain commands.

The systems belonging to this network layer can be passive sensors, which do not require a power supply, or
active sensors for which an energy source is needed for power supply. These sensors are characterized by limited
information processing capabilities and have apparent hardware limitations on data storage.

To allow communication with the second level units, they are provided with specific network interfaces for wired
(wired) connections or radio (wireless) connections.

At the second level belong all the "objects" that can:

- read the identification codes (ID);
- to convey network traffic.

---

3 [https://en.wikipedia.org/wiki/Industry_4.0](https://en.wikipedia.org/wiki/Industry_4.0)
The systems belonging to this network layer are mainly RFID readers and gateways. The role of these "objects" is critical as they have to deal with the collection of information coming from the nodes belonging to the first level and propagate them to the systems belonging to the third level or the Control Centers.

Finally, the systems able to:

- receive information from second-level units;
- memorize the information received;
- process the information collected;
- make the processed data available.

Central purchasing systems and operations centers perform the tasks listed above. They require superior hardware and software technical features as they play a decisive role in the elaboration of the information acquired by the nodes belonging to the network sub-levels.

While the technologies used for the production of objects of the first level is now consolidated and follows specific standards as well as systems belonging to the third level of the network (server and database), the set of other technologies used for the production of methods pertaining to the second level (gateway), however, are affected by the problem related to the lack of official standards which, moreover, are not always followed for the production of hardware and software.

The need to implement standards is more evident if we consider that the information received from different networks can be shared and forwarded to the systems belonging to the Control Center only if previously translated into an intelligible standard data format.

The current limit of the different IoT devices on the market is that they are produced with characteristics that frequently are not able to share the communication standard (e.g., proprietary network protocol) and the application protocol in contravention of the technological paradigm of Internet of Things or communicate and cooperate directly in an automated way.

The previous is referred to in the technical jargon of Machine to Machine (M2M) communication, which differs from the Machine to Human (M2H) communication which indicates, instead, the exchange of information between the device and the real mode surrounding it (people).

According to the analysts of the IoT Observatory of the Politecnico di Milano⁴, a possible solution to allow a new approach to the design of network architectures for IoT systems is to move from a vertical path interested in ad-hoc design of software, hardware and communication protocols, a more horizontal approach oriented to the design of applications able to exploit sensor networks that are interoperable with each other at the apparatus level.

The technologies involved by the IoT are many and concern the most different devices in everyday and industrial use, among which:

- Cameras;
- Environmental sensors;
- Thermostats;
- Detectors;
- wearable items, such as watches and bracelets;
- Electric meters;
- Medical devices;
- Advertising signs;
- Variable message panels.

⁴ https://www.osservatori.net/it_it/osservatori/internet-of-things
IoT systems are to improve the quality of the service offered to the consumer with the aim of improving the quality of life. The technological innovation we are observing has allowed us to increase actual development in the bright field.

3.2 Future evolution of the IoT

A.T. Kearney [10] recently conducted an in-depth research and analysis of IoT to more thoroughly understand the value it offers the EU28 and the ways that member countries can address in the best way the barriers that will keep them from realizing its fullest benefits. There overarching finding: Within the next ten years the market for IoT solutions will be worth €80 billion, and its potential value for the EU28 economy could reach nearly €1 trillion, as shown in Figure 2 below.

![The market for IoT solutions and three areas where IoT will create value](image)

There are many areas of interest related to the future development of innovative IoT solutions, all of which are interested in improving sectors such as industrial production, agricultural cultivation, energy saving, physical, road, and IT security. For this reason, companies will be directly involved in economic growth combined with the competitiveness that will encourage operators in the sector to emerge and position themselves among the pretenders to commercial success.

The expected result will be a sufficient change in the way people work and face everyday life, which will be increasingly combined in the IoT ecosystem.

Thanks to the use of IoT solutions, companies will be able to process the data received from smart devices obtaining increasingly accurate and useful forecasts for production phases, managing to adapt production to demand with significant cost savings dynamically. The entire production chain will be optimized thanks to the possibility of taking decisions quickly and automatically if necessary, to achieve company objectives. The history of the information acquired by the "objects" will allow the development of applications able to process vast amounts of data (Big Data) to prevent breakdowns and in the optimal case avoid them through automatic
machine maintenance schedules. All this will result in higher profitability for companies and consequently better results for customers.

An important consideration regards the growth trend of "online" devices. 2.9 billion People—40% of the world's population—are online today. It has been predicted that by 2020, over 40 billion more devices will be made "smart" through embedded processors and intelligence. The Internet of Things (IoT) has already grown beyond niche industrial and medical applications and has entered every market and industry. Observers expect its growth to be exponential. So transformative are its expected ramifications that some have labeled it "Industry 4.0." The transformation will, in any case, result from an understanding of how digitization is modifying existing relationships and balance of power and responsibilities among the different actors along the value chain: suppliers, buyers, competitors, and substitutes. The following shifts in relationships and strategies are expected from digitization:

- Growing integration of the value chain, full life-cycle management supported by a continuous data-thread.
- Shift from the transport of goods to the transmission of data, enabling distributed production, predictive maintenance, and optimization.
- Enhanced customization / collaborative design, trend back to customer proximity, shift from a consumer to a "prosumer" model.
- The emergence of new factory types: smart automated plants, customer-centric plants, e-plants.
- Development of new business models.
- Competitiveness goals mainly drive the digitization of industry; to reach this, the key challenges are related to security, safety, productivity, efficiency, acceptability, and adoption.

The IoT indicates a context consisting of billions of devices connected to the Internet during their normal operation and have the ability to communicate, perceive and have intelligence. These devices also have a physical/virtual identity, multi-modal attributes, and interfaces (Haller et al, 2008, Wann and Ranjan, 2015). It is expected that in the next future developments will be based on systems that contain semi-automated IoT applications. The IoT industry assumes that you can trust your data, but this usually does not respond to the truth because each placement could potentially be easily hacked.

---

5 Source: HIS – Market, as reported in Forbes –
Current changes in the Intelligent Transport System (ITS) and the adoption of a collaborative paradigm in information systems generate a continually evolving cybernetic space which is often associated with new vulnerabilities and defense requirements.

3.2.1 Evolution and Trends in IoT Security

The meteoric rise in the development of technologies over the internet has been boosted by increased internet access and improved speeds. The evolution in IoT is not only about guiding devices through mobile phones. The ever-evolving landscape has also created a chance for concepts such as ‘connected vehicle’, ‘the smart city’ and ‘Industrial IoT’. From workplace environments to public places and transport vehicles, connected gadgets and IoT are increasingly opening up new opportunities for the smart and communication between machines and humans. For any organization developing IoT applications, such new trends have the key chances of outperforming the competition and go on to be great organizations.

With such great speed of evolution through connected devices, environments and sensors, some of the latest trends have come in to change the entire landscape. They include:

A lot of investment in projects of IoT: Many organizations and individuals have made massive investments in project involving IoT and more is yet to come. Innovative applications of IoT are being developed and many other innovative connected devices being created as well.

Blockchain powered IoT: at the moment, IoT is run using a centralized architecture with all accessibility protocols and controls being controlled by just one responsible device. That creates vulnerabilities in IoT to breaches in data than it was the case before. Many cyber-attacks have been launched over the past few years and exposed all the weaknesses of IoT. However, all this can be solved with the use of a comprehensive distributed architecture for data that is in Blockchain. This is mainly because Blockchain offers a distributed database, making it accessible to every individual and that easily prevents breaches in data with authentic access to each user (Román-Castro, J. López & S. Gritzalis, 2018) [29].

Connected Healthcare: connected Healthcare is one of the greatest prospects perceived to benefit from the use of IoT. At the moment, there are a lot of efforts being directed towards creating IoT integrated solutions as healthcare gadgets along with smart billing systems are being developed.

3.2.2 A Framework for Threat-driven Cyber Security Verification of IoT Systems

There is an increased trend in the use of Industrial Control systems from monolithic to interconnected and distributed architectures, coming into an era of IIoT. One of the major issues that security features of such distributed systems of control are just empirically verified, at the time of development and after the system has been deployed.

IoT offers a practical and cheap paradigm that can be used by stakeholders in various industries to ensure interconnection of their product as well as create solutions that will facilitate large data amounts to be collected to track the performance of systems and also push updates for software. Nevertheless, because of the complexity of architectures of IoT and data sensitivity, security is turning out to be a great challenge for the infrastructures of IoT, in a way similar to safety.

Elimination and mitigation of attack after deployment of an online deployment of a system can be very costly since it might entail isolation of the subsystems that have been compromised or in worst case scenario, having to shut down the whole control system. This might in turn lead to harmful repercussions. A good trend in the analysis of security is application of formal methods in eradicating the possible threats at the early phases of design. The formal methods approach can be illustrated by the H2020 VESSEDIA project [47]. VESSEDIA promotes to design security by construction with a bottom-up approach, from the hardware/software to the system. If early detection of threats ensures cheaper mitigation and elimination, CHARIOT has adopted a systemic approach from the known attack surfaces to the software/hardware components. Both approaches are
complementary and compatible; Hence formal trusted components will be identified in CHARIOT as components with a lower attack surface.

3.2.3 Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking

IoT has enabled realization of a vision whereby several interconnected gadgets are deployed all over, from small inside people’s bodies to the most remote locations around the world. Considering the fact that IoT will be witnessed in every aspect of people’s lives, it is good to deal with the main IoT threats in security.

The conventional methods whereby security is applied as a patch and aftermath is not enough. The challenges that are likely to come in IoT will need a new vision of secure-by-design, whereby the threats are dealt with in a proactive way and IoT devices getting used to adapt dynamically to various threats. Thus, software-defined and machine learning networking will be vital to offering both intelligence and re-configurability to the devices of IoT.

3.2.4 IoT security tools as recommended by ENISA

According to ENISA, there are a number of items and tools that each organization must have for it to ensure IoT security. On that note, ENISA released a tool to be used online whose sole purpose will be guiding the operators of IoT as well as industries of Smart Infrastructure and IoT while assessing risks involved in different aspects. The tool offers a combination if the good features and practices of security which have been developed by ENISA for the past few years to attain security on IoT, smart infrastructure as well as Industry 4.0. The information offered through the tool for every thematic area is a reflection of the information contained in correspondence to reports of ENISA which have been released over the past. Through the tool, it is possible to come up with conclusions between different sectors of IoT because the same threat taxonomy used by ENISA has been applied whenever identifying the measures to security.

3.2.5 Alliance for the Internet of Things Innovation (AIOTI)

EU established in March 2015 an Alliance for the Internet of Things Innovation (AIOTI) with the purpose of supporting the development of the most dynamic and agile IoT ecosystem and industry in the world. This alliance, built in the framework of the IoT European Research Cluster (IERC), aims to spill over innovation across industries and business sectors of IoT transforming ideas into solutions and business models. The IERCs main purpose is to develop a common vision as well as the technologies for IoT in order to adopt and define standards. The AIOTI has successfully contributed to convergence and interoperability of IoT standards, as well as the Digitizing European Industry policy.

The AIOTI is divided into 4 groups: Management Board (MB), General Assembly (GA), Working Groups (WG), Steering Groups (SG) and thirteen WGs divided into four horizontal (H) and nine vertical (V) groups.

INLECOM, as the project coordinator, is a fully registered member of AIOTI at active in many WGs and intends to extrapolate many results of CHARIOT into the AIOTI working groups while at the same time discuss with various key-players from the working groups on recent trends, industrial requirements and research challenges. The CHARIOT WGs have been added below with descriptions on the intended scope of activities in each:

- **WGH 01: IoT Research**
  In this WG (horizontal), CHARIOT expects to discuss various IoT challenges that relate to the overall field of IoT connectivity, data security, privacy and safety as related to the CHARIOT scope. In this new technology will be investigated and analysed as input to CHARIOT, whereas CHARIOT solutions and technical competencies are presented and discussed to the group. Prioritization and structuring of threats related to IoT data security are also expected to be widely discussed.

- **WGH 03: IoT Standardisation**
In this WG (also horizontal), CHARIOT contributes in the area of IoT solutions and their standardization. Following the CHARIOT patenting and innovation steps, CHARIOT intends to make the first steps actively contribute to the AIOTI strategy for standardizing and approaching large standardization bodies for standards’ contributing. CHARIOT expects large visibility of its results through this group and large opportunities for public dissemination and update.

- **WGV 08: Smart cities**
  Although CHARIOT is not centrally focused on the smart cities concept, CHARIOT also participates to this working group to link its outcomes to the framework of smart cities, cyber security, industrial IoT as there are technical commonalities and similar challenges with the building and transport infrastructures that CHARIOT focuses on.

- **WGV 09: Smart Mobility**
  Mobility is a partial focal point of CHARIOT, through the TRENITALIA and ATHENS Airport use cases. This is being tackled in CHARIOT and its participation in AIOTI, in the fields of cyber security and industrial IoT devices. CHARIOT participates in this WG to disseminate research challenges and industrial IoT solutions or bottlenecks in the field but also expects to get updates from other industrial and research parties in the same fields as well as other technical uptakes in the framework of the industrial IoT.

- **WGV 13: Smart buildings and architecture**
  Smart buildings are also a focal point of CHARIOT, through the IBM living lab, that includes smart building infrastructures and a smart campus. Again here, CHARIOT brings recent outcomes into discussion as far as industrial IoT devices’ safety, security and privacy are concerned.

- **WG: Distributed Ledger Technologies**
  Distributed ledger technologies (DLT) and blockchain in particular, are major focal points in CHARIOT and parts of its technical solution. Recent challenges, new technologies and solutions are being discussed into this working group. CHARIOT is very active into this WG having a great competence and activity in the fields of DLT.

### 3.3 IoT in compliance with the GDPR and the NIS

Communications carried out through the many modern smart systems contain specific indications concerning the personal data of users. Also, the devices can communicate the position of individuals through geolocation and track the various activities they perform during regular use. The resulting risk is the possibility of storing this information, making it available and available to third parties interested in the value of the data itself which, if combined and aggregated, becomes a potential source of business. As is understandable it is necessary to pursue the achievement of a balance between the need to apply security rules and at the same time protect the privacy of the individual.

From May 25th, 2018, the European Data Protection Regulation (679/2016), known by the acronym GDPR (General Data Protection Regulation), was implemented by all EU Member States. The introduction of this regulation is aimed at the protection of individuals with particular attention to the processing of personal data and the free circulation of the same and regards both the public sector and the private sector.

The legislation will be applied and also extended to companies that reside outside the European Union and process data coming from the European territory. The regulation has become necessary in the face of technological development that has involved in an overwhelming way advanced technical solution capable of endangering the protection and security of personal data.

The GDPR Regulation has two primary objectives:

- Adaptation of Data Protection (data protection);
- Elimination of the application fragmentation of the legislation.
In the first point, the regulation aims to adapt data protection to the continuous and exponential technological progress that increasingly involves the transmission of personal data through the Internet connection which has simplified the transit of data between the Member States of the Union European and extra-European.

In the second point, the fundamental objective is to group under a single shared law all the European States, effectively eliminating the problem due to the presence of different standards applied in the European Union.

According to Regulation 679/2016, a strengthening of the rights of persons is envisaged, to which greater control will be provided on personal data. Furthermore, the consent to the processing of the same must be explicit in such a way as to constrain the data manager to formalize the request for treatment in an unequivocal manner. The individual may avail himself of the right to be forgotten, which will allow the data subject to request the deletion of personal data where there are no longer any legitimate reasons for their maintenance. The list above is of fundamental importance for achieving the objective of greater security of personal data protection.

In addition to the previously introduced GDPR Regulation, the European Directive for Network and Information Security (1148/2016) entered into force on 9 May 2018, known by the acronym NIS (Network and Information Security). The primary objectives of this directive are the following: - Achieving a high standard level of security of networks and information systems in all EU Member States; - Improve collaboration between them; - Create a culture of risk management; - Improve the sharing of information between public and private.

This directive is fundamental because it is part of a European strategy that aims to strengthen the so-called cybersecurity and IT resilience throughout the European Union. Telecommunications networks, services, and IT systems play a critical role in society and must be as reliable and secure as possible to allow the smooth running of economic and social activities.

Consequently, to all this, the Internet of Things systems will have to be developed according to criteria compatible with the objectives established by the European GDPR Regulation and the European NIS Directive. This is because they are devices that, due to their technical characteristics, turn out to be potential targets for direct or indirect cyberattacks. In the second case, the IoT systems could be used to carry cyber-attacks distributed to specific targets, substantially increasing the effectiveness of the damage caused.

3.3.1 Detecting Privacy Threats in IoT Neighborhoods

With the increased prominence and use of IoT, a surge in the use of wireless connectivity can be anticipated. Centrally managing such universal wireless communication will be very hard and so will be their control. There is need to integrate heterogeneous smart devices which need transparent connectivity to the internet. Particularly, standards of communication like Bluetooth, Zigbee, Wi-Fi as well as Bluetooth Low Energy are anticipated to offer such infrastructure as either traditional single hop access points or mesh networks. At the same time, the end users might not understand it well enough. Because of that, users and owners of physical space feel threatened to losing control over the digital environment that they operate (Siby Maiti, & Tippenhauer, 2017) [11].

One of the best ways to detect IoT threats in neighborhoods is through the use of an IoTScanner, a relatively new concept aimed at reducing threats by detecting them early enough. The scanner works through integrating a variety of radios to enable local inspection of the available wireless infrastructure and active/participating nodes. It then identifies the patterns of connection, enumerates the devices and offers valuable information for the end users and technical support. The use of an IoTScanner helps in investigation of metrics which might be applied in classifying devices as well as identifying the threats to privacy in neighborhoods to IoT (Siby Maiti, & Tippenhauer, 2017) [11].

3.4 IoT security

Cyber-threats which target the IoT infrastructure are aimed at destroying or harming some of their aspects like integrity, consistency, availability, integrity, privacy, and trust. Some of the most harmful cyber-threats aimed
Towards IoT include botnets, malware, and leakage of information, Denial of Service, Ransomware and physical manipulation.

Malware is malicious software which works through hijacking the functions of sensors and then spread them in the IoT infrastructure to gather operational intelligence. The botnet, on the other hand, entails a network of devices that are infected and spread through the world and controlled remotely from a single master, using a client-server architecture. On the other hand, ransomware attack by targeting facilities of data storage and then blocks the access to the data collected through encryption (Distefano, Merlino and Puliafito 2012). [16]

The issue of computer security has evolved over the last decade in a predominant IT (Information Technology) focusing first on the protection of computers, then on the protection of smartphones and tablets to currently focus on the protection of all Internet objects of Things (Figure 4) including vehicles, appliances, environmental sensors, technical and health equipment, wearable products such as bracelets, watches and many other devices connected via the Internet.

The growing number of interconnected and pervasive IoT devices present in the most varied daily activities draws attention to a very critical issue called cybersecurity (Cyber Security) which, compared to the classical concept of computer security, focuses more on "objects" interconnected the latest generation belonging to the Internet of Things ecosystem. Each of these smart devices can potentially be exposed to security problems ranging from the typical cyber-attack to the most subtle and veiled espionage (Steffen et al., 2017). [24]

Intruders can target many connected devices of daily use with consequent risk for privacy and physical security of people. Critical vulnerabilities have been highlighted by specific studies concerning not only the IoT devices connected but also the related management applications and not least the cloud services increasingly used by companies and users. Verizon has recently conducted a study that has made it possible to determine that most vulnerabilities have been identified by security researchers. These vulnerabilities allowed and still allow to take control of multiple devices among which we can highlight:

- Supply systems of a building;
- Water heating systems;
- Road traffic management systems;
- Devices for the administration of wind power plants;
- Systems for the management of automatic car washings.
There are also areas even more critical than those indicated above because they intervene in specific environments and public utility:

- Systems and devices used in healthcare;
- Transport networks, monitoring, and energy control;
- Devices used in industrial production;
- Application systems in the military field.

The analysis carried out by Gartner highlights the great innovation introduced by the IoT6: "The ability to change the state of the environment around connected objects and even their state." This implies the possibility that an IoT system, compromised by an attacker, modifies its "behavior" by altering the actions that had been configured initially. The system could dangerously change the management of the plant to which it refers, for example, could modify the surrounding environmental values to damage and danger of public health in a controlled environment as could be a chemical laboratory, a nuclear power plant, a refinery oil. Not only that, the device could irreparably change the trajectory of an aircraft or the course of a boat with potential risks to safety.

The enormous diffusion and density of vulnerable IoT devices provide cybercriminals with numerous opportunities to break the system and exposes the inexperienced to the real risk of becoming unknowingly infectious. These episodes are evidence of the fact that companies and consumers often ignore the basic principles of security applied to peripheral devices or networks, with consequences that may prove disastrous.

A very critical event occurred in October 2016 when the most massive DDoS attack7 (Distributed Denial of Service) was distributed to a significant service provider called Dyn using an IoT botnet (IoT device network). Remotely controlled by a hacker and composed of devices infected with specialized malware). The result of the cyber-attack through the Mirai malware was the extended interruption of the Internet service that hit and damaged significant entities such as Twitter, Guardian, Netflix, and CNN. The spread of malware was possible because each infected system continuously searched the Internet for vulnerable IoT devices using predefined utilities and passwords to access and propagate the infection (Steffen et al., 2017). [24]

3.5 IoT threats

The changing technological developments mean changes in the way people and organizations operate. It also means that malicious people have developed new ways to spread their harmful actions across the internet. With the emergence of the Internet of Things (IoT), the level of threats facing the organizations using it is on the rise. IoT is known to have a great effect on many daily aspects of personal lives and businesses. This happens in the case whereby the sensor measurements can be processed, measured as well as analyzed (Distefano, Merlino and Puliafito 2012)[16].

As mentioned in section 4.2 of [47], threats can be present in the perception layer, in the network layer and at the device level. These general threats will be developed in Section 3.7.

Since the mobility and limitation of many resources has been limited of late and the interconnection between devices and system, the vulnerabilities that could be used by intruders have increased greatly. The use of 6LoWPAN, which is made up of IPv6 and IEEE 802.15.4 weaknesses and brings in many other threats from both sides, therefore, aiming for different IoT network architecture layers. That starts from the network’s application layer, all the way through to the physical layers. The most usual threats against the network’s most vulnerable three layers include availability attacks or DoS attacks and unauthorized data access according to Ferdous et al., (2016). [17]

---

3.5.1 Threats on the perception layer

The layer entails the physical place where highly-distributed, resource constrained and heterogeneous IoT devices operate (Distefano, Merlino and Puliafito 2012) [24]. Considering the constrained type of the devices used and also given that objects are not resistant to tampering and the lack of sufficient security mechanisms in place, different attackers can easily gain access to the physical layer of devices with a motive of reprogramming their functionalities or damage them. Some technologies such as LTE, Wi-Fi, RFID as well as WiMax can be applied as input vectors to tamper the system. Some of the most common attacks have been discussed below:

3.5.1.1 Brute force attacks

The attacks are cryptanalytic in nature and can be applied in attempts to do data decryption on any form of data that has been encrypted for security purposes. In many cases, several smart home devices are quite susceptible to such types of attacks. That leaves home internet users connected with IoT very susceptible to attacks. Some of the most common attacks include:

i) Side-channel attacks
ii) Masquerading attacks

3.5.1.2 Side-channel attacks

According to the Cloud Security Alliance (2013) [21], the attacks are any forms of attacks done on the basis of the information obtained from physically implementing a certain cryptosystem. The attacks entail issues on evaluating leaked data and information that comes from physically implementing to recuperate the password or pin being used by the gadget under attack. That can be done by tracing power or timing the operations of the device’s inner operations, or even defective outputs that the device produces. Considering IoT’s openness, there are many types of side-channel attacks that can be initialized including fault induction attacks and timing attacks (Gope, and Hwang, 2015)[20].

3.5.1.3 Masquerading attacks

In this regard, the hacker hardens and attempts to utilize the identity of the node that has been authorized by the device in the given network. In most cases, such attacks are triggered and initiated at the network layer. Different other attacks, in this case, can include physical and tampering attacks, jamming attacks, collision attacks, eavesdropping and corrupting data (Gope, and Hwang, 2015) [20].

3.6 Network layer threats

In networks, the network layer contains the most intermediate layer applied in transmitting and aggregating any form of sensed data moving from the perception layer in a network, to the application layer in the same network. The movement of data is done through the use of existing wireless and wired networks of communication like Wi-Fi and LAN. Ferdous et al., (2016) [17] state that the network layer is IoT’s “backbone” of them. The network layer is a Wireless Sensor Network and it is a very popular IoT network I term of the capability to cover different huge areas of things and still be able to maintain enough energy for consumption. It is vital to point out that the network layer has to offer support to communication latency need, security, and bandwidth. All the same, the IoT features need to be pinpointed in all networks of 6LoWPAN, the layer is made up of two other smaller layers that make the 6LoWPAN quite susceptible to any form of routing attack. Different forms of attacks that target the two smaller layers within the layer are quite well-known (Gope, and Hwang, 2015) [20].

3.6.1 Attacks on the adaptation layer

The adaptation layer concentrates the main attacks. Its main function is the translation of the packets between the internet and 6LoWPAN network. Thus, the layer is susceptible to various attacks related to 6LoWPAN including:

i) Authentication attacks
3.6.1 Authentication attacks

The major weakness of 6LoWPAN is that it has no mechanism that can be used in authenticating its nodes before they are allowed to join and be part of the network. Thus, it is quite clear that any harmful nodes can easily enter into the network and activate other attacks from within the network, which is a very dangerous thing to any IoT applications. There have been proposals for several protocols of authentication but only in theory and literature and have not seen their implementation taken seriously. Despite all the proposed protocols, there is still very high danger looming through threats and attacks to IoT applications and devices (Gope, and Hwang, 2015). [20]

3.6.1.2 Fragmentation attacks

In many cases, the border router is a node wired and is well-protected through very strong security mechanisms. Nevertheless, the progress of reassembling and packet fragmentation will still be susceptible to some extent. In such attacks, the hacker can reconstruct or change the fields of fragmentation of the packet such as the datagram offset. Such attacks are dangerous and can lead to considerable damages to a certain node, like the overflow of reassembling buffer due to re-sequencing of packets, exhaustion of resources or even shutting down and restarting of the device or application. At the same time, there is no existing technique to authenticate and at the receiver end to check if the fragment received is not duplicated or spoofed as the attacker could insert his personal fragments in the chain of fragmentation (Liu, Xiao, and Chen, 2012). [19]

3.6.1.3 Confidentiality attacks

In a well-secured network, it is expected that only the authorized nodes can gain access to, overview and control data within the network. Offering sufficient confidentiality in 6LoWPAN can assist in abating different attacks like eavesdropping, spoofing attacks and MITM. When it comes to authentication. Managing identities forms part of a very aspect to make sure that there is sufficient confidentiality. All the same, cryptography is taken as one of the major techniques used in dealing with authentication and confidentiality problems. It is also important to note that IPSec offers layer security on the network on the basis of end-to-end through enabling the encryption and authentication of interchanged packets of IP (Liu, Xiao, and Chen, 2012). [19]

3.7 IoT security

The issue of computer security has evolved over the last decade in a predominant IT (Information Technology) focusing first on the protection of computers, then on the protection of smartphones and tablets to currently focus on the protection of all Internet objects of Things (Figure 4) including vehicles, appliances, environmental sensors, technical and health equipment, wearable products such as bracelets, watches and many other devices connected via the Internet.
The growing number of interconnected and pervasive IoT devices present in the most varied daily activities draws attention to a very critical issue called cybersecurity (Cyber Security) which, compared to the classical concept of computer security, focuses more on "objects" interconnected the latest generation belonging to the Internet of Things ecosystem. Each of these smart devices can potentially be exposed to security problems ranging from the typical cyber-attack to the most subtle and veiled espionage. These types of attack can be used by hackers to condition certain production processes heavily or to detect confidential information and the whole "simply" appropriating the control, for example, of a mechanical thermostat placed inside a corporate plant or a smart TV which usually has a camera and an integrated microphone. As it is obvious to infer, the greater the number of "objects" interconnected to the Internet domain, the higher the risk associated with a possible violation of the system.

Intruders can target many connected devices of daily use with consequent risk for privacy and physical security of people. Critical vulnerabilities have been highlighted by specific studies concerning not only the IoT devices connected but also the related management applications and not least the cloud services increasingly used by companies and users. Verizon\(^8\) has recently conducted a study that shows that most existing vulnerabilities have soon been identified by security researchers. These vulnerabilities allowed and still allow to take control of multiple devices among which we can highlight:

- Supply systems of a building;
- Water heating systems;

There are also areas even more critical than those indicated above because they intervene in specific environments and public utility:

- Systems and devices used in healthcare;
- Transport networks, monitoring, and energy control;
- Devices used in industrial production;
- Application systems in the military field.

Cybersecurity has become a very well-known topic in the Internet of Things field because the IoT paradigm has changed the approach to information security. Cybersecurity in IoT inherits from security of the Web, so concepts developed in the Open Web Application Security Project [48] directly applies. The attack surfaces defined in OWASP\(^9\) will be developed for the transportation (Section 3.8) and smart building sectors (Section 3.9). The analysis carried out by Gartner highlights the great innovation introduced by the IoT\(^10\): "The ability to change the state of the environment around connected objects and even their state."

This implies the possibility that an IoT system, compromised by an attacker, modifies its "behavior" by altering the actions that had been configured initially. The system could dangerously change the management of the plant to which it refers, for example, could modify the surrounding environmental values to damage and danger of public health in a controlled environment as could be a chemical laboratory, a nuclear power plant, a refinery oil. Not only that, the device could irreparably change the trajectory of an aircraft or the course of a boat with potential risks to safety. The enormous diffusion and density of vulnerable IoT devices provide cybercriminals with numerous opportunities to break the system and exposes the inexperienced to the real risk of becoming unknowingly infectious. These episodes are evidence of the fact that companies and consumers often ignore the basic principles of security applied to peripheral devices or networks, with consequences that may prove disastrous.

A very critical event occurred in October 2016 when the most massive DDoS attack\(^11\) (Distributed Denial of Service) was distributed to a significant service provider called Dyn using an IoT botnet (IoT device network). Remotely controlled by a hacker and composed of devices infected with specialized malware). The result of the cyber-attack through the Mirai malware was the extended interruption of the Internet service that hit and damaged significant entities such as Twitter, Guardian, Netflix, and CNN. The spread of malware was possible because each infected system continuously searched the Internet for vulnerable IoT devices using predefined utilities and passwords to access and propagate the infection.

The danger that runs is not only related to the possible violation of the security of the devices by malicious hackers but is also represented by the real possibility of circumventing the protection of the data. Companies that produce and distribute IoT devices may also use them to improperly acquire personal and confidential consumer information that is essential for obtaining the so-called profiling used for commercial purposes. In this case, the best defense for the consumer is not technological but the knowledge of the policies of the producer regarding the processing of data and the sharing of acquired information.

\(^9\) https://www.owasp.org/index.php/IoT_Attack_Surface_Areas
3.7.1 General threats

All IT infrastructures and devices have common general threats that can generate a vulnerability or act as a vector.

![General threats](image)

The table below contains the general threats that could affect an IT infrastructure like railways, airports, and smart buildings. These threats can be divided into 3 groups: malicious actions, human errors, and system failures. The first group related to the malicious actions and methods updates some general threats identified by Microsoft in the STRIDE Thread Model [49].

<table>
<thead>
<tr>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of Service</td>
<td>Typically, IoT devices communicate through radio access technologies in the physical layer. The wireless link is very sensitive to Denial of Service (DoS) attacks, which may take their form in signal distortion or jamming. DoS attacks may compromise system availability. While spread spectrum techniques can be used against wireless jamming,</td>
</tr>
<tr>
<td>Exploitation of software vulnerabilities</td>
<td>Malware, software vulnerabilities have very adverse implications in security. There are so many devices connected through IoT than in the previous years. That is a great advantage to the hackers since they make sure that they utilize machines like cameras and printers that were never created with protection from strong attacks. That has led to several organizations restructuring their plans to deal with the latest vulnerabilities. The attackers use the vulnerabilities found in such software and penetrate to the firm networks, affecting all the IoT connected devices. The vendors of software know that such vulnerabilities exist, thus the reason why they frequently release updates on their software to counter them (Atzori et al., 2010) [37].</td>
</tr>
<tr>
<td>Misuse of authority/authorization</td>
<td>The increased interconnection between devices in IoT has led to a great demand for strong responses in security, including storing sensitive information about some companies and individuals, data on financial transactions, marketing, and product development. That has prompted companies to ensure that they restrict the number of people with access to such information. The misuse of authority delegated to individuals leads to access and sharing and even wrong use of</td>
</tr>
<tr>
<td><strong>Network/Interception attacks</strong></td>
<td>Information for individual gains instead of the company’s interest (La Diega and Walden, 2016) [38].</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Social attacks</strong></td>
<td>The IoT networking layer suffers all sorts of security threats that are known within the computer networks community. There are specialized attacks for Wireless Sensor Networks (WSN), the aggregation network (i.e. Gateway or Link layer), and the transport network between aggregation points and the cloud and its applications [46].</td>
</tr>
<tr>
<td><strong>Social attacks</strong></td>
<td>Social attacks entail the manipulation of people with the aim of having them release or offer confidential information. With the use of IoT, the risks of social attacks have increased since people have their devices interconnected, thus easy access to information. The forms of information being searched by the attackers can be different, but in most cases where there are individual victims, the attackers look for their banking information. At the same time, they could be trying to install a Trojan horse in the computer that will keep them updated on the passwords and other information stored in the computer or system (La Diega and Walden, 2016) [38].</td>
</tr>
<tr>
<td><strong>Tampering</strong></td>
<td>Tampering is an action when via an attack, physical modifications on the device or on the communication link can be performed. Hardware elements can be accessed and identity the stolen (or replaced one), which can violate confidentiality, availability and integrity objectives. Using of tamper-resistant packaging is one way to the correct direction to avoid this, but it can be too expensive solution, considering cheap low-power sensors or consumer devices which are the main drivers of IoT. Tampering the communication link can be performed on disconnecting or changing the physical link (Denial-of-Service attack case) or changing the transmitted data (Man-in-the-Middle case attack).</td>
</tr>
<tr>
<td><strong>Breach of Physical access controls</strong></td>
<td>The breach of physical access controls in a system or organization comes from the people within the company. Even though there are strong measures in place at a data center, the greatest security risk emanates from inside the organization. Despite some individuals accessing systems with malicious plans, some of the security breaches are accidental making up for 9-18% of all breaches. Many standalone traditional systems can only be breached through physical access, and interconnected devices are affected after such attacks. Thus, the breach of physical access controls is a great concern that should be dealt with through ensuring physical security like lock-ups to servers and rooms with delicate information access (Khan &amp; Khan, 2012) [39].</td>
</tr>
<tr>
<td><strong>Malicious software on IT assets</strong></td>
<td>Malicious software on IT assets This threat comes from the download of malicious software without the knowledge of users, integrating them with the existing IT software and assets. Research shows that 83% of software downloaded by individuals and companies cannot be classified or verified to be legitimate or malware. That leaves room for attackers to come in and take advantage of unsuspecting users. Some of the software act as Trojan, pretending to be doing some function, while they are actually collecting information from the IT assets and sending it to the attackers. Buying original software from well-known vendors can help minimize risk and threat (Wu, 2012) [40].</td>
</tr>
</tbody>
</table>

Then another important threat is related to human errors (mainly done involuntarily) that remain one of the most important aspects that impose to invest in training to improve awareness and knowledge.
Third party failures it means for example service provided by Internet-based smart technologies can rely on cloud service providers or the maintenance services that is not correctly carried out and planned could provoke damage. After understanding the different general threats, it is also vital to briefly introduce and understand the threats that face our SPS (Security, Privacy and Safety). With regard to security, it can be grouped in terms of the CIA triad:

a) Confidentiality  
b) Availability  
c) Integrity.

According to Sicari et al. (2015) [23], threats to safety can be taken as being similar to those of privacy and security. The threats to safety come from flaws in aspects like maintenance, production, design, or even deployment of various IoT projects. The other issues that cause safety flaws include infrastructure failures and unprecedented changes to the interaction between various objects of IoT. Lastly, the objects of IoT are not frequently offered with updates in software, making them weaker and vulnerable to leaks in security all the time.

Such issues can come at a time the personal data of different clients is by insurance firms for price discrimination or even used by the police in determining the profile of an individual. Authorities and organizations can also use IoT to frequently monitor the character of individuals, which can be considered a violation of privacy and make people change their behavior.

Additionally, data could be utilized to accomplish different purposes and tasks than the initial intention when the data collection was being done (normally referred to as a function creep) (Sundarkumar et al., 2015) [14]. Encrypting data is not a permanent solution to the above issues since encrypted data can in many cases be decrypted through a combination of various sets of data.

As stated above, the threats to safety are not intentional. Just the same as the privacy threats and security threats, the threats to safety come from flaws like maintenance, production, design, or even deployment of various IoT projects. The other aspects that lead to problems in safety include infrastructure failures, unpredictable changes to system operations because of interfacing between various objects of IoT (Sundarkumar et al., 2015) [14].

The SPS threats have to be taken into consideration at the time of the entire IoT system lifecycle (pre-, during and post-deployment). In the pre-deployment stage, the threats to SPS need to be applied while making IoT system designs. That is normally called Safety design, privacy and security. When applied to gather and store personal data, the devices of IoT should be changed to be SPS-friendly, for example, through the addition of features like a button to offer "Delete" option and also an option to leave the system when one needs. At the time of deployment and after post-deployment, there should make efforts to ensure that the devices of IoT are accountable and transparent enough (Sadeghi, Wachsmann, and Waidner, 2015) [22].

The framework proposes the deployment of SPS by design to minimize SPS threats, and identifies four obstacles in realizing this: 1) IoT complexity, 2) lack of awareness, 3) lack of incentives, and 4) lack of monitoring and enforcement. The framework also shows how these obstacles, and solution directions to overcome them, are related to each other in that addressing one impacts the other one(s) and vice versa. The conclusion that can be drawn from this work is that there is no one-size-fits-all measure to address SPS threats. Instead, a variety of measures is needed to create an SPS-friendly IoT.

3.7.2 A deep Recurrent Neural Network based approach for Internet of Things malware threat hunting

As time goes by, the prominence of IoT is increasing and it is being applied in various industries for different purposes. The fact that it brings together many devices through a connection network makes it a prime target to attacks. Reports by Kaspersky 2016 Lab indicate that many of the devices that were examined were not secure because they either had a default password or vulnerabilities that are unpatched. That is to say, compromising the devices can be done easily through the use of malware like Mirai and Hajime.
The current learning-based approaches towards dealing with malware have placed much of their focus on patterns of energy consumption as well as OpCode. This looks quite unsurprising as OpCodes and system calls are the two main aspects of malware hunting. Over the past few years, there has also been the use of deep learning techniques to analyze malware and detect them.

3.7.3 Hardware and software limits of IoT objects

The main problem associated with IoT devices is the level of security which is very low because they are interconnected objects through insecure channels and transmission protocols. This flaw makes the systems belonging to the Internet of Things ecosystem a reasonably straightforward target for cybercriminals.

IoT devices are mainly divided into embedded systems, sensors and actuators. For this reason, the hardware of which they are composed turns out to be very variable and limited. IoT systems are typically small in size, equipped with operating systems associated with processors (CPUs) and memories with essential performance and features. Many devices are designed with the aim of being inexpensive, effectively renouncing the use of performance components. They also employ simple network connection interfaces that are not suitable for supporting integrated security protocols. The same consideration can be made regarding the software that the devices are equipped with. Also, intending to contain costs, it appears to be characterized by essential and specific functions, resulting in little or no adequate security. An illustrative example is the list of hardware features typical of the simplest IoT devices:

- Flash Memory: 196 kB;
- SRAM: 24 Kb;
- Clock Speed: 32 MHz

From the information above, it can be understood how a simple IoT device, used in a specific field such as temperature or pressure monitoring, is characterized by minimum components that are not able to guarantee the necessary predisposition to the development of safety. Analyzing the chapter on IoT security written by Verizon, we can deduce that the increase in each bit of memory and the increase in processing capacity on devices considerably increases production costs. The economic burden also doubles for the development of software which must be able to support the functionality necessary for system security. According to the same report conducted by Verizon, it is clear that the priority for a developer is addressed to the so-called Time To Market (TTM) or the time between the conception of a product to its actual marketing, as this time interval is significant and critical in order to compete competitively in a rapidly expanding technology market. For what above mentioned it can be understood that it is unthinkable that a developer includes at the design stage an SSL encryption system on an 8-bit microcontroller which is designed, for example, to interact with the lighting system and turn on and off lights under certain environmental conditions or that a system administrator regularly distributes patches or updates for the firmware integrated into the IoT device.

3.7.4 The weak link of IoT devices: "the Firmware"

In today's context, smart devices belonging to the Internet of Things ecosystem are increasingly present. However, the technology companies producing these evolved systems tend to underestimate the potential risks to which they are exposed since the latter are connected continuously to the Internet. The greatest danger is caused by superficial behavior conducted by the manufacturers themselves who are oriented to release the firmware updates with an excessively low frequency and sometimes, fortunately only in extreme cases, and the updates are not indeed released. This superficial behavior allows hackers to take advantage of a huge amount of potentially vulnerable devices.

The firmware, an expression consisting of the terms firm (stable) and ware (component), is a program present within each electronic component. Its fundamental role is to start the functioning of the same component.

---

allowing it to communicate with further integrals or cards present in the device in which they are installed. How much shared allows us to determine the importance it has to release firmware updates otherwise it may happen that an IoT device, updated and therefore safe at the time of purchase, becomes dangerous for the consumer when cybercriminals discover a vulnerability of the system. This event usually occurs when the manufacturer decides to allocate its internal resources to the production of a new product to be proposed on the market, effectively stopping the development and release of updated firmware versions for existing and already marketed products. Consequently, the most significant risk for the consumer is that of finding obsolete and potentially dangerous hardware for security. Not always the failure to update the software is attributable to the choices of the manufacturer; also, the end user plays an active and harmful role in this sense. Often, due to personal inexperience or lack of knowledge of the technological product used, the consumer does not check for updates and does not install the firmware versions released and recommended by the manufacturer. To overcome this specific situation and reduce as much as possible the risks related to the security of software platforms, the most advanced devices, including computers, are programmed to perform updates automatically without the need for customer intervention the final. Unfortunately, protecting and updating the security features of the systems belonging to the Internet of Things world is not, and for this reason, it will not be trivial to implement solutions oriented to this purpose. Companies' commitment to firmware security is increasing, but the economic resources required to start new investments in this specific field of information security are the main obstacle to face.

To achieve a high level of security for IoT devices, it is necessary to introduce a shared standard that can guarantee a common methodology during the design, development and above all the issue of updates. In this regard, the company ARM Holdings\textsuperscript{13}, a company specializing in the technological development and known on the market to be the manufacturer of processors based on the ARM architecture, is engaged in the launch of the process that will lead to the approval of a standard for the Internet of Things. The company ARM Holdings has already released a formal document called "IoT Firmware Update Architecture"\textsuperscript{14} demonstrating the commitment placed in the firmware security field. The paper presents a set of rules that all smart system manufacturers should follow during the implementation steps of the firmware update mechanism of the implemented devices. The most necessary prescriptions contained in the document are the following: - Use of end-to-end encryption; - Prevention of cyber-attacks; - Facilitate the distribution of updates with different modes (USB, Bluetooth, Wi-Fi, etc.); - Maintaining the same file formats for the firmware. The method presented is an excellent starting point for the achievement of a concrete standard. However, the document shows some aspects that need to be deepened and improved to make it valid in all its parts. Achieving the goal of introducing a constructive standard for smart systems would be able to mitigate the numerous security flaws in the connected devices. The updating of the firmware of the devices is a critical operation since for some years there are search engines specialized in identifying the services exposed by devices connected to the Internet. A very well-known search engine is shodan.io through which specific searches can be made to obtain a list of smart systems belonging to the vulnerable Internet of Things ecosystem. This portal can be used by anyone therefore also from any hackers willing to find targets to be targeted by cyber-attacks. However, to avoid facilitating the task for the bad guys, registration is scheduled on the website, and in any case, only a few information is provided free of charge. Fortunately, the portal can also be used consciously by company personnel to monitor the level of security of their business devices. Thanks to this web service it is possible to carry out targeted scans to detect vulnerabilities and intervene promptly to secure your work environment.

The problem of security is even more evident if we consider that IoT devices are already on the market already vulnerable and become useful targets for cybercriminals from the first connection to the Internet. As highlighted

\textsuperscript{13} https://www.arm.com/
\textsuperscript{14} https://tools.ietf.org/id/draft-moran-suit-architecture-01.html
in an editorial called "Cyber Security News" published by the General Department of the General Staff of the Air Force\textsuperscript{15}, it is clear that:

- IoT devices are often sold with default credentials or known security holes.
- Millions of unsafe devices are already connected, and millions of new ones are added every day.
- IoT devices are connected to the Internet 24 hours a day, so they are available for an attack at any time.
- IoT devices are often connected to high-speed Internet connections allowing the spread of extended attacks.
- IoT devices are extremely useful to use as anonymous proxies.
- The technology and knowledge to detect, violate and use IoT devices, and then use them in cyber-attacks, have been made public and are currently used in various services.

3.7.5 Taxonomy of Firmware Trojans in Smart Grid Device as examples

Electric grid modernization and the use of advanced information technology techniques has opened up several opportunities to enhance better communication as well power system efficiency. Whereas the environment for smart grid provides vital reliability and economic benefits, it has also disclosed a wide range of issues with regard to cyber-attacks. The attacks have always been made embedded on devices that are microprocessor-based such as Stuxnet and have clearly shown that the control equipment firmware can be vulnerable towards breaches in security and create substantial damage to the given system (Konstantinou et al., 2016) [53].

Besides the fact that there are many studies that have been conducted on the security of power systems, there are many researchers who do not have the right benchmarks and classes of taxonomy to manage and create enough mitigation and detection strategies against such attacks. Thus, Konstantinou et al. (2016) [53] suggest a taxonomy for firmware Trojans and create firmware Trojan benchmark to be used for future research.

Some of the latest smart grid embedded gadgets include smart meters, IEDs (Intelligent Electronic Devices), PMUs (Phasor Measurement Units) and PLCs (Programmable Logic Controllers). All the gadgets are integrated into the grid as demonstrated in the image below. Typically, they entail designs that are microprocessor-based. Because of that, they are exposed to the same weaknesses that face microcontrollers and processors (Konstantinou et al., 2016) [53].

![Firmware Trojans in Smart Grid Devices](image)

Figure 7 - The taxonomy of firmware Trojans in smart grid gadgets.

\textsuperscript{15} https://www.af.mil/
3.7.6 Impact of Firmware Modification Attacks on Power Systems Field Devices

The combination of physical and cyber components has put cyber-security in the limelight in the power industry. Communications, sensing as well as technologies of intelligent control are being applied in the field devices, bringing a change to the conventional structure of systems for power and changing the infrastructure of power into a more interactive, controllable and dynamic system. Because of that, the created smart grid environment enhances the probability of being attacked maliciously. Control and monitoring decision apparatus like protection relays based on micro-processors provide the easiest weak point for attacking to hackers (Konstantinou, 2015) [45].

Ensuring that electric power grids (based on a wide variety relay status signals) function properly is vital towards maintaining secure and stable operations for the systems. The main function played by the relays in a power system’s operation is preventing or limiting the damage caused by the faults and overloads, therefore reducing their impact on the other part of the system. This is attained through the separation of the system into protective areas with circuit breakers to separate the other part of the system (Konstantinou, 2015) [45].

3.7.7 Critical infrastructure protection

At the Global level, all nations defined a list of Critical Infrastructure (and related services) that must be considered strategic and need to respect determinates rules. The US level issued the first approach during the Clinton Administration in the 90s, then followed by Canada (in February 2001, Canada initiated OCIPEP (Office of Critical Infrastructure Protection and Emergency Preparedness) within the National Defense organizational structure Department and Europe. The European Commission adopted a Green Paper on a European program for Critical Infrastructure Protection, and in 2008, the European Council issued the Directive 2008/114/EC. The main characteristics essential for evaluating Critical Infrastructure are resilience, absorbability, adaptability, robustness, structural robustness, precautionary robustness, susceptibility, preparedness, recoverability, responsiveness, reparability, redundancy, overload capacity, safety, and security. These characteristics apply to each type of Critical Infrastructure (e.g., transport) and for any level of detail selected for the Critical Infrastructure analysis (system, subsystem, component). To exact description of Critical infrastructure characteristics and assessment them through parameters was possible, the set of features must be internally consistent.
The Critical Infrastructure characteristic's tree shows the relationship between the Critical infrastructure characteristics by the logic gates AND. Resilience is a series of processes form an umbrella attribute which is formed by partial features. Resilience so can be divided down to the basic indivisible features. These essential characteristics can be evaluated through one or several parameters. Furthermore, the components at a higher level can be assessed through appropriate settings. Based on the Critical Infrastructure characteristic tree we can identify two types of interrelations among the Critical Infrastructure: additive and non-additive. The additive interrelation is valid for the Critical Infrastructure characteristics. The resilience can be fully described as the sum of the individual features. However, it is not possible to obtain the value of the resilience parameter as a sum of values of parameters of partial Critical Infrastructure characteristics. This non-additive must be respected when tools and methods of Critical Infrastructure assessment are selected.

Another important aspect is related to the Critical Infrastructures interdependencies that usually fall into four principal classes:

- **Physical**: operating one infrastructure is dependent on the other one’s real output.
- **Cyber**: The level at which the information transmitted via the infrastructure can be depended upon.
- **Geographic**: The level of depending on the local environmental effects which instantaneously impacts several infrastructures.
- **Logical**: Any dependency not grouped as geographic, cyber or physical. A comprehensive analysis of all types of interdependencies is challenging and requires extensive modeling efforts to provide a better understanding of CI systems.

In this framework railways and airports are considered as Critical Infrastructures. The table below provides an overview of the legal framework adopted at EU and US level that identify the role of critical infrastructures and their management including at general standards.

**Table 3 - Regulations Overview**

<table>
<thead>
<tr>
<th><strong>EU Regulations</strong></th>
<th><strong>US Regulations</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The cyber-security strategy for the EU (2013)</td>
<td>NIST 800-30</td>
</tr>
<tr>
<td>European Agenda on security (2015)</td>
<td>US WH EO 13636</td>
</tr>
<tr>
<td>CPPP Initiative (2015)</td>
<td></td>
</tr>
<tr>
<td>NIS Directive (2016)</td>
<td></td>
</tr>
</tbody>
</table>
Concerning the ENISA report on past incidents of cyber-attacks and ENISA's role in cyber-security, it is known that cyber threats are a growing menace, spreading to all industry sectors that are relying on ICT systems. Such incidents could be reasonable reduced by policies that neutralize the various market failures acting as a barrier to optimize private investment in cyber-security from public and private institutions, where an efficient cooperation and coordination in the real-world experiences highlight the economic need for coordinated cyber defense (Brynjolfsson and Oh, 2012) to lower expenses on security for all partners involved.

The EU is working towards eliminating the cybersecurity threats. Although the issues of cyber-security are on the rise, the EU MS have all the policies and tools needed to deal with the issue of Cyber-security. All member states in the EU should come together and work towards achieving the common goal. Among the solutions proposed by NIS include all the members of the EU to bring in and implement independent national strategies on the security of information systems and networks. ENISA has the responsibility of implementing the directive provided by NIS. At the same time, ENISA is expected to support the member nations in creating their own National strategies and ensuring that they are properly implemented. When implementing the policies, ENISA should ensure that the cyber-security policies focus on both the past experiences and the possible future events over the same (ENISA, 2017).

### 3.7.8 Classification and comparison of critical infrastructure protection tools

Risk and interdependence analyses can be quite involving to compute, but it can also lead to important results which will enhance the assessment of risks and provide alternatives to mitigating risks. However, many of the techniques and tools are just forgotten and left without support as soon as the projects that created them are terminated. There is needs to focus more research towards dealing with the mitigation of risks through qualitative instead of quantitative analysis.

### 3.7.9 A process-based dependency risk analysis methodology for critical infrastructures

The common analysis of risks for critical infrastructures entails analysis of dependency whenever the risk assessment refers to a cross critical infrastructure analysis. It is not considered to be part of the risk analysis for the operators. However, it is dependent on the sector and the level of maturity of the critical infrastructure. Nevertheless, related research in the area has shown that analysis of the dependencies of critical analysis can create important results when looking into the possible threats facing the system. The issues grow and become hard to control whenever making attempts to have a time-based and dynamic dependency risk analysis. Mapping the dependencies in assets in every business transaction will enable proper calculation of the dependency chains and make good use of them in checking the cumulative and cascading risk of possible threats on the business processes (George et al., 2017).

### 3.7.10 Standards

There is a lot of guidance created by the NIST (National Institute of Standards and Technology) and any organization can easily use such guidance. For instance, the SP (Special Publication) for NIST was created for different information systems and it is very efficient in the creation of a plan for security in any firm (Quashie & Tweneboah-Koduah, 2016) [30]. The other standards of NIST offer more guidance in details. For instance, NIST SP 800-82 offers guidance for security on specific systems of control, NIST SP 800-50 guides on the creation of IT training and guidance for certain incidences while NIST SP 800-61 guides towards the creation of incident response plans and management. The IEC (International Electrotechnical Commission) along with ISA (International Society of Automation) have created several standards of ISA/IEC-62443 which help in defining the procedures used to implement secure systems of control and the directions are applicable to system

---

16 Sectors relying on ICT are the most vulnerable to attacks
integrators, end-users, manufacturers of control systems and also the personnel dealing with system security issues. The Railway system is a very important infrastructure at both the international and national levels. For instance, the EU, Germany, and USA have been able to successfully point out the issue. They have in turn created well-defined policies to help in supporting the implementation of IT standards of security that are sector-specific and industry defined (GAO, Government Accountability Office, 2015) [26].

One of the major ways to close down on the gap existing between the standards for information security for railways and general systems has been offered by the European Commission regulation (Roman, Zhou & Lopez, 2013). That can be found in regulation number 402/2013 which deals with the most common methods of safety. The regulations point out three major techniques to help show that there is sufficient safety in railway systems:

a) Through following the available standards and rules (applying the codes of practice).
b) Through analyzing in a similar way, by displaying that the selected railway system can equally serve as a used and proven one.
c) Through explicitly analyzing risks, whereby the risks are clearly assessed and demonstrated as being acceptable.

It is assumed that from the process perspective, security can be regarded just as safety is, thus indicating that the threats might be treated as specific threats. That is done through the use of an approach under mutual criteria or in the case of railway systems, there can be the use of ISA99/IEC62443. However, there would be a need for customization because of the different requirements in safety and conditions for application. Through this method, there is approval of a code of practice in other sections of technology, offering enough level of security that is applicable to railway systems. That helps in making sure that there is enough security. Nevertheless, using ISO/IEC 15408 offers a criteria upon which evaluation can be done for security in IT, which is commonly known as a “common criteria”. The standard is exclusively centered on the use of information systems are is not directly related to safety systems (Boyes, 2013) [27].

There are efforts by Shift2Rail (a program aimed at uniting the major stakeholders in Europe to attain one railway area in Europe) to define the way that various cyber-security aspects need to be used in the railway sector. Thus, Shift2Rail has evaluated the standards that are applicable and chose the IEC 62443 series because of the following aspects:

- The group of standards is devoted to IACS.
- It deals with the product and system lifecycles.
- It deals with the processes of security risk assessment.
- It describes the levels of security on the basis of functional requirements of security.
- It is applied by other important infrastructures.

The main challenge is identifying which of the standards can be applied in the railway systems. That is what is being done at Shift2Rail17, whereby the stakeholders are looking at the standards in the industry, meaning that IEC 62443 will be applied in the railway system (Gubbi et al., 2013) [28]. The standards exist, only their adoption is what remains (Quashie & Tweneboah-Koduah, 2016) [30].

Considering the fact that IEC 62443 is coming up as a center for the group of standards18 for the railway system, with some reiterating that IEC 62443 is a standard for cybersecurity to approach the use of IoT in railway systems.

The group of standards entails the three main stakeholders in protecting production firms against being attacked through different cyber threats. The system integrators, shareholders and suppliers of products are involved. The main notion of IEC 62443 is that it needs a group of synchronized steps to be taken, a technique that is mainly considered as defense-in-depth. The common adoption of IEC 62443 is can be seen in the DIN VDE V

17 https://shift2rail.org/
18 A Railway Group Standard (RGS) is a standard that defines what must be done to achieve technical compatibility on the GB mainline network. https://www.rssb.co.uk/
3.7.11 From SCADA to cloud computing and IoT in the supply chains

The first use of SCADA (supervisory control and data acquisition) started in the ’60s to monitor and control part of the Control Systems family, that includes ICS (Industrial control system), PCS (process control system), DCS (Distributed control systems) etc. These systems required the interaction with humans but with the technological development became automated reducing the involvement of human control. SCADA Systems are mainly used to monitor and control a plant in industries in many different sectors like energy, transport, waste control, etc. With the new paradigms introduced by the adoption of Cloud Computing and Internet of Things (IoT) that are considered as the two fundamental technologies of the "Future Internet" concept, various IoT systems are designed and implemented following to the IoT domain requirements, without consideration issues of openness, scalability, interoperability, and use case independence. This approach leaves potential open risks related to the information security and privacy, data protection and safety, that need to be considered as single issues. The costs of cyber-attacks in such settings is estimated to reach over 2 trillion USD in the next coming years, and today IoT is just beginning to emerge with vulnerabilities and exploits reported at a steady pace and showing that information security and operational security are already the most important challenges to be faced. Since the IoT ecosystem can often have critical components, will unavoidably be a target for attacks and espionage, denial-of-service along with many other types of cyber-attacks (Chiappetta, 2017) [6]. IoT Industry 4.0 and interconnected devices along with the infrastructures are expected to be a standard in the near future, introducing disruptive changes as we move from the era of personal devices to an era where the is a promotion of large-scale interconnected (and highly integrated) devices and platforms (supporting real-time monitoring, autonomous adaption, instrumentation, actuation, control logic, etc.).

Since the beginning of the 1980s when Anderson [13] published his work about network security monitoring a large number of researches have been conducted around intrusion detection. In the below Table 3 are listed the main cyber-security attacks on transports that shows how are continually growing along with a description on typologies, methodologies, and damages that were reported.

<table>
<thead>
<tr>
<th>Location of attack</th>
<th>Typology</th>
<th>Methodology</th>
<th>Damage done</th>
</tr>
</thead>
<tbody>
<tr>
<td>Worcester Airport (1997)</td>
<td>phishing</td>
<td>The hacker managed to disable a key telephone company computer servicing at the Worcester Airport. In doing this, he sent a series of commands from his personal computer and disabled key services at the FAA control tower, spanning six hours long.</td>
<td>He disabled the key services at the FAA control tower and crippled the airport for a total of six hours. In the course of the attack, services at the airport stood still and did not move, leading to massive losses and confusion.</td>
</tr>
</tbody>
</table>
| Port of Houston (2001)   | Denial of service attack  | A teenager from Britain is said to have brought to knees all internet systems and services of a major port in the US, in an attempt to revenge on a fellow user of IRC. In doing that, he directed an attack to a fellow user in the chatroom, with the attack managing to slow down the systems at the port through a DoS. He took out the network connection of the fellow chat room user through a ping flood attack. | The system was running alongside other server systems, and the ping flood attack affected all the systems, but the most affected was the port system that could not work because of slowed operations. The attack made it impossible to access data (on weather, tides and water depths) at the port. Even though no physical injuries or damages were
<table>
<thead>
<tr>
<th>Location</th>
<th>Method</th>
<th>Actions</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>CSX US Railway (2003)</td>
<td>DoS</td>
<td>The hackers gained access into the system and disrupted the operations</td>
<td>System operations were derailed for quite some time before they</td>
</tr>
<tr>
<td></td>
<td></td>
<td>for some time. The system was accessed through three IP addresses,</td>
<td>were normalized, the attack disrupted traffic in 23 states in the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>probably from another country. The company attacked was not named,</td>
<td>eastern half of US. During the attack, trains were halted due to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>neither was the country of the attackers.</td>
<td>dark signals and delays throughout the day ranged from 15 minutes to</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>6 hours.</td>
</tr>
<tr>
<td>L.A. Traffic engineers’ Strike (2007)</td>
<td>Hacking</td>
<td>The two engineers went on strike and were locked out of accessing the traffic lights control systems. However, they hacked themselves in and changed the settings back to what they were before and could easily access them. They said that their motive was protecting the system from any form of attacks.</td>
<td>Only system settings were changed and it took four days to have them back to normal and operating well. No accidents were reported at the time.</td>
</tr>
<tr>
<td>Lodz Trams Poland (2008)</td>
<td>Hacking</td>
<td>A polish teenager is said to have derailed a tram after he attacked a train network. In doing this, he turned the tram system in the Lodz city into his personal train set, which brought about chaos and derailing a total of four vehicles in the process. He modified a TV remote control in that it could be used in changing track points. He managed to trespass the depots of the tram and collect information required to create the device. He said that he had done it only to create a prank.</td>
<td>Four vehicles were derailed and a total of twelve people were injured in the process.</td>
</tr>
<tr>
<td>Pacific Northwest (2011), USA</td>
<td>DoS</td>
<td>An unidentified railway company was hacked into, disrupting all its railway signals for a period of two days, December 2011. The Railway located in the Northwest of Pacific was slowed down and could not perform its operations normally.</td>
<td>System shutdown for two days, meaning that the operations were shut down at the railway company for two days.</td>
</tr>
<tr>
<td>Port of Antwerp (2011 and 2013)</td>
<td>Hacking (use of Trojan hoses)</td>
<td>In this case, a group of drug traffickers hired hackers to breach the IT security systems that controlled the location and movement of containers. The hackers began by emailing malicious software to the port’s staff. Through that, they were able to gain access to the data through remote access, which they applied in identifying and intercepting the containers carrying drugs and cleared them. After being</td>
<td>Physical damage, port’s physical computing equipment were taken away. At the same time, the systems were compromised and it took time to normalize operations by neutralizing the Trojan Hose used in the attack.</td>
</tr>
<tr>
<td>Event</td>
<td>Technique</td>
<td>Event Description</td>
<td>Impact</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Port of LA (2015)</td>
<td>Ransomware</td>
<td>Maersk confirmed that a Ransomware attack had hit their services and they could not operate in all their outlets around the world. The attack meant that the LA port could not work and it was shut down for a whole day.</td>
<td>Operations were stopped at the APM terminal leading to imminent closure of the port.</td>
</tr>
<tr>
<td>Uber (2016)</td>
<td>Ransomware</td>
<td>Hackers gained access into Uber systems and obtained data of 57 million users worldwide, among those being customers and drivers. However, the attack was concealed by Uber when they paid $100,000 to the hackers and told them to delete the data and not make the breach public.</td>
<td>User data was obtained illegally and Uber lost $100,000 as ransom to the users.</td>
</tr>
<tr>
<td>Port of Rotterdam (2016)</td>
<td>Ransomware</td>
<td>A ransomware attack was initiated on the system and the virus crippled several businesses around the world. The businesses included Maersk and APM.</td>
<td>Many businesses were affected by the attack, bringing down their operations and services that depended on the affected system.</td>
</tr>
<tr>
<td>Ransomware UK Rail (2016)</td>
<td>Ransomware</td>
<td>The attackers locked the San Francisco Municipal Transport Agency computers and demanded to be compensated with 100 bitcoins as payment to have the services back to normal. The municipal transport agency was forced to offer free rides to passengers because they could not access their systems to book the passengers and keep data.</td>
<td>A total of 2,112 computers were crippled and could not work. Customers were given free rides, making the agency lose a lot of revenue in the process.</td>
</tr>
<tr>
<td>Tesla Hijacking competition (2014)</td>
<td>Hacking</td>
<td>A group of Chinese researchers managed to interfere with a Tesla car by taking remote control of the Model S from a distance of 12 miles. They hacked into and interfered with the car’s door locks, brakes as well as other electronic features, showing an attack that could possibly lead to hijacking and compromise of Tesla cars.</td>
<td>The car’s systems were totally interfered with. However, no major damages as this were for testing purposes.</td>
</tr>
<tr>
<td>Sweden Airports (2015)</td>
<td>DoS</td>
<td>A DoS attack was carried out on Swedish airports in the year 2015, raising alarm to NATO and other stakeholders to come in. The attack is said to be linked to a group of Russian intelligence individuals and the system’s services were totally crippled.</td>
<td>The systems of the airports were crippled for some time before they could be normalized.</td>
</tr>
<tr>
<td>Port dimensions: 612.0x792.0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
malware called HDDCryptor was used in infecting a total of 2,112 computers and encrypted all the data.

Maersk (2017)  
JNPT (2017)  
Ransomware  
A ransomware attack was carried out on the port and brought down the operations at the port of JNPT. The system terminal was shut down by the attack after the ransomware attack was carried out.  
The port’s operations were totally crippled and could not be done normally. The system’s terminal was also shut down.

Deutsche Bahn (2017)  
DDoS  
The attackers spammed users with emails that they were tricked to open and give them access to the system. They used a ransomware called WannaCry, which later encrypted the computers and their data demanding fees of $300 and $600 to have the services reinstated back to normal.  
A total of 57000 computers were affected and could not be accessed, with the hackers only promising to reinstate them back if they paid.

Danish State Rail Operator (2018)  
DoS  
A DoS attack hit the Danish State Rail, paralyzing several operations including the communication infrastructure and ticketing system. The attackers also took offline control of telephone infrastructure and mail system. The attack was meant to destroy the entire system and bring it down to its knees, but managed to slow their operations for some time before everything was normalized.  
The ticketing systems were totally affected and could not work. The communication infrastructure was also damaged and no communication could be done.

3.8 Cybersecurity in a Transportation Sector & Airports

Intelligent Transport systems are always more available providing support to control road and rail infrastructures, improving vehicle performance and enhancing the passenger and driver experience also in terms of safety and security. The proliferation of connected devices or sensors inside vehicles, interfacing with external data sources including entertainment, GPS, and diagnostics, creates new vulnerabilities and opportunities for cyber-intrusion if not secured. A fundamentally fresh and holistic design approach, building security into vehicles and transportation from the ground up, is required to overcome threats, and the firmware plays a specific role.

Analyzing the transport section of the Cisco 2017 Cyber Security Report, based also on the evaluation of feedback received from its customers, we can determine the following exposures as listed in the table below.

<table>
<thead>
<tr>
<th>Threats</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced persistent threats (APTs) / Increased use of mobile devices</td>
<td>59 % of transportation security professionals said that cloud infrastructure and mobile devices are among the most challenging to defend against attacks.</td>
</tr>
</tbody>
</table>

Lack of qualified personnel | Half of transportation security teams reported having fewer than 30 employees dedicated to security. And, 29% said the lack of trained personnel is a major obstacle to adopting advanced technologies and processes.

Data Breaches | Half of transportation security professionals have already dealt with public scrutiny due to a data breach. In fact, 35% said they see thousands of daily threat alerts, of which only 44% are investigated.

Outsourcing | 50% organizations outsource some or all their security tasks to offset a lack of internal expertise.

Transportation across all modes is a vital service in all smart cities. Traditionally cities' transportation infrastructure has been built on closed, proprietary systems, today smart cities are increasingly moving toward more digitalized and connected transportation infrastructure. Doing this, many benefits such as improved safety, faster response times for emergency responders, timelier infrastructure repairs, and improved traffic flow and even reduce CO2 emissions are related to the transportation services provided to the citizens.

However, cities keep adopting more complex transport systems and over the time they becoming more and more connected. This leads to have a continuously grown attack environment and more exposure on new threats that are keep appearing. Because more than one transport infrastructure in a city - such as traffic lights, road sensors, public transport or bus lines, ports and airport systems - connects to the network, cybercriminals are increasingly able to attack not only information technology, but also the operating systems technology that manages the signaling and control systems of a city. This means that cybercriminals could potentially cause significant disruption by switching off public transport services, altering traffic signals or otherwise by running away parts of the city's transport infrastructure.

### 3.8.1 Rail sector

The purpose of this section is to analyze the aspects of computer security applied to the railway transport sector with the aim of analyzing exposures deriving from the use of IoT systems. The dynamism of our times, the need to provide information in real time and competition with other forms of transport, today also requires the use of IoT devices in this sector. These applications can be identified, for example, in sensors for track switches, sensors for detecting transit and train control, ticketing and information services for travelers and video surveillance. Take for example what happened in 2016 in the United Kingdom, where the railway network suffered four cyber-attacks\(^20\).

Although these attacks have been more than exploratory and non-destructive, the introduction of digital rail transport plans such as digital signaling as part of the European Railway Traffic Management System (ERTMS) and other modernization initiatives will increase the likelihood of network infiltration. Both in number and extent of the impact. Such infiltrations could be used for data collection, perturbations or, in extreme cases, for potential derailments. The risks of IT security in infrastructure have increased worldwide, with a consequent increase in concern that it could potentially be exploited by terrorists. What mitigation of all this is useful for analyzing even global incidents to increase risk awareness? We cannot exclude a priori that some train accidents in the world cannot be a contributory cause of a cyber-attack.

In March 2016, the South Korean National Intelligence Service said it had halted the attempt to hack the railway workers and close their e-mail accounts\(^21\). Switzerland is already using the ERTMS digital system on some of the busiest railway lines, while in March of this year hackers violated the websites of the Swiss Federal Railways


\(^{21}\) [https://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0WA0B6](https://www.reuters.com/article/us-northkorea-southkorea-cyber-idUSKCN0WA0B6)
exposing the vulnerability of the portals to online attacks\textsuperscript{22}. In addition, in India in 2016, Al-Qaida hacked a microsite of the Railnet page of the Indian railway\textsuperscript{23}. The hacked page of the Bhusawal division of the central railway personnel department and part of a large intranet created for the administrative needs of the department was replaced by Al-Qaida who left a distinctive message.

While many companies seek forms of insurance for vital data or processes in the event that cyber attacks occur, it is essential that companies identify the various risks of infiltration to put in place appropriate measures. The first consideration is that deriving from the fact that most companies, regardless of their size, seem to have very similar problems: ineffective internal policies and procedures, inability to deal with perimeter risk, poor understanding and little competence on the type of IT risks as well as an inadequate communication between the IT team and the board of directors; all this translates into very little real supervision.

While much on the prevention and detection of cyber-attacks is constantly evolving, it is absolutely clear that companies need to be aware of all the risks and resources that can help in preventing risks. Cybersecurity will and should remain a priority in infrastructure for years to come. Compared to what we analyze, we can consider that the main areas of exposure that will be analyzed are the following:

Table 6 - Cybersecurity and Privacy Technologies with respective Cybersecurity and Privacy Engineering Process

<table>
<thead>
<tr>
<th>Cybersecurity and Privacy Technologies</th>
<th>Cybersecurity and Privacy Engineering Process</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity of sensors and cyber-physical systems</td>
<td>Cybersecurity engineering process</td>
</tr>
<tr>
<td>Design of resilient architectures and applications</td>
<td>Privacy by design</td>
</tr>
<tr>
<td>Privacy and data protection issues in transportation systems</td>
<td>Security throughout the system life-cycle</td>
</tr>
<tr>
<td>Hardware security and secure hardware modules</td>
<td>Vehicle-related information sharing and vulnerability coordination</td>
</tr>
<tr>
<td>Security of vehicular communications (onboard, between vehicles, and between vehicles and infrastructure)</td>
<td>Software assurance and formal methods</td>
</tr>
<tr>
<td>Security of application platforms</td>
<td>Security standardization</td>
</tr>
<tr>
<td>Intrusion and anomaly detection systems with a specific activity of Forensics and analytics</td>
<td>Supply chain integrity and traceability</td>
</tr>
<tr>
<td>Security of legally mandated applications (e.g., event and flight data recorders, tachographs, etc.)</td>
<td>Communication of cybersecurity risks</td>
</tr>
<tr>
<td>Security of cloud-based infrastructure</td>
<td>Cybersecurity assurance testing</td>
</tr>
<tr>
<td>Security of road pricing, restricted area access, and vehicle monitoring</td>
<td>Information and processes to drive organizational awareness</td>
</tr>
<tr>
<td>Security of road pricing, restricted area access, and vehicle monitoring</td>
<td>Incident response</td>
</tr>
<tr>
<td>Security of vehicle theft deterrent, immobilization, and theft response solutions</td>
<td>Collaboration and engagement of stakeholders</td>
</tr>
<tr>
<td>Security of vehicular rights control and audit (e.g., feature activation)</td>
<td>Reverse engineering and penetration testing</td>
</tr>
<tr>
<td>Security of emerging technologies (e.g., automated driving, unmanned aerial vehicles, and electric vehicles)</td>
<td></td>
</tr>
<tr>
<td>Anti-reverse engineering</td>
<td></td>
</tr>
</tbody>
</table>

\textsuperscript{22}https://www.ibtimes.co.uk/hackers-breach-swiss-political-party-federal-railways-websites-exposing-vulnerabilities-1550907

\textsuperscript{23}https://www.indiatoday.in/technology/news/story/al-qaida-allegedly-hacked-indian-railways-website-311375-2016-03-02
The track-guided system of railway transport provides vital automation advantages since a train cannot go away from the track while it is regularly operating. For instance, vehicles operating on a road have both the freedom to move freely within their path of travel and can leave or change the lane at will without any damages or any other effects. That is to say, its environment is more flexible and less homogenous as compared to that in the railroads. Such features mean that Railway automation is quite simple and straightforward than the use of roads. However, there is a need to ensure cybersecurity while automating the railways and ensure that there is little or no interference to their operations. The infrastructure of railways, the rail vehicles (and stations) as well as control and command systems are fully networked and digitalized components of IoT. Every element has been enabled with local artificial intelligence that provides the ability to undertake tasks that are goal-oriented with a high autonomy level.

Combining highly responsive, intelligent and autonomous vehicles helps in enabling the communication amongst the vehicles, helped with the intelligent infrastructure, making sure that there are reliable and safe operations. That is done while ensuring that there is a combined running as well as contribution to drastically decrease the costs of the life cycle. That is achieved upon successfully deploying the next generation of management systems used in traffic like the ERTMS (European Railway Traffic Management System) and mass transit CBTC (Communications-based train control).

The use of distributed management of automated trains enables the stakeholders to accurately and adaptively adjust the patterns of transport in demand, drastically increasing the flexibility and capacity of the railway transportation system for all operational forms (high speed, urban rail, rural rail, mass transport system, and freight). The operation of fully automated trains, vehicles and other systems that are intelligent helps in providing the assurance of unprecedented safety level. At the same time, the autonomous operations support new forms of mobility on a rail like the shuttles that are self-operated, thus enhancing smooth connection and movement through different infrastructural sectors involving the use of IoT.

### 3.8.2 European Integrated Radio Enhanced Network (EIRENE)

While introducing the EIRENE project, the European nations realized that they needed to introduce and enhance interoperability through their networks. On that realization, they came up with different prototypes and new radio system to help them meet the international and global standards of such networks, consequently, the railways required a complete comprehension of the issues connected to the installation and operation of the different digital cellular networks, enabling verification along with investigation of the actual costs related to implementing a future radio in European Railways.

Considering the current systems, the project has been modified and created to support standard applications of managing European Railways and an extension will be provided for to the multimedia services provided to passengers. That includes extending the GSM standard system, so as to be the bar with the following requirements of safety and operation:

a) Railway Operations: MMI (Man Machine Interfaces) numbering and addressing schemes.

b) Railway telecommunications: group and broadcast calls.

c) European Rail Traffic Management System (ERTMS).

### 3.8.3 European Rail Traffic Management System (ERTMS)

Digitizing the railway sector and the step taken towards going from the electromagnetic operations to operations that are IP-enabled has been supported by the European Union, coming in the form of ERTMS. The ERTMS can be described as a standard system used in managing and interoperating the signaling for different railway systems, with its application going beyond Europe into some Asian, American and African countries.
IACS (Industrial Automated Control Systems) no longer appear or operate alone from the outside, with the interconnection of railway systems continuing through the use of ATO (Automatic Train Operations) and as a form of intelligent transport mechanisms. However, cyber-attacks on different commercial and industrial systems of control hiked by over 600% between the year 2012 and 2014. Such attacks have led to intense safety and financial concerns.

In 1924, there was the establishment of IEC TC 9 electrical systems and equipment to help in the development of standards for the railway sector that entails fixed installations, rolling stock and management systems for different railway operations. IEC TC 9 is known to be part of the advisory committee for IEC on data and information security (ACSEC). The IEC TC 9, CENELEC mirror committee has directed its efforts towards the CENELEC electrotechnical standardization dealing with railway systems cyber-security.

3.8.3.1 Railway sector cybersecurity threats

The modern railway systems are reliant on a wide variety of digital tools. That exposes them to greater risk levels as hackers have a lot of avenues through which they can attack. Train stations and waysides depend on digital systems for CBI (computer-based interlocking), centralized control of traffic, protecting level crossing and automation of yard switching. SCADA has carried out research on different occasions on behalf of the railway stakeholders from across the globe to determine the levels of security and threats facing them. After long periods of being in the dark, railway stakeholders have finally been provided with the right type of information and are aware of what they face. Researchers with the SCADA StrangeLove pointed out the major issues pertaining to security in many interlocking and train control services. Experts in the area state that hacking the railway systems is not hard, but the hackers must be knowledgeable enough of what they are dealing with. Despite the fact that the software used in railways are not publicly available, the testing of such systems has been done in real-world railways and they are known to be vulnerable to some extent (Kovacs, 2015) [41].

Ensuring mapping of asset dependencies in each business process enables for the calculation of chains and use them in determining the cumulative and cascading risk of possible threats on a business. Railway operators have specific business processes to schedule the train routes. The business process works in that the train routes timing information and stop reschedules are all managed using the appropriate timing software. The program is used to store data about the routine times of the railways, providing and querying timing information as well as making the employees informed about the route changes and reschedules for delayed trains. Thus, an attack on such a system would derail all the operations of railways, leading to massive delays and losses to the affected companies.

3.8.3.2 Kinetic attack on railways

Securing railway systems from cyber-attacks has turned out to be important in digitizing the systems. There is a close interlink between the cybersecurity of railways to railway safety, leaving a gap for the attackers to take advantage of. This has led to the systems being in constant attacks from the hackers (Ivesic, 2018) [4].

For a long time now, railway systems have been very critical to different economies. People and goods are moved from one area to another in great masses. Securing such systems has always been a great challenge, with mass transit systems having several miles of track and several mechanisms of control along the tracks and routes. For a long time, the systems have been solely mechanical. Nevertheless, the operators in railways are increasingly using open-source control systems obtained off-the-shelf. That further increases the challenge of ensuring that the systems are secured from hackers (Ivesic, 2018) [4].

3.8.4 Airports Sector

The security devices at the airports are applied in different configurations, on grounds of various security dimensions, stakeholder requirements, the flow of passengers, the space of operation and different other requirements of cybersecurity and infrastructure (Atzori et al., 2010) [37]. To respond to the latest escalating
cyber-security threats, ENISA has provided a report which will work as a guide to the decision-makers to help them in implementing the existing policies and practices, ensuring passenger security as well as the security of their operations (ENISA, 2016). There are a number of recommendations provided to enhance a resilient and secure operating environment for European airports and they include:

- Setting cyber-security as a top priority for safety.
- Creating clear cyber-security policies in airports and ensuring enough allocation of resources to cybersecurity experts.
- Continuously revising the existing policies of cyber-security on the basis of good monitoring practices.
- Implementation of threat management, holistic risk, and network-based processes and policies for cyber-security at airports.

According to (ENISA, 2016), the integration of IoT on the available infrastructure in airports will help bring new challenges to security. To make sure that there is sufficient security, the operators have to include cyber-security in all phases of the lifecycle of security. Smart airports ensure that they integrate components of IoT to bring services that are value-added. Through the integration of smart components, there is exposure of airports to new attack vectors and a larger attack surface (SESAR, 2017). Thus, the airports have to guarantee daily improved cyber-security levels because of the possible effect that the cyber disruptions and attacks can hold on operator and passenger safety. Enhanced awareness of the risks of cyber-security and enhancing the resilience and security of the whole airport lifecycle at the airport is a top priority.

After the terrorist attack of 11 September 2001, there have been profound changes regarding the approach to airport security, “Cyber” issue is identified as a new risk for aviation security. At the global level, the governing body is ICAO that described in Annex 17 to the Convention on International Civil Aviation, introduced in 1974 as the first release and amended, improved etc. (Aven, 2006) [32]. 15 times, the 10th edition became applicable in 2017, describe the Security – Safeguarding International Civil against acts of unlawful interference introducing the universal security audit programme.

At the European level, the first legal framework was contained in the EU policy activities in commercial aviation are undertaken by the European Commission (EC) and the European Aviation Safety Agency (EASA) (established by EC regulation no 216/2008), EU-LISA. This is an EU Agency responsible for managing and promoting information and communication technology. There is a specific focus on airports cybersecurity which is analyzed in the Single European Sky, in the framework of the SESAR Project that provide a detailed analysis of the cyber risks and in a recent study done by ENISA. In the report “Addressing airport cybersecurity” the costs of a cyber-security breach can be extremely high as shown in the table below.

<table>
<thead>
<tr>
<th>#</th>
<th>€1m/hour cost to the economy of disruption at a major European airport</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>€2m+ direct cost of a serious cyber-compromise</td>
</tr>
</tbody>
</table>

25 https://www.icao.int/
29 https://www.eulisa.europa.eu/
30 https://ec.europa.eu/transport/modes/air/esar_en
Specifically, 3 main areas were taken into consideration and required particular attention:

![Diagram showing three major areas of concern: Air Traffic Management, Aircraft, and Airport. Each area is connected by arrows showing the flow of security considerations.]

- **Air Traffic Management** involves many different services such as Airspace Management, Air Traffic Flow Management, and Air Traffic Control.
- **Aircraft** can be defined as the prevention of and/or reaction to deliberate malicious acts undertaken via cyber means to either compromise an aircraft's systems directly or indirectly where those systems play a key role in the wider aviation system.
- **Airport** can be defined as the prevention of and/or reaction to deliberate malicious acts undertaken via cyber means to either compromise an airport's systems directly or indirectly where those systems play a key role in the wider aviation system.

In the framework of the Chariot Project, the research is focused on the **Airport side**, providing an overview of the main threats that could interest the landside, Airside, and Terminal.

1) Landside representing the nearby airport structure, such as roads and connecting tracks, bus stops, nearby hotels, etc.
2) Airside, which is the operational part of the flight such as Air Strip, Air Parking, Taxation Areas, Service Areas, Supply Areas, etc.
3) Terminal where passengers are registered and redirected to their doors.

Each of these parts are managed by connected devices in the:

- Landside layer, where the passengers are allowed to access without any restriction;
- Airside part, where the passengers are not allowed to access since it is a staff only area with access only to authorized personnel;
- Terminal Layer, a middle layer in which some passengers are gathering more authorization after strict control in order to access;
- Flight gate which is the closest point to the Airside.

All these areas are generally controlled by security IP cameras, connected by hardliners or LAN to the main network center. For the literature available it is shown how it is possible to gain unauthorized access from Landside to airside, attacking the firmware of the security cameras and performing a privilege escalation in order to break into the authorization database and creating a superuser for access to all areas (Darklord, 2008) [18].
Figure 11 - Airport High-Level Representation

Analysing the result of numerous studies conducted to evaluate the effectiveness of the security measures taken at airports, a useful contribution is contained in the Securing Smart Airports study carried out by ENISA. In particular, it emerges that the adoption of a hyper-connected model - in which passengers at airports want fast internet and where we also find the commitment to digitization in relationships with airlines and resellers and/or suppliers - is increasing cyber-risks creating more opportunities for cybercriminals (Elias, 2008) [33]. With respect to what is shared we can determine the main elements to consider in order to guarantee an appropriate cybernetic resilience:

- Ensuring that an airport is secure by design
- Establishing strong cybersecurity leadership and effective governance
- Adopting a lifecycle approach to cybersecurity
- Aligning cyber, physical and personnel security
- Establishing a security monitoring and incident response capability
- Ensuring cybersecurity stakeholders are identified and managed
- Underpinned by the establishment of a strong cybersecurity culture

Major risks can be identified in the following segments: increased use of technology, hyper-connectivity, data sharing obligations, customer focus, IT / IoT towers, towers and remote airports such as mega hubs. The assets considered here are derived from the ENISA Smart Airports Functions and Assets document. Assets can be classified according to the impact of a determined disruption time. An asset can be considered vital if its disruption cannot last more than 2 hours because too many flights would be immediately delayed and then canceled. An asset is critical if its disruption cannot last more than 24 hours because too many flights would be delayed. Otherwise, an asset is useful or not applicable (N/A).

Table 8 - Functions and Assets

<table>
<thead>
<tr>
<th>Functions</th>
<th>Assets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airline/Airside operations</td>
<td>Airport Operation Plan AOP</td>
</tr>
<tr>
<td>IT and Comms Airline/Airside operations</td>
<td>Local Area Network Systems (LAN)</td>
</tr>
<tr>
<td></td>
<td>De-icing systems</td>
</tr>
</tbody>
</table>

[32] Securing Smart Airports – December 2016 - ENISA
Current optimization trends indicate the relevance of integration strategies and real-time communication in the management of existing systems, overcoming system isolation (i.e. SCADA systems) and therefore improving performances. Modern hubs are hyper-connected environments where information flow connects all systems. For instance, Passenger Name Record (PNR) system and Network Operation Plan (NOP) will be connected to the Airport Operation Plan (AOP).

Augmented connection within and across the aviation domain enables efficient communication among all stakeholders (managing authorities, companies, end-users) implementing data aggregation, fusion, and analysis techniques (i.e. Collaborative Decision Making CDM processes). Standard commercial technologies are increasingly used and effective, as it emerges also from Airports Council International’s Aviation Community Recommended Information Services (ACI - ACRIS) specifications for standardized web services, which in some cases can be related to system inadequacies as a factor of vulnerability.

Automation-based cyber threat vectors in airports include Airport Systems, Access Control, Perimeter intrusion systems, Credentialing Systems, Document Management, Radar systems, Airport business system, FIDS Network, Wired and wireless networked systems, Industrial control system, Facility management, SCADA. Cyber-attack typologies and effects include: Advanced Preexistent Threat Campaign targeting Airports; Malicious traffic from two nation-states as result of a phishing email, public document used as an e-mail source; Passport control system affected as potential result of malware; Intrusion to airport private network baggage system, a potential result of malware; Attack on Airlines grounds to flights: ground operator system affected, as result of suspected DDOS attack; Mass hack to loyalty accounts. The assessment methodologies are a significant aspect of mitigation strategies and they include:

- Penetration testing;
- Compliance Requirements;
- Network Traffic Review;
- System Configuration Review;
- Network Discovery: Airport and Protocol Identification;
- Vulnerability Scanner.

Security assessment in aviation sector refers to CANSO Cyber Security and Risk Assessment Guide.\textsuperscript{34}

3.8.4.1  \textit{Increased technology usage}

Technology plays a key role in airport operations. And unsurprisingly, airports have significantly increased their reliance on technology and automation in recent years to meet their business objectives. Airports continue to

\textsuperscript{34} https://www.canso.org/canso-cyber-security-and-risk-assessment-guide
invest in new and innovative Operational technologies to increase speed and reliability at common bottlenecks. Examples of this include the use of electronic tags for baggage handling and tracking, remote check-in, smart boarding gates, faster and more reliable security screening technologies, and biometric immigration controls, which drive major efficiency benefits at airports.

The reliance on cutting-edge, yet less mature, Operational technologies might bring significant improvements but could also expose airports to new risks and unknown threats. In particular, many of these new developments automate existing passenger processes. They give users a more direct interface with complex automated operational systems, for example, self-check-in, self-bag drop or self-boarding.

Communication between the air traffic control tower and aircraft is increasingly shifting away from traditional radio voice communications towards data-link technologies. This is facilitated by the use of electronic flight strip systems in tower environments, which support the automatic generation of clearance messages. The use of data-link in this way provides clear benefits to both controllers and pilots, in terms of efficiency and the removal of human error and ambiguity in voice messages. However, it also introduces significant new risks, in particular, the loss of the credibility check that is inherent to a voice communications environment, where all parties are using a shared voice channel. While a pilot may be able to identify an unfamiliar or suspicious-sounding clearance received as a voice command from another human, a data-link message from a malicious source may be impossible to identify.

3.8.4.2 Hyper-connectivity

Aiming to make the best of the available information, airports have moved towards centralized architectures. These connect different systems through middleware platforms, integrating all the information in central operational data repositories, often called airport operational databases.

These centralized systems take account of the different information requirements of the users involved in the operations, allowing for real-time and two-way data sharing across diverse systems and networks of the different internal and external airport stakeholders (e.g. ground handlers, airlines, etc.).

At the same time, travelers’ expectations for connectivity are ever increasing, and they demand access to high bandwidth networks wherever they go. Even at airports, passengers want easy and high-speed internet and multimedia options. They’re also increasingly looking for real-time information, and to interact with the airports and related stakeholders directly and on the go. This brings a larger attack surface for cybercriminals to exploit and the possibility that they could affect multiple stakeholders.

3.8.4.3 Data-sharing obligations

Air navigation service providers (ANSPs) are increasingly under pressure to reduce charges and to integrate and harmonize national airspace and air navigation services. System Wide Information Management (SWIM) has evolved into a global concept that has been adopted by the International Civil Aviation Organization to facilitate greater sharing of air traffic management (ATM) system information.

The SWIM programme is an integral part of this transformation. It will connect air traffic control systems and will also enable interaction with other decision-makers, including other government agencies, airports, and airspace users. SWIM is now part of development projects in both the European Union (SESAR35) and the United States of America (Next Generation Air Transportation System - NextGen36).

35 https://www.sesarju.eu/
36 https://en.wikipedia.org/wiki/Next_Generation_Air_Transportation_System
3.8.4.4 Customer centricity

Following in the steps of airlines, airports are now increasingly seeking to engage with passengers through airport-related apps, providing consistent messaging to develop brand recognition and sharing notifications of flight delays and services.

To achieve this, operators need to be able to track passengers throughout the airport in order to gather and link information to understand the preferences and behavior of individual customers. They then need to customize and adapt the services provided to them. As a result, airports will hold more personally identifiable information and have to deal with related security issues.

3.8.4.5 IT/OT towers

Some airports generate significant income from non-aviation sources, such as retail concessions. Traditionally, IT systems have been now isolated from the Operational Technology (OT) systems. However, the integration of the two can bring significant efficiencies, allowing real-time data gathering, processing, and decision-making.

The ability to constantly monitor a system’s “health”, track the operational processes, receive real-time information and exchange data with IT systems gives the opportunity to improve airport operations but also expand the threat attacks.

This integration is becoming easier with the growing use of commercial off-the-shelf products, and typically IT-related protocols (e.g. the Internet Protocol) found in most modern OT systems. The record amount of information on ICS and OT online, including user and operation manuals, can potentially facilitate cyber-attacks.

3.8.4.6 Remote towers

ANSPs, airport owners and operators, and related stakeholders face growing pressure to reduce their operating costs while maintaining safety and efficiency. In this context, the interest in digital remote towers as a replacement for the primary control tower, or even as a contingency, has grown significantly in the last few years.

Ornskoldsvik Airport in Sweden was the first in the world to get this system approved as the primary provider of air traffic control. And since 2015, flights have been controlled by a remote tower 110 miles away. Today, there are several test sites around the world (Leesburg International Airport, the United States; Vaeroy heliport, Norway; Alice Springs airport, Australia), and many major airports across the world, that are considering adopting this approach. In 2009, the virtual contingency facility at Heathrow was the first virtual tower to achieve certification to provide contingency operations if the main visual control tower became inoperable. This facility, which is much more cost-effective than building a secondary tower, can provide a capacity of up to 70 percent of the main tower.

Unlike physical control towers, these critical systems become highly dependent on the data links that transmit the information from one place to another. So, a cyber-attack (such as denial of service or network flooding) or physical attack (such as cable cutting or damaging network equipment) could disrupt operations and transform the airport traffic, impossible to be managed.

3.8.4.7 Airports as mega hubs

In their ambition to grow their business, airports have become hubs, providing services for particular airlines or regions, and bringing a significant increase in operational volume and the need for greater integration. As the airports become larger, even more common collaborative decision-making technologies and processes are implemented and more integrated systems are utilised. These allows them to share greater amount of data between the different stakeholders involved in airport operational processes.

Larger infrastructure and greater operational complexity are also needed to achieve more passenger throughput, which results in the installation of more efficiency-oriented technology and greater automation of the IT and OT systems.
These airports are then more exposed to attacks, and their iconic status makes them more “attractive” for attackers. The main threats that could involve airports, according to the SESAR projects results are listed below:

- **Scenario 1: Distributed denial of service attack on the Airport’s internet connection**
  A group of attackers wants to blackmail large companies into paying a ransom by threatening them with a volumetric distributed denial of service attack (DDoS). The attackers have identified that an airport operating company could be a great target since it relies on its Internet connection and controls significant financial resources.

- **Scenario 2: Deep and slow infiltration to steal data**
  A group of highly motivated and skilled cyber-criminals wants to infiltrate an airport network to steal data. The final part of their attack is to clean their tracks by destroying some of the airports’ IT systems.

- **Scenario 3: Major integrity loss**
  A highly motivated group wants to disrupt operations at the airport and, if possible, operations at other European airports. In order to do this, they send incorrect flight information to the targeted airport using a messaging service deployed around the world and used by airlines, airports, handlers and other businesses related to aviation. It is, therefore, relatively easy for an attacker to gain physical or digital access to a connection by compromising one of these legitimate businesses.

- **Scenario 4: Blended attack**
  A group of hackers wants to disturb an airport but without being noticed too quickly. They could achieve this by modifying flight information using the method described in Scenario 3 however this type of attack is too obvious. Instead, to reach the goals they use a blended attack that consists of several attacks with one being obvious, intended to divert attention, and the main attack intended to be conducted in such a way as to remain unrecognised.

- **Scenario 5: Low-level attack on APOC ICS/SCADA infrastructure**
  Programmable Logic Controllers (PLCs) are simple devices that can be used to control physical processes. They run bespoke firmware and do not use conventional operating systems. No logging or forensic capability typically exists for these devices nor do they have any intrusion detection facility. PLCs are an integral part of Supervisory Control and Data Acquisition (SCADA) devices. There are hundreds of thousands of them at every airport, but they are often ‘invisible’ because they are stand-alone components controlling everything from power distribution through air-conditioning and baggage handling. APOCs increase the integration of these devices through IP interfaces that enable stakeholders to monitor their behavior.

The vulnerabilities that can allow or enable the attacks, have been identified for each scenario and are listed in the table below.

<table>
<thead>
<tr>
<th>Types</th>
<th>Vulnerabilities</th>
<th>Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 2 3 4 5</td>
</tr>
<tr>
<td>Hardware</td>
<td>Lack of periodic replacement schemes</td>
<td>✓</td>
</tr>
<tr>
<td>Hardware</td>
<td>Lack of efficient configuration change control</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Well-known flaws in the software</td>
<td>✓</td>
</tr>
<tr>
<td>Software</td>
<td>Lack of an audit trail</td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td>Poor password management</td>
<td>✓</td>
</tr>
<tr>
<td>Software</td>
<td>Uncontrolled use and downloading of software</td>
<td></td>
</tr>
<tr>
<td>Network</td>
<td>Unprotected lines of communication</td>
<td>✓</td>
</tr>
<tr>
<td>Network</td>
<td>Single point of failure</td>
<td>✓</td>
</tr>
</tbody>
</table>
### 3.9 Smart building

The BAS (Building automation systems) and BOS (Building Operating Systems) have greatly improved and changed from the physical aspects to IT-enabled smart operations. At the same time, there is currently a new generation of intelligent and new buildings that are IoT powered. The increased entry of several vendors in technology packages indicates a totally transformational stage in the trajectory of smart buildings.

![Figure 12 - The landscape of smart building service providers.](image)

The modern smart buildings are increasingly being connected with IoT and made to operate well through the increased convergence of Information technology and Operational Technology systems in the buildings. Many new components like remote access, the cloud, data analytics and sharing as well as shared and connected networks have basically changed the way different environments are being operated and used. At the same time, such components have utilized a closed-loop architecture in buildings and changed them into components that necessitate the open control and access of several service providers and operators (Aazam et al., 2014).

The role played by the components is very important in achieving the benefits of a connected and converged space. Nevertheless, many buildings are left vulnerable to a new type of threat, whose effects are undervalued and downplayed. After seeing the latest chain of security breaches across different organizations, smart building...
stakeholders are coming into recognition of the possible damage that the cyber threats hold against their businesses and their related industries.

A functional management plan for intelligent buildings is vital as it helps in mitigating the risks likely to be faced throughout the phases of design, installation, and operation in the lifecycle of a system. Several firms emphasize more on the creation of secure designs and taking fewer steps towards the maintenance of security as they progress over time. Such a method is analogous to creating a protective wall securing a castle and deciding not to use guards watching over, which will allow people to intrude easily. Creating a plan like that needs coordination from all parties involved in the system all the time as it is in its lifecycle. Some of the parties include the network administrators, system integrators as well as facility personnel. Everyone contributing should have an idea of the unique challenges of ensuring security in an intelligent building management system.

### 3.9.1 Integrated building networks

A smart building’s integrated network is one whereby the actual benefits of a converged and smart infrastructure are obtained by the building operators and owners. Nevertheless, this is also the stage that a building is exposed to extreme threats. Moving from the conventional standalone systems to smart buildings, the industry of smart buildings has greatly moved towards a flexible environment characterized by open protocols and systems governing their aspects of the operation.

![Figure 13 - Exhibit: security threats of an integrated network in a smart building.](image)

The old norm where there was protection through obscurity used in standalone systems is not an option in the interconnected and intelligent systems that run on open protocols with remotely each physical system integrated into the building under the control of some supervisors. For example, a BAS enabled with a network can practically control each physical system, starting from ventilation, heating, lighting, air conditioning, physical security and much more. In this case, if attackers manage to infiltrate the BAS, they will also be able to infiltrate and interfere with the whole firm (Aazam et al., 2014).

### 3.9.2 The most famous smart building attacks

Smart buildings have experienced a great surge over the past few years and this has put them much on the limelight and attracting attackers from all walks of life. With many planned attacks on the way, the consequences are far reaching and deadly. Some of the attacks have become recognized across the globe, like the Sydney attack on Google Australia office which took place on May 2013.

[https://www.theregister.co.uk/2013/05/06/google_building_automation_fail/](https://www.theregister.co.uk/2013/05/06/google_building_automation_fail/)
The attack exposed about 40 million credit and debit cards and their respective accounts over a period of three weeks (Boyes, 2013) [27].

Another great example is an attack on the St. Regis 5-star Shenzhen Hotel, with the attack seeing the hacker control of hundreds of hotel rooms in the hotel on July 201438. Another prominent attack was on the power Grid of Ukraine on December the year 201539, leading to very great repercussions in the end. In the process, several hundreds of people in cities were left in the dark for many hours and many other cities affected along with businesses. This was a great catastrophe indicating the power that hackers can have in controlling IoT systems (Steffen et al., 2017) [24].

### 3.9.3 Possible solutions to Protecting Smart Buildings from attacks

On top of knowing more about smart buildings, how they work and possible attacks, it will be good to understand the methods that can be used in protecting the systems from imminent attacks (Rodrigo et al., 2018) [29]. These include:

- **Physical Access Control**: This is the most basic ways of controlling attacks as attackers could be within the premises or gain access into the premises and plant their attacking software and hardware on the system. A strategy for prevention for such attacks on the physical level if a service that the building automation can offer. The most basic scenarios are those where the PIN is used in accessing rooms, or even using biometric identification and authentication. However, not in all cases will this method apply as some of the attackers could be authorized individuals within the organization who might go without being noticed (Steffen et al., 2017) [24].

- **Automation systems hardening**: In this case, hardening embedded workstations and systems at all levels on the hierarchy of automation is important and needs to entail a secure practice of coding and hardening of the operating system along with application and provision of security patches (Steffen et al., 2017) [24].

- **Hardening operating systems**: The equipment used in manufacturing automation systems run in a number of either externally developed or self-developed environments on their respective devices. Over the past few years, the most commonly applied systems include Linux-based systems and also Windows CE on devices that are embedded. The workstations that do monitoring normally run a windows version or a QNX real-time OS. All the systems need to be hardened but require various approaches to have the same good results. It is extremely hard to patch embedded system. Because of that, the systems’ attack vectors should be kept minimal. All the standard approaches to this are aimed at eliminating all services that are not needed and ensure port closure. Some distributions on older Linux do not permit foe the compilation of stack software that are smash-protected or do not have other important security features and need to be replaced with other newer systems (Steffen et al., 2017) [24].

- **Secure Coding**: There are many guidelines provided for testing and writing source code security. Whenever such rules are used, many vulnerabilities like format string overflows and buffer can be prevented or minimized. At the same time, tools exist for automatically analysing the code and determine the existing flaws in programming (Rodrigo et al., 2018) [29].

### 3.9.4 Smart Building design and related components

Smart building designs give a reflection of the smart features that exist in the building itself. It is created in a manner that it enables changes to be made while it is being used. The internal design of the smart buildings give

---

a reflection of the building’s dynamic nature through being adaptable to the different needs that the inhabitants have.

![Figure 14 - Heating, Ventilation and Air Conditioning Control](image)

Typically, an example of a smart building and the components in it are shown in the figure below:

- **The air conditioning, ventilation and heating systems**: These are used to control the temperature, humidity and the air quality within the building. Because of a high level of heat produced within the big buildings, the systems can be very complex. Such systems entail several components such as chillers, boilers, VAV (variable air Volume) tools, as well as AHUs (Air Handling Units). Connecting them to IoT exposes the buildings through many ways that might jeopardize the security of the inhabitants (Steffen, et al., 2017).

- **Access control systems**: the systems are used in a smart building to control the people allowed to access the building and different resources in the building. The physical access control systems work to limit unauthorized people from entering and accessing the network of the building. Generally, the systems entail different components such as sensors, card readers as well as sirens, all connected to the building control panel, controller and central host server (Steffen, et al., 2017).

- **The lighting control system**: The systems offer lighting facilities for the people living and using the smart buildings, based on their individual requirements. A building’s lighting is dependent on the location, the number of people occupying the building and time of the day among other factors. The collected data through monitoring by the light sensors can be applied in scheduling the light controls in an efficient way. Some of the tools used in the given system include timers/clock, occupancy sensors, lamps and control units.

- **Fire alarm system**: the system is vital for the safety of people and also the building itself. Such systems aim at reducing the damage done to the building and the people living in the building caused by fire, heat or smoke. A normal fire alarm system is integrated with the access control systems to help them unlock the doors just in case an emergency erupts any time and people are unable to get out for their safety, with the HVAC system helping in removing smoke from the building, fire and as well as heat through the automated fans.

- **Video surveillance systems**: they are used in recording the different activities being carried out within and outside the smart building. Typically, they need cameras for surveillance that can be remotely controlled through a security controller. In the modern-day world, the cameras that have features like...

---

panoramic view, zoom and tilt are used in such buildings. The videos and pictures of assets that are captured by the cameras are protected and secured from tampering and theft mainly caused by unauthorized individuals accessing the building (Steffen, et al., 2017).

- **Facility Management systems**: the systems have their main focus on ensuring control of operational management of the smart buildings. Such systems are quite different from the BMS (Building Management Systems) that monitor and control the operational functional systems of the building. The facility management systems aid in managing the flows of work, assets, procurement and inventory of their respective buildings.

<table>
<thead>
<tr>
<th>ISO standard</th>
<th>BACnet</th>
<th>KNX/EIB</th>
<th>EnOcean</th>
<th>ZigBee</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Topology</td>
<td>Tree</td>
<td>Tree</td>
<td>Star, mesh, p2p</td>
<td>X</td>
</tr>
<tr>
<td>Number of OSI layers</td>
<td>4</td>
<td>5</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Wireless</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Wired</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>Encryption</td>
<td>AES-128 (CBC)</td>
<td>AES-128</td>
<td>AES-128</td>
<td>AES (CCM*)</td>
</tr>
<tr>
<td>Authentication</td>
<td>HMAC</td>
<td>AES-CBC-MAC</td>
<td>AES-CMAC</td>
<td>MAC</td>
</tr>
<tr>
<td>Security features easily deployed</td>
<td>X</td>
<td>X</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### 3.9.5 Cyber-threats to smart buildings

With the help of converged and complex IoT systems, the hackers can take advantage of the weak points in smart buildings to make their way into areas with better protection. For instance, Stuxnet only used a USB drive to enter into and affect nuclear centrifuges, whereas Havex utilized an infected website as their vector for attack (Aazam et al., 2014) [236].

1. **Communication Threats**

Attackers on smart buildings use channels of communication between various IoT connected devices to launch their attacks. Some of the threats include availability threats, spoofing, eavesdropping, replay attacks, and MITM (Man-in-the-middle) attacks.

- **Availability Threats.** The hackers utilize DoS (Denial) of Service attacks in preventing the authorized users from accessing the system by stopping the service through exhausting of the communication channel. The attackers also fill the system with numerous access requests, which the system cannot be able to handle, and eventually crumbles down.

- **Eavesdropping.** This form of attack enables the attacker to access various channels of communication and take advantage of the channels through the extraction of shared data transferred from one entity to another in the company. The data gained can be used in further attacks that will lead to great loss financially and in terms of information (Aazam et al., 2014).

- **Spoofing.** This type of attack enables the attacking individual to impersonate another user within the system over the same channel of communication, soliciting very important information that can be used against the company. The most common spoofing attacks in smart buildings include Address Resolution Packet (ARP) spoofing and IP spoofing.

- **Man-in-the-middle attack.** In this form of attack, the attacker unsuspectedly becomes an intermediary between the sender and receiver of important information. Through that, he or she can easily intercept data packets being transferred and gain important information. At the same time, the attacker can
intercept the data and replace it with malicious data, which will be used when it reaches the destination (Aazam et al., 2014) [36].

2. Physical cyber threats to smart buildings

These threats are actualized if the attacker can be able to compromise the physical devices operating on IoT belonging to this category. The main threats include node damaging and device capture (Aazam et al., 2014) [36].

- **Node damaging.** In this attack, the attackers with physical and access to the physical address of IoT devices can damage them physically to an extent that they cannot be used in data transfer. If by any chance the attacker is able to damage them in large numbers, a possible DoS situation will occur and paralyze normal operations in such smart buildings (Alohali, Merabti & Kifayat, 2014) [35].

- **Device capture.** Here, the attackers access the physical environment where the deployment of IoT devices has been done. Getting such an access enables them to access the deployed IoT devices in the smart building and then obtain information through the use of various means before sending the information to the system. That gives the attacker an upper hand in gaining information even before the intended receiver gets it (Kim and Kim, 2015) [34].
4 Consolidated CHARIOT Design Method

Subtask 1.4.2 (’Consolidated Chariot Design Method’), consolidates outputs from T1.1 to T1.3 (and also from Task 2.1- ‘Architectural Specification of the CHARIOT Platform’), to produce the CHARIOT Design method that captures the ‘system of systems’ aspects, encapsulating the vision, actors, objectives and drivers, principles and constraints to business functions, services, processes, data and their relationships and covering all stages of risk and resilience management. Also, dealing with IoT capability maturity assessment, cost benefit analysis, change management, impact strategies, benchmarking qualification and certification.

4.1 Overview

The CHARIOT method is a ‘system of systems’ engineering methodology because it deals with the design, configuration and concurrent operation of multiple systems: the IoT system, the CHARIOT system and the industrial system. These systems are outlined below.

The IoT system is the network(s) of sensors and other devices that capture data from the industrial system and its environment. As explained in Deliverable D2.1 (’Design specification for CHARIOT cognitive IoT Architecture’), the Industrial System (for example a manufacturing process control system, a building management system, a rail safety system, etc.), utilises the IoT data to monitor, control and optimise its operations. Typically, this is achieved with the use of a Controller that manages the operational performance of the industrial system, ensuring that it adheres to its goals and that it operates within the desired envelope.

The third system of the CHARIOT family of systems, is the CHARIOT Platform itself. The CHARIOT Platform acts as a mediator between the IoT system and the Industrial System (or its Controller), to ensure that the IoT system does not introduce risks that affect the correct operation of the Industrial System.

Therefore, the overarching driver of the CHARIOT method is the Industrial System and the mission, goals and constraints that define its operation. It is the Industrial System that will specify the operational envelope of the IoT system and set goals and constraints in terms of performance, safety, security, privacy, and so on. The IoT system is external to the Industrial System and interacts with it (i.e. through exchange of information), and through this interaction introduces risks for the correct operation of the Industrial System. The most common types of risks are those of safety, security and privacy and are in fact the types of risks managed by the CHARIOT system.

Some of the risks introduced by the IoT system can be controlled by the careful configuration, design and installation of that system. This is achieved through the application of an IoT Engineering methodology that can ensure that certain quality characteristics are met by the IoT system. However, the engineering of the IoT system is not always within the scope and control of the Industrial System operators. Many industrial IoT systems are purchased ‘off the shelf’ and installed and maintained by third parties. Their quality standards are unknown or uncertain and for all intents and purposes they can be considered as ‘black boxes’ by the Industrial System.

To some extend this can be mitigated if the operators of the Industrial System apply additional quality inspections to the IoT system, such as software, hardware and network operation inspection and tests, however this may not always be feasible due to lack of technical competence or resources. Thus, the IoT system can introduce unforeseen (and unknown) risks for the integrity of the Industrial System. Such risks can however be minimised (although never entirely eliminated) by a managed approach. This is affected through the CHARIOT Platform that presents a managed environment for IoT systems and data that minimises risks associated with the use of the IoT system.

Figure below illustrates the above ‘onion’ approach of viewing the IoT system in the context of the larger Industrial System.
The phases of the CHARIOT method are visualised in the diagram of Figure below. The Diagram shows that the CHARIOT Platform is an additional layer of engineering method which adds to the quality assurances of System Engineering and IoT Engineering.

The CHARIOT method therefore is neither a system engineering methodology, or an IoT methodology. It is a managed approach for Industrial IoT that minimises its safety, security and privacy risks to the Industrial System.

As a managed approach to IoT installation operation and evolution, the CHARIOT method advocates the use of concepts and techniques from system and software engineering methodologies. This includes for example techniques for source and binary code analysis for the IoT devices. It also encompasses techniques from the cybersecurity area such as firmware verification. However, the CHARIOT method needs to be widely applicable and compatible with the existing standards of maturity and practice both at the system/software engineering as
well as the IoT Engineering. As such the CHARIOT method cannot afford to be overly prescriptive, taking instead the shape of a high-level framework of guidelines where different techniques, practices and tools can be used, as appropriate to the particular organisation adopting (and adapting) the CHARIOT method.

As shown in Figure 16, the CHARIOT methodology considers three distinct concerns:

- **System Engineering**: Modelling and understanding safety, security and privacy aspects of the Industrial System. This is used for further refining functional and non-functional requirements for the IoT System.
- **IoT Engineering**: In this phase, the existing or planned IoT system is described and analysed to ensure compliance with requirements and constraints defined in the previous phase. Additional non-functional requirements for IoT such as reliability and serviceability are identified. The software/firmware of IoT subsystems and components are updated/overhauled where necessary to ensure that they are up to date. Several analysis and testing activities take place in this phase involving both the source and binary code of the IoT component/devices firmware, where possible. All necessary network / hardware / software interfaces are reviewed and completed as necessary.
- **CHARIOT Platform configuration and deployment**: The CHARIOT Platform is a complex system whose components need to be suitably configured and connected via gateways to both the Industrial System and to the IoT System. The CHARIOT Platform components need to be provisioned computational, storage and network resources that match the needed performance requirements. Finally, they need to be connected to external services, for example Cloud based analytics services.
- **Continuous engineering**: Neither, the Industrial System, the IoT system or the CHARIOT Platform are static. This means that as the functionality, interfaces and requirements of these systems change, the methodology is supposed to assist performing the necessary modifications and updates without (a) disrupting the operation of any of the three systems, and (b) violating existing requirements and constraints. Thus, in this phase, techniques such as regression testing, agile delivery and Devops can be utilised. The CHARIOT Platform has been engineered to support an agile/continuous delivery approach, using for example software repositories and containerisation. This enables CHARIOT Platform subsystems to be continuously engineered.

Therefore, each of the above concerns of the CHARIOT method comprises a number of system and software engineering tasks and activities with a specific outcome. These are outlines in the following sections.

### 4.1.1 CHARIOT Methodology Stakeholders

Designing, configuring, deploying and maintaining a CHARIOT installation is a multi-disciplinary endeavour, requiring participation from stakeholders with a wide range of expertise, skills and roles. The main categories of stakeholders and the phases they are involved in are outlined below:

- **Systems Engineers**: They are primarily concerned with the configuration, operation and evolution of the Industrial System that CHARIOT supports. They can be further sub-classified according to the Industrial Domain they belong to as reliability engineers, electrical and electronics systems engineers, process engineers, etc. They set the overall context of the CHARIOT system, its high-level mission and requirements/constraints.
- **ICT System Engineers**: They are primarily concerned with the ICT systems and networks installed in the Industrial System. They can be further classified as IT architects, network engineers, software engineers and so on. They specify the IT system interfaces to both the Industrial System and the IoT system. They also specify functional and non-functional requirements that the ICT systems place on the IoT system.
- **Business Operations**: This is the category of users that ensures the day to day continuous correct operation of the Industrial System. They employ ICT systems to monitor critical parameters about the operation of the Industrial System and to control its operation if necessary, via the appropriate Control systems. They are the indirect users of CHARIOT as their systems receive process and display information derived in part from the IoT sensors via the CHARIOT system.
• **IT Operations.** These are the people responsible for the correct continuous operation of the ICT systems according to the existing service level agreements. Their systems rely in part on data received from the IoT system via the CHARIOT system. They are responsible also for enforcing the ICT policies in place by their organisation.

• **IoT Engineers,** including the designers of the overall IoT network and the installation / configuration / integration teams. They are responsible for ensuring that the IoT Network is deployed and operating according to the requirements placed by the ICT and other systems of the Industrial System.

• **CHARIOT System Operations.** This includes IoT installers, engineers, developers, testers, administrators and deployment teams, as well as CHARIOT system administrators. These are the people responsible for the continuous operation of the IoT system, according to the requirements and constraints placed by the other systems connected to IoT. They are direct users of the CHARIOT system as they configure both the IoT sensor connections to the system, as well as the components of the CHARIOT system such as the CHARIOT Engines.

In summary, the CHARIOT methodology presented below, aims to be flexible and open acknowledging the broad set of techniques, methods, tools and technologies currently employed in the IoT and industrial domains. Therefore, an organisation adopting the CHARIOT methodology is free to use its own (or existing standards) methods, tools and techniques in the relevant phase of the CHARIOT methodological framework.

### 4.2 System engineering

#### 4.2.1 System and context modelling

The purpose of this task is to capture information about the Industrial System in a precise and efficient manner. This will enable the IoT system, during the second phase, to be understood in a system context, to analyse and evaluate and resolve system requirements and architectural issues, and to support trade-offs. The intention of this phase is to communicate information about the Industrial System correctly and consistently among its various stakeholders, but also among the IoT stakeholders (e.g. engineers and software developers), as identified in the previous section. The purpose also is to help define the boundaries of the Industrial System and design its main interfaces to the IoT system.

Regarding the utilized techniques, system modelling notations and languages such as Systems Modeling Language (SysML) can be utilized for this task. SysML is a general-purpose modeling language for systems engineering applications and supports the specification, analysis, design, verification and validation of systems and systems-of-systems. Other architecture-oriented modelling approaches such as the ‘Architecturally-Based Process Flow Diagrams for IoT functions’ can be also used in this stage.

As an outcome at the completion of this task the Industrial System and its main architectural components and interfaces to the IoT system are described.

#### 4.2.2 Collecting, analysing and specifying Industrial System requirements

After the architecture and main functional subsystems of the Industrial System has been defined, the focus shifts on defining what are the potential consequences (risks and benefits) of connecting it to the IoT system. Positive consequences are the qualitative or quantitative improvements to the operation, performance, etc., of the Industrial System, due to the additional information brought in by IoT. However, this subtask focuses not on the positive consequences but on the negative ones (i.e. the risks) of connecting the Industrial system to the IoT system. In other words, in these tasks we capture the unintended consequences of connecting the two systems in terms of safety, security and privacy risks. Upon completion of these tasks, the risks created by the IoT connectivity will be understood. These will be managed by the correct configuration of the IoT system components and by its continuous monitoring by the CHARIOT Platform. The tasks corresponding to these activities are described in subsequent sections.
4.2.2.1 Security requirements and constraints

The purpose of this task is to collect the security risks brought to the Industrial System by its connectivity with the IoT system. This in turn will help to define controls that reduce such risks. Such controls/measures will be translated into IoT configuration and deployment actions and to the setting up/configuration and correct deployment of the CHARIOT Platform as explained in the following tasks. Some of the security controls will be implemented by the CHARIOT Platform’s Security Engine as explained in Section 4.3.4.

General principles of the ‘security by design’ philosophy can be utilized here. Techniques for security modelling and analysis have been described in previous sections of this report. Cybersecurity methods and techniques can be applied, for example, threat modelling. Software Engineering techniques for capturing non-functional requirements, i.e. security related ones, such as the SQUARE methodology\textsuperscript{45}. Proprietary techniques-tool supported such as for example Microsoft’s ‘Engineering-based threat modeling driven by data flow diagrams (DFD)\textsuperscript{41}’ can be used if the IT team has experience in such approaches.

Upon completion of this task, the security risks brought by the IoT connectivity to the Industrial System will be documented, analysed and understood. Subsequent tasks of the CHARIOT methodology aim to control such risks, through correct configuration, installation and deployment of the CHARIOT Platform.

4.2.2.2 Safety requirements and constraints

The purpose of this task is to catalogue and analyse the safety risks brought to the Industrial System, due to its connectivity to the IoT system. In general, it is possible that certain functionalities or connectivity of the IoT system can intentionally (e.g. via malicious act) or unintentionally (e.g. due to malfunctioning), bring the Industrial System (one or more of its components) into an unsafe state.

There are several methods for functional safety analysis such as FMEA, FMECA, FTA, etc. in use by the industry\textsuperscript{42}. While these techniques are not specific to IoT, they nevertheless can be suitably adapted for the purpose. The general approach is to analyse safety critical functions that are dependent on IoT input, to identify events or causal paths that begin with an IoT element and propagate to an Industrial System safety critical function, in a way that (a) prohibit the performance of such function or (b) cause the unwanted performance of that function. Once such IoT system components are identified, the safety risks they cause needs to be quantified, so that appropriate controls can be put in place. Such controls are implemented mainly by CHARIOT Platform components such as the Safety Engine, as explained in Section 4.3.4.

Upon completion of this task, the set of safety requirements that will need to be met by the IoT system will be defined. This will set as input to subsequent tasks that implement the safety controls (Section 4.3.4) in the CHARIOT Platform, such as the Safety Engine.

4.2.2.3 Privacy requirements and constraints

The purpose of this task is to elicit and document the privacy risks introduced by the IoT system’s connection to the Industrial System. Privacy risks are risks that relate to the unauthorized disclosure of personal data of subjects. An industrial system that captures private (personal) data has the risk of unintended or deliberate disclosures of such data to unauthorized parties, due to the inherent connectivity of the IoT and to lack of or incorrectly configured authorization settings, allowing such data to be diverted via the IoT to unauthorized parties. It is also possible that privacy requirements are violated not by direct divulgence of private data but indirectly, via their association with other IoT data and metadata, for example positioning (location) related data.

Some industrial domains such as healthcare have established privacy practices such as HIPPA\textsuperscript{43}. Techniques such as Privacy Impact Assessment A Privacy Impact Assessment can also be employed. HIPPA is a process which

\textsuperscript{41} https://threatmodeler.com/2018/08/01/iot-threat-modeling-example-iot-security/
\textsuperscript{42} These are reviewed in CHARIOT deliverable D1.1: Classification and use guidelines of relevant standards and platforms
\textsuperscript{43} https://www.hippa.com/
assists organizations to identify and minimizing the privacy risks of new projects or policies. Quality methodologies such as Product quality (ISO/IEC 9126) could also be relevant.

The outcome of this task is an assessment of the privacy risk of the IoT system on the Industrial System’s (private) data. This will serve as input to subsequent tasks that control the privacy risk using controls such as the CHARIOT Platform’s Privacy Engine (Section 4.3.4).

4.3 IoT system engineering

4.3.1 IoT system and context modelling

Many industrial organisations procure ‘off the shelf’ IoT systems and have them installed and operated by third parties. Thus, many activities of IoT engineering are not performed by the industrial organization but by third parties if at all. Some engineering activities can of course be retrofitted such as for example software tests and other quality inspections.

One important such activity is that of modelling the architecture and context of the IoT system. Although some kind of architecture and modeling may be carried out prior to the installation of the IoT system, this may not always be available to the operators of the Industrial System, who therefore lack an accurate and complete model of the deployment topology of the IoT system. Although IoT is conceptualized as a distinct system from the Industrial System, in physical terms the two systems are interdependent. For instance, both systems may occupy the same physical space, or be in physical proximity. Both systems are subject to the same or similar external forces such as for example environmental conditions. Finally, both systems may share common infrastructure such as energy supply (e.g. electricity power supply). The purpose of this task therefore is to describe the IoT system in terms of a context, i.e. environment and other entities to which it connects to, captures data from and about, and otherwise interacts with. This will allow to assign the safety, security and privacy requirements captured by previous tasks, to specific IoT subsystems and components, by virtue of their context, for example, their location.

Modelling techniques are used to describe the IoT system in context. Such models include data flow/connectivity models, functional models and even physical architectural models such as physical network model drawings and building drawings, showing the actual physical locations where IoT components are installed. As such models may need to be machine processable, formal languages such as Domain Specific Languages (DSLs) may be used to describe them. CHARIOT Platform’s Safety Engine for example, employs a DSL to describe IoT context models.

Once such models have been created, system safety, security and privacy requirements defined in earlier tasks can be assigned to IoT components or subsystems. This leads to the detailed definition of IoT functional and non-functional requirements as explained in the following task (4.3.2).

4.3.2 IoT Requirements specification

The purpose of this task is to specify functional and non-functional requirements for each of the IoT components. In turn, this will lead to each component to be correctly configured connected and monitored as described in subsequent tasks. Such requirements include:

- Performance requirements: relate to processing speed, throughput at the component and at the network level etc.
- Reliability Requirements. Measured for example with Mean time between failures (MTBF) metric.
- Serviceability requirements: refers to the ability to install, configure, and monitor the IoT devices.
- Functional Requirements Functional behavior of the IoT components- main functions performed.
- Data requirements: types, formats, volumes, accuracy and precision of measurements, and similar data related requirements for data produced by the IoT system components.

Software Engineering methods and techniques can be utilized for this purpose, for example IEEE 1233-1996/Cor a-1998 – (‘IEEE Guide for Developing System Requirements Specifications’).
The outcome of this activity is a complete set of functional and non-functional requirements the components of the IoT system will have to comply with. These will provide inputs to subsequent tasks that configure both the IoT system (Section 4.3.3) as well as the CHARIOT Platform (Section 4.3.4).

4.3.3 IoT component testing and configuration

The purpose of this task is to audit the IoT components to ensure that they can perform their functions according to the functional and non-functional requirements identified in the previous step, in a manner that does not violate the safety, security and privacy requirements imposed by the Industrial System. This also means that all IoT components identified as critical with respect to safety, security or privacy risks are catalogued in a Blockchain registry and are connected to the CHARIOT Platform via the Southbound Gateway as explained in the following tasks. IoT quality assurance can be achieved through a multiplicity of ways according for example to the available documentation and interfaces to the IoT components (i.e. IoT component as a white box versus black box). It also depends on the IoT vendors and the certification programs that are available for the particular IoT system/component used, and also on the available budget for quality assurance.

IoT component certification is a new area and certification bodies and standards are only just emerging. For example, the CTIA Cybersecurity Certification Program for Cellular Connected Internet of Things devices is a standard only introduced in 2018. The NIST Interagency Report (NISTIR) 8200, published in 2019, provides security guidelines covering components, systems and services that will make up a wide range of Internet of Things applications. Additionally, a variety of techniques is used for quality assurance of the critical IoT components. These are classified into system techniques and into component techniques.

System techniques ensure that the sensor is configured, deployed and connected correctly in accordance with the System and IoT architectural models defined in earlier tasks (sections 4.3.1 and 4.3.2). These include simulation, emulation, prototyping and model-based verification techniques. For most IoT installations, it will be prohibitive to individually test each sensor or other IoT device, hence testing of samples will need to be used instead.

Component techniques include the static analysis of the software code (both source and binary, at the firmware, operating system or application level) executed by the IoT device. At the source code level, static analysis can easily by applied during compilation by setting all the compiler warnings (gcc -WAll) and by applying some adequate analysis with the clang static analyzer for example. Testing can operate on non-functional properties with code sanitizers (ex the clang compiler-rt library). In CHARIOT, Testing also includes the input output tests for each component type, for example, each sensor type used. Such test results can be used to create digital profiles for each IoT device category. These can in turn become utilized by runtime sensor checking functions.

For IoT sensor software testing, techniques such as those defined in ISO/IEC/IEEE 29119 Software Testing Standard can be utilised. For static sensor firmware code analysis, specialised tools, such as those developed in CHARIOT Task 1.3 can be employed.

The outcome of this task is that the critical IoT sensors (or at least a representative sample of them) is tested and profiled. Against this profile, various additional runtime checks will be carried out on the sensors and the sensor data by the CHARIOT Platform Engines, as explained in the following tasks.

4.3.4 CHARIOT platform configuration, deployment and continuous delivery

At this stage, a Project that employs the CHARIOT method, will have accomplished the following:

The safety, security and privacy requirements of the Industrial System and their impact on the IoT system (both architecture wise as well as on individual subsystems and components) will have been specified.

---

44 https://clang-analyzer.llvm.org/
45 https://compiler-rt.llvm.org/
46 CHARIOT D1.3 : Specialized Static Analysis tools for more secure and safer IoT software development
As a result, the IoT system will have been deployed and configured within the correct context (e.g. location of sensors), network connections and authorisations, and operating software (both in terms of firmware and in terms of calibration of the sensor outputs). Digital fingerprints of valid sensor properties (such as for example checksums of the correct firmware) as well as models of the correct behaviour of IoT sensors and devices will be produced. These will be utilised in correctly connecting the IoT system components to the CHARIOT Platform as described below.

How this task will be carried out depends to a large extend on the nature of the IoT system (size of IoT network, types of sensors, i.e. ‘dumb’ versus ‘smart’ ones, wired versus wireless, and network connectivity and layout. It needs to be emphasised again at this point that due to all reasons explained above, IoT risks will remain even after installation and configuration steps are followed, as not all risks are identifiable and controllable by the Industrial System alone. Therefore, to control such risks, the managed approach of the CHARIOT Platform needs to be configured and installed. The main tasks towards that end are as follows:

- **Configuring the Southbound CHARIOT Gateway.** The Southbound CHARIOT Gateway is the architectural component of the CHARIOT Platform that connects the IoT system components (sensors, and other IoT devices) to the CHARIOT Platform. (Conceptually, there is only one Southbound Gateway, although several physical IoT Gateways may be present in an IoT installation). All critical components of the IoT system must be connected to the Southbound Gateway both in terms of networking and in terms of other connectivity software required for them to transmit data to the Gateway.

- **Configuring the Northbound CHARIOT Gateway.** The Northbound CHARIOT Gateway is an architectural component of the CHARIOT Platform that connects the CHARIOT Platform to the Industrial System. Configuring the Northbound Gateway entails connecting it to the interface(s) provided by the Industrial System, allowing IoT data to be transmitted from the CHARIOT Platform to the Industrial System.

- **Fog Network configuration.** The Fog Network is the set of networked computational, storage and network resources available locally on the components of the CHARIOT Platform such as the Blockchain and the Engines. A CHARIOT Platform component utilizes Fog Network services for deployment, storage, computation, networking etc. A Fog network needs to be specified and configured taking into account the performance and other non-functional requirements (e.g. volume of sensor data) specified in previous tasks. The physical resources that will therefore be required to implement the Fog Network depend on such criteria and considerations.

- **Blockchain configuration.** The Blockchain is an architectural component of the CHARIOT Platform. It is used for recording the digital fingerprint of valid/authorized firmware for sensors/devices of the IoT system, allowing CHARIOT Platform components such as the Security Engine to check sensor/device firmware against the Blockchain data for validity, at runtime. The Blockchain is deployed and run on the computational resources provided by the CHARIOT Fog Network.

- **Safety, Security and Privacy Engines configurations.** The CHARIOT Platform Engines are software systems developed in the Project that are concerned with managing safety, security and privacy risks created by the IoT system, as explained earlier on. The Engines act upon data received from the IoT Network. The Engines mission is to filter IoT data that can cause a safety, security or privacy risk. Each CHARIOT Platform Engine needs to be configured according to its deployment requirements and to have access to the right resources such as Industrial System and IoT parameters and models (‘profiles’). Fog administration services allow the Engines to be automatically deployed, configured and continuously updated as explained in the following section. Containerisation using the Docker technology is currently provided by the Fog Infrastructure, although potentially other deployment technologies could be utilized.

- **External service configuration and connections.** Several External Services need to be connected to the CHARIOT Platform. These are used for example, for logging, reporting of CHARIOT Platform activity and for importing analytics.
At this stage of the project the system is ready to ‘go live’. Critical (i.e. from a safety, security, privacy perspective) IoT sensors/devices are digitally fingerprinted and connected to the CHARIOT Platform, and their data routed to the Industrial System via the CHARIOT Platform. It needs to be pointed out that a new IoT setup that follows the CHARIOT method might coexist with previous installation. As a matter of fact, both existing and CHARIOT compliant IoT installations can co-exist for a period of time, until the CHARIOT installation is operationally tested. Also, all external services connections are tested at this stage (using real or dummy data as appropriate) to ensure correct operation. Key personnel operating the IoT installation (IoT Operations Team), CHARIOT Platform (administrator and operator roles) and relevant departments/functions of the Industrial System, such as the Operations/Control Room, the IT/security function etc., have been trained to the new operating methods.

4.4 Continuous engineering

Continuous Engineering describes a closed-loop engineering process for the Internet of Things. In the CHARIOT methodology its purpose is twofold: on one hand is to continue to derive value from the IoT operational data, for example through analytics for efficient operation of the Industrial system. On the other hand, the purpose of continuous engineering in our methodology is to ensure that IoT does not introduce new undetected risks and or worsen the risk factors through deterioration of existing controls. Neither the Industrial System nor the IoT system remain static. Additionally, the CHARIOT Platform itself is supposed to improve with better risk management capabilities enabled by the use of data analytics techniques. Thus, continuous engineering consists of continuous delivery of new capabilities to the CHARIOT Platform and the accommodation and validation of changes to the IoT and Industrial systems.

Agile methodologies (such as Scrum47, MSF48, XP49) and continuous delivery, are arguably suitable techniques for coping with the characteristics of the IoT. Agile methodologies simplify software development through reduced development cycles. This fits with the need to integrate into the CHARIOT Platform changes in the IoT, the Industrial System and in the platform itself, as quickly and smoothly as possible. With an agile approach automation of new functionality and subsequent tests (e.g. regression testing) becomes efficient. Additionally, agile methods can benefit by facilitating the collaboration between the Industrial system, IoT and CHARIOT Platform teams, allowing them to exchange knowledge and information.

The outcome of this task is that the CHARIOT system not only continues to be ‘fit for purpose’ but also expanding its capabilities through analytics-based learning. Tasks such as its interoperability, scalability and regression testing are automated and continuously performed, triggered by changes to the IoT or Industrial system and their environments. This allows the increased uptime of the CHARIOT Platform (which ideally is a 24/7 function with no downtime), and the continuous monitoring of the IoT installation.

47 https://www.scrumalliance.org
48 https://docs.microsoft.com/en-us/previous-versions/tn-archive/bb457060(v=technet.10)
49 https://www.agilealliance.org/glossary xp/
5 Simulation Tools

According to DoA, under this subtask, a simulation tool has been developed (and will continuously been upgraded) in order to support IoT applications modelling and Privacy, Security, Safety Threat Vulnerability Analysis using multiple methods of assessment such as agent and network-based methods utilizing existing tools from CORE. At the moment, a prototype version of this tool has been implemented and this is described in sections 5.1 and 5.2 below.

5.1 Project requirements

A number of discussions around the Simulation Tool, have been performed during the early stages of the Project in order to identify, the Project needs, the capabilities of the potential Simulation Tool and how this tool will add a value to the Project. According to these discussions, there were 2 visions of how a Simulation Tool will possibly work and support the Project. These options are listed below:

1. Simulate the CHARIOT network topology

According to this vision, the implementation of a Simulation Tool should have been completed before the initiation of the platform development. It was also required to be implemented early enough and in parallel with the architecture, in order to be able to validate it and support the technical partners during the future platform implementation, by testing the various network topologies of the LLs.

2. Simulate the CHARIOT LL scenarios

According to this vision, the implementation of a Simulation Tool will be initiated in parallel with the platform implementation and deployment. In that case, the Simulation Tool would mostly support the business partners, by modelling the scenarios already defined in each LL, generates IoT data (i.e. sensors and gateway data), and provide useful results (i.e. Privacy, Security, Safety Threat Vulnerability Analysis) to the final users. In addition, it would also support the technical partners and the LLs, by generating and providing sample set of data and showcase the usability of different IPSE components (i.e. Dashboard).

After discussions, it was finally decided to proceed with the 2nd option, “Simulate the Chariot LL Scenarios”. The reasons have mainly to do with the project need to have a more LL-oriented Simulation Tool.

According to that, one of the main outputs of this version of the Simulation Tool is to generate data for the IoT topology components of each LL and forward them to the CHARIOT platform (and moreover to the Dashboard). This can showcase how the dashboard displays the real time readings from the sensors and mitigate one of the risks that have been identified where the LL infrastructure could not provide data early enough, with negative impact on the implementation and the proof of concept of various IPSE components.

5.2 Market research

In order to initiate the implementation of the Simulation Tool, a research on different IoT simulation solutions exists in the market has been performed. The reason for doing this research was not to purchase or use one of the existing market solutions, but to identify the usability of such tools in the IoT world (but not limited to it), along with the best-practices that were eventually followed during the implementation of a customized solution to support the needs of the CHARIOT project. Moreover, the results of this research, guide us to identify the behavior, functionalities and the design that were followed during the implementation of the first version of the CHARIOT Simulation Tool. A list with the different market solutions, are described below.

Popular simulators can be classified based on the big data programming model, and the resource abstractions they are capable of simulating and modelling. Most of current work has focused in particular on modelling MapReduce (MR) processing. Some of the simulators are only suitable for simulating and modelling performance of the MR programming model, hence insufficient in the context of modelling and simulating the behavior of IoT Data Analytics Platform (IoTDAP), which requires multiple big data programming models and diverse resources types relevant to Edge Datacenter (EDC) and Cloud Datacenter (CDC) environments.
• **Iotify** 50. Iotify is an IoT simulator that allows users to develop IoT solutions in the cloud. This tool lets users simulate large scale IoT installations in their own virtual IoT lab. Users can generate customizable traffic from thousands of virtual endpoints and test their platform for scale, security and reliability in order to identify and fix issues before rolling out the final product. Users can also simulate heavy network traffic to see how network latency affects their overall system performance.

• **MATLAB** 51. MATLAB features an IoT module that allows users develop and test smart devices, as well as collect and analyze IoT data in the cloud. IoT platforms collect data from smart devices, aggregate it in the cloud and then analyze it in real time. Patterns and algorithms are then extracted and engineers can then use this information to create prototype algorithms and execute them in the cloud. Users can also prototype smart devices using Arduino and Raspberry Pi.

• **NetSim** 52. NetSim is a network simulator that be used to simulate IoT systems and to test the performance of real applications over a virtual network. If users building a new IoT network from the ground or expand an existing one, they can use NetSim to predict how the respective network will perform.

• **BevyWise** 53. This IoT Simulator is a complex and easy to use MQTT simulation tool that allows users to simulate tens of thousands of IoT devices. Through a UI lets users create and add the necessary devices in no time. Users can configure the simulated IoT devices so as to publish messages at a very precise time. IoT Simulator can store simulation data in FLAT files or MySQL and SQLite databases.

• **Ansys** 54. This IoT simulator can help users develop and test IoT devices and networks. Users can use this tool in a variety of fields, including wearables and medical devices, drones, connected cars, industrial equipment, and more.

• **IBM Bluemix** 55. IBM’s Bluemix is an innovative cloud platform that allows users to sample the company’s Internet of Things Platform even if they don’t have a physical device, using simulated data. The built-in web console dashboards let users monitor and analyze their simulated IoT data and then use it to build and optimize their own apps. The tool supports a wide variety of functions for manipulating data, storing it and even for interfacing with social media.

• **CupCarbon** 56. CupCarbon is a Smart City and Internet of Things Wireless Sensor Network (SCI-WSN) simulator. Its objective is to design, visualize, debug and validate distributed algorithms for monitoring, environmental data collection, etc., and to create environmental scenarios such as fires, gas, mobiles. Not only it can help to visually explain the basic concepts of sensor networks and how they work; it may also support scientists to test their wireless topologies, protocols, etc. Networks can be designed and prototyped by an ergonomic and easy to use interface using the OpenStreetMap (OSM) framework to deploy sensors directly on the map.

• **Packet Tracer** 57. Packet Tracer is a cross-platform visual simulation tool designed by Cisco Systems that allows users to create network topologies and imitate modern computer networks. The software allows users to simulate the configuration of Cisco routers and switches using a simulated command line interface. Packet Tracer makes use of a drag and drop user interface, allowing users to add and remove simulated network devices as they see fit.

---

50 https://iotify.io/iot-network-simulator/
52 https://www.tetcos.com/emulator.html
53 https://www.bevywise.com/iot-simulator.html
55 https://console.bluemix.net/docs/services/iot/index.html#gettingstartedtemplate
56 http://www.cupcarbon.com/
• **SIMUL8** 58. SIMUL8 simulation software is a product of the SIMUL8 Corporation used for simulating systems that involve processing of discrete entities at discrete times. This program is a tool for planning, design, optimization and reengineering of real production, manufacturing, logistic or service provision systems. SIMUL8 allows its user to create a computer model, which takes into account real life constraints, capacities, and other factors affecting the total performance and efficiency of production. Through this model it is possible to test real scenarios in a virtual environment.

• **SimpleIoT Simulator** 59. SimpleIoT Simulator is an IoT Sensor/device simulator that quickly creates test environments made up of thousands of sensors and gateways, all on just one computer and supports many of the common IoT protocols including TCP, MQTT, CoAP, HTTPS, etc. It enables IoT platform and gateway vendors to improve product quality and significantly shorten their time-to-market without incurring large capital expense for creating test infrastructure.

• **Amazon AWS** 60. Amazon Web Services (AWS) provides many services to help customers build serverless IoT applications that gather, process, analyze, and act on connected device data, without having to manage any infrastructure, which can help reduce costs and increase productivity and innovation. AWS offers a device simulation solution that enables customers to build a large fleet of virtual connected devices from a user-defined template and simulate them publishing data at regular intervals to AWS IoT.

• **MRSim** 61. It is a discrete event-based simulator for evaluating performance of Hadoop cluster. It can capture the effects of different configurations of Hadoop cluster setup on data processing activity performance in terms of job completion times and hardware utilization. MRSim is a Map Reduce simulator based on discrete event simulation. MRSim is able to simulate different type of Map Reduce applications with the ability to study with good accuracy the effect of dozens of Job configuration parameters on the job performance. MRSim enables the user to estimate the best job configurations to get optimum performance for certain algorithm. On the other hand, MRSim will capture the effects of different configurations of Hadoop setup on the algorithm's behavior in terms of speed and hardware utilization.

• **MR-Cloudsim** 62. It allows simulation of IoT application by inherently supporting big data processing system such as with MapReduce to facilitate researchers and commercial organizations to understand and analyse the impact and performance of IoT-based applications.

• **Azure IoT** 63. Azure IoT enables the user to connect, monitor, and manage IoT devices in order to develop IoT applications. It is an open and flexible cloud platform as a service that supports open-source SDKs and multiple protocols. Through it the user can fully managed IoT services and solution accelerators designed for industry and scenarios like remote monitoring, predictive maintenance, smart spaces, and connected products. It can accelerate a business transformation with IoT and reduce complexity and costs.

• **IoTSim** 64. It supports and enables simulation of batch processing activity in IoT systems limiting themselves to the MR model. They also presented a real case study that validates the effectiveness of their simulator. IoTSim largely extended Cloudsim’s functionality to support for modelling and simulation of multiple IoT applications running simultaneously in a shared cloud data centres. IoTSim is capable of simulating batch-oriented IoT applications by using MapReduce model with a high degree of accuracy. IoTSim provides better perspective to analyse IoT-based applications using MapReduce model in Cloud Computing environment with less cost and time.

---

60 [https://aws.amazon.com/answers/iot/iot-device-simulator/](https://aws.amazon.com/answers/iot/iot-device-simulator/)
61 [http://barbie.uta.edu/~jli/Resources/MapReduce&Hadoop/MRSim%20A%20Discrete%20Event%20based%20MapReduce%20Simulator.pdf](http://barbie.uta.edu/~jli/Resources/MapReduce&Hadoop/MRSim%20A%20Discrete%20Event%20based%20MapReduce%20Simulator.pdf)
5.2.1 Market research conclusion

As already mentioned above, this market research has been performed not to purchase or use one of the existing market solutions, but to guide us implement a customized solution to support the needs of the CHARIOT project. After concluding with the market research, the general idea of the IoT simulators is to allow users to design, create and test IoT applications and devices without actually using real IoT infrastructure. IoT simulators are great tools to build and test future IoT devices and networks in a virtual lab. They allow developers and engineers to reduce cost and scale their ideas in order to roll out products faster. The IoT simulators listed above are powerful tools in the market that support complex simulations that can be used to simulate and test IoT devices (i.e. sensors, gateways, etc.), network along with their behavior.

The Simulation Tool, implemented under the CHARIOT project, follows the above idea of building a topology on a virtual environment with additional customized components and configurations in order to:

- Be part of a Dashboard concept solution that is currently been implementing under T3.5 “IPSE Analytics Prediction Models and Dashboard”.
- Be in align with the CHARIOT architecture as has been designed and described in D2.1 “Design Specification for CHARIOT Cognitive IoT Architecture”.
- Be directly integrated with CHARIOT infrastructure the Northbound Dispatcher (as described in D2.2 “CHARIOT IoT Cognitive Platform”) in order to utilize the existing topology of the Safety Supervision Engine.

So, the CHARIOT Simulation Tool is not a generic simulation solution but a completely customized one, dedicated to support the needs and the infrastructure of the project. The below sections describe the development of the Simulation Tool; how this works and the ways it can be utilized to help the LLs take the correct decisions and reduce or minimize the risk based on different conditions in order to improve the resilience of Privacy, Security and Safety.

5.3 Scenarios utilising Simulation Tool

This section describes different scenarios that came up from the use cases of the 3 project’s LLs, where the Simulation Tool will be eventually be utilised. Apart from generating data for the different IoT components of each LL topology and simulates the readings from the actual IoT components the purpose of the Tool is in the future to simulate different scenarios and showcase how can we achieve early detection, diagnosis and mitigations.

In Sections 5.3.1 and 5.3.2 below, 2 different scenarios (relevant to the LLs) are described, where the role of this initial version of Simulation Tool is to generate data for each sensor (or any other IoT component). The final version of the Simulation Tool, will support additional functionalities to showcase how (based on the generated data) can we achieve early detection, diagnosis and mitigations. The final version of the Simulation Tool (including the additional functionalities) is planned to be completed by M24 and will be described in D1.6 “CHARIOT Design Method and support tools (final version)” planned to be submitted in M33.

5.3.1 Building Management Scenario

The Tool can represent the topology of a specific room either in the IBM Campus or in the Athens International Airport, including all the IoT devices along with their parameters (id, name, type, status, etc.) and the connection between them.

Use Case: Detection and mitigation of unsafe Heating Ventilation & Air Conditioning (HVAC) malfunctioning.

Scenario Information: Faults due to malicious acts or due to equipment malfunctioning can have safety implications for HVAC systems. In this use case, the HVAC system of a room in a building is supervised by CHARIOT. This means that the functionings of existing HVAC sensors deployed in the building is monitored and evaluated by CHARIOT engines.
This scenario along with the conditions and events that are happening, is described in the Table below. Moreover, this Table includes the role of the Simulation Tool for each one of these events, along with what it is currently supported and what will be supported by the final version of the Simulation Tool.

### Table 11 – Simulation Tool - Building Management Scenario

<table>
<thead>
<tr>
<th>No</th>
<th>Scenario Steps</th>
<th>Simulation Tool Role</th>
<th>Simulation Tool Supported Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Air temperature sensors (from a particular room area) transmitted values constantly fluctuates between the values of 10 and 40 degrees Celsius.</td>
<td>Simulate (generate) sensor data based on sensor’s upper and lower thresholds</td>
<td>Currently supported</td>
</tr>
<tr>
<td>2</td>
<td>HVAC controller alternates between cooling and heating up the room space.</td>
<td>Simulate (generate) controller’s status data</td>
<td>Currently supported</td>
</tr>
<tr>
<td>3</td>
<td>Due to wide discrepancies between the two temperature ranges the whole HVAC controller malfunctions.</td>
<td>Early detect and malfunction diagnosis</td>
<td>Will be supported by the final version</td>
</tr>
<tr>
<td>4</td>
<td>The ventilation unit stops operating and quickly the office is filled with unsafe levels of carbon dioxide.</td>
<td>Early detect and malfunction diagnosis</td>
<td>Will be supported by the final version</td>
</tr>
<tr>
<td>5</td>
<td>People located in the room are informed to evacuate the room.</td>
<td>Provide a mitigation plan</td>
<td>Will be supported by the final version</td>
</tr>
</tbody>
</table>

### 5.3.2 Rail Management Scenario

The Tool can represent the topology of a train wagon either handled by TRIT, including all the IoT devices (sensors, gateway) and the connection between them. **Use Case:** Detection and mitigation of unsafe communication.

**Scenario Information:** The data traffic between the on-board IoT sensors, installed in the mechanic and electronic equipment of the train, and the Dynamic Maintenance Management System (DMMS) is monitored, supervised and evaluated by CHARIOT engines. An anomalous data communication (i.e. distorted data) due to malicious acts, unauthorized IoT devices or due to equipment malfunctioning can have safety and security implications.

At the same concept as in the previous scenario (section 5.3.1) the Table below describes the conditions and events that are happening, for this “Rail Management” scenario, along with the role of the Simulation Tool and what is currently (and future) supported for each one of these events.

### Table 12– Simulation Tool - Rail Management Scenario

<table>
<thead>
<tr>
<th>No</th>
<th>Scenario Steps</th>
<th>Simulation Tool Role</th>
<th>Simulation Tool Supported Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Triaxial Vibration sensor (located in the rack near the passengers) transmitting values constantly to the DMMS and then to the Fog Server.</td>
<td>Simulate (generate) sensor data based on sensor’s upper and lower thresholds</td>
<td>Currently supported</td>
</tr>
</tbody>
</table>
CHARIOT checks the IoT Communications and collects status reports from the Safety and Privacy Engines.

Due to wide discrepancies between the ranges of the values coming from the Triaxial Vibration sensor, CHARIOT identifies a potential security violation.

The Triaxial Vibration sensor stops operating and the safety of the people located in the train becomes unsafe.

The train stops and the people located on it are informed to evacuate it.

<table>
<thead>
<tr>
<th></th>
<th>lower thresholds</th>
<th>Simulate (generate) status report’s data</th>
<th>Early detect and malfunction diagnosis</th>
<th>Early detect and malfunction diagnosis</th>
<th>Provide a mitigation plan</th>
<th>Will be supported by the final version</th>
<th>Will be supported by the final version</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>CHARIOT checks the IoT Communications and</td>
<td>Currently supported</td>
<td></td>
<td></td>
<td>Will be supported by the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>collects status reports from the Safety</td>
<td></td>
<td>Will be supported by the final version</td>
<td>Will be supported by the final version</td>
<td>final version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and Privacy Engines.</td>
<td></td>
<td>Will be supported by the final version</td>
<td>Will be supported by the final version</td>
<td>final version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Due to wide discrepancies between the</td>
<td>Currently supported</td>
<td></td>
<td></td>
<td>Will be supported by the</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ranges of the values coming from the</td>
<td></td>
<td>Will be supported by the final version</td>
<td>Will be supported by the final version</td>
<td>final version</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Triaxial Vibration sensor, CHARIOT</td>
<td></td>
<td>Will be supported by the final version</td>
<td>Will be supported by the final version</td>
<td>final version</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>The Triaxial Vibration sensor stops</td>
<td>Currently supported</td>
<td></td>
<td></td>
<td>Will be supported by the</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>The train stops and the people located on</td>
<td>Currently supported</td>
<td></td>
<td></td>
<td>final version</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## 5.4 Development

### 5.4.1 Functionalities, technology used and screenshots

As mentioned above, the Simulation Tool is part of the IPSE Dashboard solution and the current version aims to generate data for the IoT topology components of each LL, forward them to the CHARIOT platform and showcase how the real time readings from the sensors can be displayed. Simulation Tools can also be directly integrated with the Northbound Dispatcher and utilise the existing LL topology provided by the Safety Supervision Engine.

Moreover, the Simulation Tool is a web-based solution, that’s why technologies that offers a cross browser and multi device compatibility, like HTML5[^65], CSS3[^66], Bootstrap[^67] and JavaScript[^68] were adopted to support its implementation. JQuery[^69] and JQueryUI[^70] are also used for the general implementation of the user interface and data manipulation.

The Figure below illustrates the main window of the Simulation tool which is separated in 3 layers:

- **Toolbox Layer.** An area with different nodes like IoT (i.e. sensors, gateways, etc.) and other hardware components (i.e. server, workstation, firewall, etc.), along with connectors (wired and wireless) are available to be used.
- **Canvas Layer.** A canvas area where different components can be dragged and dropped in (from the Toolbox Layer), connected between them and represents an IoT topology.
- **Properties and Simulation Results Layer.** An area where the properties and parameters of each node and component (exists in the topology) is presented along with the results of the simulation as listed below:
  - Plain and graphical representation of generated values for each IoT component, based on upper and lower thresholds defined by the user/operator;
  - Privacy, Security, Safety threat vulnerability analysis and risk scoring.

[^65]: https://www.w3schools.com/html/html5_intro.asp
[^66]: https://www.w3schools.com/css/
[^67]: https://getbootstrap.com/
[^68]: https://www.javascript.com/
[^69]: https://jquery.com/
[^70]: https://jqueryui.com/
A large number of IoT devices and other hardware components are currently supported, as listed in the Table below. This list is not limited and can be further expanded based on the project needs. For each of the below IoT devices, the Simulation Tool supports a number of parameters (i.e. model, status, location, etc.). A sample screenshot presenting the parameters of a temperature sensor is shown in the Below figure.

Table 13 - Simulation Tool - IoT and Other Devices Supported

<table>
<thead>
<tr>
<th>No</th>
<th>IoT devices and other hardware components</th>
<th>No</th>
<th>IoT devices and other hardware components</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Room Temperature Sensor</td>
<td>13</td>
<td>Sun Azimuth and Elevation Sensor</td>
</tr>
<tr>
<td>2</td>
<td>Footfall Sensor (Based on video processing data from camera above the doors)</td>
<td>14</td>
<td>Electricity Meter Sensor</td>
</tr>
<tr>
<td>3</td>
<td>PIR (passive infrared) Sensor</td>
<td>15</td>
<td>Gas Meter Sensor</td>
</tr>
<tr>
<td>4</td>
<td>MapUme (Indoor GPS) Sensor</td>
<td>16</td>
<td>Water Meter Sensor</td>
</tr>
<tr>
<td>5</td>
<td>CO2 Sensor</td>
<td>17</td>
<td>Gateway</td>
</tr>
<tr>
<td>6</td>
<td>Brightness Sensor</td>
<td>18</td>
<td>Connections (wired, wireless)</td>
</tr>
<tr>
<td>7</td>
<td>Humidity Sensor</td>
<td>19</td>
<td>Server</td>
</tr>
<tr>
<td>8</td>
<td>Rainfall Sensor</td>
<td>20</td>
<td>Computer/Work Station</td>
</tr>
<tr>
<td>9</td>
<td>Barometric Pressure Sensor</td>
<td>21</td>
<td>Router</td>
</tr>
<tr>
<td>10</td>
<td>Hail Sensor</td>
<td>22</td>
<td>Firewall</td>
</tr>
<tr>
<td>11</td>
<td>Wind Speed Sensor</td>
<td>23</td>
<td>Cloud</td>
</tr>
<tr>
<td>12</td>
<td>Solar Radiation Sensor</td>
<td>24</td>
<td>Database</td>
</tr>
</tbody>
</table>
Based on the HVAC malfunctioning scenario described in Section 5.2.1, the simulation could generate the below results on its runtime execution (Console), as presented in the screenshots of the next two Figures. In the future, and based on the project needs, we might have more types of simulation data presented for an IoT device, but the below (date-time, sensor, value) are mandatory and should be included.
Except from the above, as a result of the simulation we can also have some statistics, like those are presented in the two screenshots of the below Figure showing:

- The inconsistency between the recorder temperature values between the 2 temperature sensors that caused the HVAC malfunctioning.
- The growing levels of the CO2 that caused by the HVAC malfunctioning.
- The reducing operation of the ventilation unit caused by the HVAC malfunctioning.
- The generated data of different sensors (i.e. heat and humidity).
5.4.2 Key benefits and future work

During the design and implementation period of the initial version of the Simulation Tool, all the implementation procedures were followed, starting from the understanding of Project needs, the usability of such a tool and the value added to the Project. An important key benefit of having the Simulation Tool as part of the Project is that it can generate data and forward them to the CHARIOT platform. This will showcase how the Dashboard (implemented under T3.5) displays the real time readings from the sensors (as well as any alerts) and mitigate the risk where the use cases cannot provide data early enough. In case the Simulation Tool were not exist, this risk would affect the implementation and the proof of concept of various IPSE components (i.e. dashboard).

In addition, the Simulation Tool allows a user to design a network in a virtual environment perform changes (disable some sensors or gateways, simulate broken or offline sensors), simulate the behavior of different components and demonstrate what happens.

As part of the continues implementation of the Simulation Tool, additional features will be implemented (as listed below) which will further benefit the Project.

- Performs privacy, security, safety threat vulnerability analysis using multiple methods of assessment such as agent and network-based methods based on existing tools from CORE Project as described in D3.13 “Multi-method Threat and Vulnerability Analysis Suite”
- Utilise these assessment methods to early predict IoT devices anomalies and malfunctions
- Provide a risk value /percentage of something is not behaving as expected. i.e. 30% sensor shows high readings, 50% of causing a fire
- Provide a mitigation plan in order to recommend actions after the completion of the simulation.
• Mechanism to show the single bottleneck. i.e. sensors show high temperature and gives commands to open springless and the springiness are not working then higher percentage of causing fire. Single port of failure are springless. Mitigation plan, have more springless nearby.
6 IoT search index

According to DoA, under subtask 1.4.4 (Development of an interactive web-based IoT Search Index) and 1.4.5 (Continuous update of the Search Index), an interactive web-based Search Index portal has been developed that will contain an index of IoT Threats, Protection Technologies and Governance Models. This portal will be continuously updated (throughout and beyond the lifecycle of the CHARIOT project) with contents/articles.

This Section describes the work has been done (and planned to be done throughout and beyond the lifecycle of the CHARIOT project) for the implementation and continues update of the CHARIOT Search Index. These are listed below in summary:

- Develop an interactive web-based software tool called “IoT Search Index” containing a large library (index) of IoT Threats, Protection Technologies and Governance Models. This tool will follow the standards of a portal in order to be easily used. The software tool will also be used for subsequent architectural and design tasks in WP2 and WP3 and capacity building planning in WP5.
- In align with the findings of the Survey (in Industrial IoT threats for rail, airports and smart buildings) described in Section 3 of the document, identify the major categories to structure and formulate the Search Index content.
- Develop a mechanism where the administrator can continuously (throughout and beyond the lifecycle of the CHARIOT project) enrich the contents of the search index, by adding manually or approve posts automatically imported via Rich Site Summary (RSS).

6.1 Search index development

This section describes in detail the CHARIOT “IoT Search Index” that has been implemented and can be accessed using the following URL www.knowledgeportalcenter.com/chariot. It can also be accessed via of the official CHARIOT website as shown in the below Figure.

Search Index utilizes the latest technology in order to provide to the user/visitor a rich content information through a cross-browser and multi-device compatibility. In addition, the Search Index can be configured, based on the users’ needs in order the content (articles) can be filtered based on user interests.

The “IoT Search Index” aims to provide a web location where publications, articles, and relevant documents can be centralized hosted in a well-structured and easily accessed way. This web solution will also be utilised during the exploitation and dissemination plan of the project (as part of WP5) through the establishment of communications partnerships with appropriate CHARIOT and IoT communities. It will also support the capacity building as an additional resource, by maximizing the usability and impact of the projects’ solutions within European IoT communities and consequently leverage the CHARIOT project results.
6.1.1 Methodology and development technology

The design and implementation of the CHARIOT “IoT Search Index” followed the user interface design principles with focus on how to satisfy various types of users by providing a smooth, easy and nice user experience. Furthermore, the following list highlights the Graphical User Interface (GUI) Design Principles\(^1\) were adapted in the “Search Index” interface design and implementation.

- **Clarity**: The interface is visually, conceptually and linguistically clear
- **Comprehensibility**: The interface is easily understood, friendly and the flow can be easily followed
- **Consistency**: The interface looks, and operates in the same way throughout the portal
- **Control**: The user controls the interaction and actions are performed quickly and capable of interruption or termination. In addition, the user is never interrupted for errors
- **Efficiency**: Minimize user’s eye and hand movements. The transition between the various portal control flows are easily and freely. Also, the navigation paths are as short as possible and ensure that users never lose their work
- **Simplicity**: Provide an interface as simple as possible and make common actions simple at the expense of uncommon actions being made harder. In addition, provide uniformity and consistency.

In order to archive the cross browser and multi device compatibility, during the implementation of portal’s interface, the user interface utilises the latest technologies of HTML5\(^2\), CSS3\(^3\) and JavaScript\(^4\). This means that the user is able to access the content of the portal from a smartphone, tablet, desktop PC or laptop. The above-mentioned technologies are the latest evolution, offering a state-of-the-art user interface with new elements, attributes, and behaviors as highlighted in the list below.

- **Offline and storage**: Allow web-pages to store data locally and operate offline more efficiently
- **Multimedia**: Usability of plug-ins allowing the handling of different multimedia content, such as videos.
- **2D/3D graphics and effects**: Allow the support of a wider range of presentation options
- **Performance and integration**: Provide greater speed optimization, use and take advantage of the computer hardware
- **Device access**: Allow the use and accessing from various type of devices
- **Styling**: Allow authors to write more sophisticated themes

6.1.2 Market research and desired features

This section describes the research on several existing portals that are similar to the “Search Index”, in order to identify the required features, functionalities and design types that needs to be followed during the CHARIOT “IoT Search Index” implementation. A detailed list of the researched portals (along with an access link) can be found in the Annex 1. Existing portals and knowledge bases implemented in previous projects like Skema, CORE, EuTravel and SELIS, have also been explored in order the existing implementations to be reused and expanded in order to support the CHARIOT “IoT Search Index”.

After conducting the above-mentioned research, we have identified the required features to be included in the development of the CHARIOT “IoT Search Index” along with the utilization of existing components implemented for the Knowledge Base of previous projects. A list with these features is listed below:

- **Categorization.** The backbone of the “IoT Search Index” portal is the articles. These articles are categorized and grouped into categories and sub categories. This categorization can be generic in order all the relevant (past and future) projects to be hosted under a single portal, providing ease accessibility to the community.

---


\(^2\) [www.w3schools.com/html/html5_intro.asp](https://www.w3schools.com/html/html5_intro.asp)

\(^3\) [www.w3schools.com/css/css3_intro.asp](https://www.w3schools.com/css/css3_intro.asp)

\(^4\) [www.w3schools.com/js/](https://www.w3schools.com/js/)
• **User Registration.** The user can create/register a new account, by providing a valid email, password, and full name. Upon approval, the user receives an email confirmation and can then login to the portal.

• **Anonymous User.** A user can anonymously access the portal as guest, navigate through it and access articles without being previously registered and logged in.

• **Preferences.** The user can choose which articles will be presented to the portal, based on his selection on preferred categories and sub-categories. These preferences can be stored in the browser’s cookies and be available while navigating through the portal.

• **Page Types and Common UI.** There are mainly three types of pages: Home, Categories (and Sub-Categories) and Articles. Pages are separated into a number of sections (Latest, Most Popular and Sticky Articles) for better structure and presentation purposes.

• **Search.** The user can use portals’ search functionality to search through the entire content of the portal including articles, categories, subcategories and uploaded documents.

• **Administration.** Administrator(s) has access to the admin control panel, and through it can create articles. Additionally, through the control panel Administrator(s) can configure automatic backups of the entire portals’ content.

• **RSS Feeds.** The portal will provide RSS feeds to provide to the users the latest content. RSS feeds are moderated by the Administrator. That means the content coming from the RSS, will be automatically only after the approval by the administrator(s).

• **Cross-Browser and Multi Device Compatibility.** The portal is operating in the same way under the major browsers (Safari, Chrome, Firefox, and Internet Explorer/Edge) without affecting its functionality. In addition, the portal is fully compatible with different type of devices like laptop, tablet, desktop PC and smartphone.

• **Social Media Integration.** Functionality for the user to sharing content (articles) to Social Media Networks (i.e. Twitter and LinkedIn). This generates additional website traffic and enhances the portals’ Search Engine Optimization (SEO) and popularity.

### 6.1.3 Categorization

To structure the “IoT Search Index” and formulate the relevant content based on different topics, an initial two-level categorization has been followed, consisting of a basic set of categories and sub-categories. This categorization will enable an article that is relevant to a particular subject to be located under the appropriate category and sub-category, based on its content. In this way, the major categories and sub-categories are forming the Search Index content. Different elements have been taken into consideration for the identification of this categorization as listed below:

• Project needs as described in DoA.
• The categorization defined in T5.1.2 (Web-based CHARIOT Forum) and described in D5.1 (Creation of a web-based CHARIOT Forum)
• The top-level requirements of the Living Labs.
• The knowledge achieved from previous project (i.e. CORE, SELIS) along with the repository and the knowledge base implemented for these projects.
• The findings of the Survey (in Industrial IoT threats for rail, airports and smart buildings) described in Section 3 of the document.

Annex 2 contains a list with the categories and the related sub-categories as agreed between the consortium partners. This categorization aims to be generic, easily expandable and can support multiple projects apart from CHARIOT.

---

75 https://en.wikipedia.org/wiki/Search_engine_optimization
6.1.4 Front-end initial designs

This section includes the initial mockup designs of the Search Index. As mentioned in above (Section 6.1.3), a two-level categorization has been taken into consideration. Following this concept and in order to provide a simple, easy and user-friendly navigation within the portal, 3 types of pages have been identified. These page types are listed below:

- Welcome or Home Page
- Categories and Subcategories Page
- Article Page

The Figures in Annex 3 shows the mockup designs of these 3-page types. As already mentioned, the Article page is the core of the CHARIOT “IoT Search Index”, that’s why, can be accessed from any of the other page types, as shown on the navigation flow in the below Figure.

![Figure 23 - IoT Search Index – Pages Structure](image)

6.1.5 Front-end implementation

6.1.5.1 Welcome page

The first page of the Search Index is the “Welcome” page, which is separated into sections. The main concept of the “Welcome” page is to well-organize the content (articles) and present them nicely into different sections. The content can be filtered based on user preferences and selections of the user. The “Welcome” page includes a number of different sections (with grouped articles) such as “Latest”, “Most Popular” and “Sicky”, thus providing a clear separation and well-organized structure of the content.

During the implementation, there was a special focus on the design of a responsive portal that can be nicely viewed and ensure an easy and smooth navigation on smaller screens. As shown in the Figure below, the portal is available and can be accessed through other devices than a computer, like a smartphone or tablet.
The first section of the “Welcome” page is a “Search” mechanism, reinforced with an “auto-completion while typing” functionality, as shown on the Figure below. User is able to use “Search” mechanism to search anything within the entire content of the portal, including articles, categories, subcategories and within attached documents.

Upon search, all the results are presented to the user in a well-structured list, as displayed in the Figure below. The search results are listed in an ascending order based on the relevance percentage of matching during the finding process. Each result, when selected, can redirect the user to the relevant article page.
Users will be able to personalize the “Welcome” page (and the preferred articles to be presented) by choosing the “Categories” and “Sub-categories” they are interested in, from a predefine list under “Settings” (marked in the Figure below). When a user assigns a number of preferences through Settings option, only articles related to these preferences are displayed. This is applied not only in the “Welcome” page, but in the entire portal.

In addition, for each selected “Category” or “Subcategory”, the “Welcome” page presents only the latest, most popular and sticky articles. The “Latest Articles” section (as shown in the Figure below) consists of a formatted structured list with the latest articles, in which the newly published articles are presented first. Each article is presented in a box and includes the article title, a short description, along with a main picture (if there is any). The Title is clickable and redirects the user to the specific article page upon selection. The category of each article is highlighted in order to be easily recognized by the user. In addition, it is clickable and upon selection, it redirects the user to the particular category page.
The “Most Popular” and “Sticky” articles follow the same presented concept as the “Latest” articles section. “Most Popular Articles” section, contains a number of articles sorted by the total number of viewings and the “Featured Articles Section” includes the articles that the Administrator has marked as important.
6.1.5.2 Categories page

The “Categories” page follows the terms of concept and design of the “Welcome” page, and has the similar sections (latest, most popular and sticky articles). So, in order to provide a user-friendly design and articles organization, each “Sub-Category” (and its latest articles) is presented in a separated section.

The “Search” functionality is also available in categories page and gives the option to the user to search within the entire content of the portal (including the attached to the articles documents).

Assuming that the user chooses a Category, then he/she is automatically redirected to the specific “Category” page with access on the relevant articles. A screenshot of the “Categories” page is presented in a Figure under Annex 5.

6.1.5.3 Sub-Categories page

The “Sub-Categories” page follows the design and concept the “Categories” page (already explained in the previous section). That’s why the “Sub-Categories” page consists of a number of sections such as “Latest”, “Most Popular”, and “Sticky” articles. Search option is also available here and allows the user to perform a search within the entire content of the Search Index portal. Annex 6 shows how the user interface of the “Sub-Categories” page looks like.

Assuming that the user chooses a “Sub-Category”, he/she is automatically redirected to the specific “Sub-Category” page. The relevant page is then formulated based on the selected sub-category, thus the title changed and gets the name of the sub-category and the presented articles are related to this sub-category. A screenshot from the Sub-Categories Page can be found at Annex 6.

6.1.5.4 Article page

The “Article” page is basically the articles’ presentation page and follows an analogous design as the aforementioned pages. Nevertheless, it is enhanced with some amendments with emphasis in the content of the selected Article. A screenshot of an Articles’ Page can be found at Annex 7.

After choosing an article, the user is redirected to the specific “Article” page which includes the below listed information:

- **Article section.** It contains the article title, article photo, subcategory name, publish date, and the main article content.
- **Attachment list.** It contains all the articles’ attached documents where the user can click and download them.
- **Related Projects.** As already mentioned, the “IoT Search Index” it is designed in such a way, to be easily expanded and support not only CHARIOT, but multiple projects. In related projects area, a list with all the related projects to the article will be presented.
- **Related Articles.** This section is a list with all the related articles. Users are able to click and be redirected to the selected article within the portal.

Through the “Article” page, the Search Index portal provides additional functionalities for the user to:

- Print an article
- Share an article to social networks
- Email an article
- Export and save it locally as a .pdf file
6.2 Continuous update, Maintenance and Impact Maximization

Under this subtask throughout and beyond the lifecycle of the CHARIOT project, the administrator will have the ability to continuously enrich the contents of the search index to provide a one-stop info source for all players in the industrial IoT ecosystem. A connection to Rich Site Summary (RSS) feeds for automatic content updating upon administrator’s reviewing and approval will be performed.

6.2.1 Administration

This section describes the administration site of the CHARIOT IoT Search Index which is only accessible by the Administrator(s). The administration site has been implemented using the Content Management System (CMS)\textsuperscript{76} of eBOS and by utilising existing components designed in other H2020 projects (i.e. the Knowledge Base implemented under SELIS\textsuperscript{77} project). The CMS is a comprehensive web solution that empowers users to create and easily maintain a website, build a strong online presence and deliver huge dissemination results. Moreover, it manages all workflow needs, while allowing the user to manage and customize a website content without any previous IT knowledge. The utilized CMS database engine is powered by the Microsoft SQL Server\textsuperscript{78} and is built on the .NET Framework\textsuperscript{79} and this allows extreme flexibility and expandability based on the user and project needs.

The Figure below presents the welcome page of CMS. This is the main page and it is displayed as soon as the user logins into the CMS. The “Navigation Menu” which exists on the top of the page, helps the user to easily navigate through the CMS. The “Actions Menu” (located on the left-hand side) changes according to the administrators’ selection on the “Navigation Menu”.

---

\textsuperscript{76} https://www.wiseboscms.com
\textsuperscript{77} http://www.selisproject.eu/
\textsuperscript{78} https://en.wikipedia.org/wiki/Microsoft_SQL_Server
\textsuperscript{79} https://en.wikipedia.org/wiki/.NET_Framework
By using the CMS, the administrator can create manage the entire Search Index. Can create a new page, rename or delete an existing one, as well as to change its’ content as shown in the Figures of Annex 8. In addition, the administrator can perform other website management actions like scheduled backups, changing the position of a page, checking the available space. Administrator can also define or modify the structure of the categorization, by managing the different Categories and Subcategories.

### 6.2.2 Content structure

This section describes the Search Index required content structure. This content structure consists of the process needs to be followed by the Administrator(s) using the above-mentioned CMS, along with the fields that needs to be filled-in in order to publish an article/publication into the Search Index portal. These fields along with a description and their type are listed in the Table below.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Article Title</td>
<td>The actual title of the article.</td>
<td>Input Text</td>
</tr>
<tr>
<td>Short Description</td>
<td>A short description of the article which gives an indication of its subject</td>
<td>Input Text</td>
</tr>
<tr>
<td>Entry Date</td>
<td>The article entry date.</td>
<td>Date</td>
</tr>
<tr>
<td>Article Body</td>
<td>The actual content of the article.</td>
<td>Input Text</td>
</tr>
<tr>
<td>Image</td>
<td>An image relevant to the article.</td>
<td>Attachment (.jpg or .png format)</td>
</tr>
<tr>
<td>Attachments</td>
<td>Attachments that are relevant to the article.</td>
<td>Attachment (Image or pdf format type)</td>
</tr>
<tr>
<td>Reference Link</td>
<td>A link that reference to the actual article.</td>
<td>Input Text</td>
</tr>
<tr>
<td>Sticky Article</td>
<td>Mark the article as “Sticky” means that is an important article and will be presented in all portals’ pages.</td>
<td>Checkbox (Yes / No)</td>
</tr>
<tr>
<td>Category</td>
<td>Assign the article to a specific category.</td>
<td>Dropdown with the predefined categories</td>
</tr>
<tr>
<td>Sub-Category</td>
<td>Assign the article to a specific sub-category.</td>
<td>Dropdown with the predefined sub-categories</td>
</tr>
<tr>
<td>Related Projects</td>
<td>Assign the article to project(s).</td>
<td>Checkbox (list with projects)</td>
</tr>
<tr>
<td>Tags</td>
<td>Tags are keywords that apply to the specific article and are used by the system during each time a user search for something.</td>
<td>Input Text</td>
</tr>
<tr>
<td>Author</td>
<td>The actual author of the article.</td>
<td>Input Text</td>
</tr>
</tbody>
</table>

An article can be added into the portal only by the administrator. Apart from the manually addition of articles, the automatically mechanism has been implemented for an automatic content updating. Based on that mechanism, a connection to specific RSSs automatically feeds the Search Index with content. This mechanism is fully moderated. That means in order an article (coming from an RSS) to be added in the portal it requires the reviewing and approval of the Administrator.
6.2.3 Impact Maximization

The Search Index portal does not have the concept of an online forum, so the users are not able to make comments to the articles, but they are able to register and share articles via social media. Since the portal is publicly available and it has no access limitations, even people that are not part of the Consortium could use it. That’s why it needs to stay “alive” during the entire project life cycle. In order to achieve that and as part of the dissemination process, it is essential all the partners to keep using it, share its content over the social media and make it known in the IoT world. To ensure this, the following actions are planned to be taken:

1. An email invitation will be sent to the Consortium members;
2. A live demo will be scheduled to show to people (within the Consortium) of how to use it;
3. Will ensure that all Consortium members have been registered to the Forum. A direct contact will be performed with the partners that have not been registered;
4. The Administrator will ensure the weekly publication of interesting articles;
5. Weekly “what’s new” messages will be sent to partners;
6. Bi-weekly share of an important article in project’s website and social media accounts;
7. A series of touch points (via email campaign) will be created, that tells people why the Forum is important and guides them to use it.
7 Conclusions

This document firstly describes and analyses an extensive survey that has been performed in the Industrial IoT security threats for rail, airports and smart buildings area and some conclusions are highlighted below.

The latest trends in technology come with different challenges as the society embraces new techniques like IoT and cloud computing. Cloud computing offers a new model for processing which in turn improves efficiency, provides on-demand access to the pool of resources being shared. Consequently, IoT offers a platform through which people and devices interconnect, enabling them to seamlessly interact and communicate. A combination of the two paradigms of technology to enable the processing and storage of unlimited amounts of data created by various IoT devices is the next assignment that innovators are considering.

With the new trends in technology, several privacy and security issues have emerged in different sections like airports, railways and smart buildings. Many of the cyber threats come because of the intrinsic nature of IoT, as different IoT devices create the data which involves human beings. Based on the device generating the data, the type of personal data created can be very sensitive to be exposed. Data of that type can be simultaneously collected in an automatic way with the victims being unaware of the process behind the collection of their data. That, in turn, makes it very hard for anyone to offer a clear consent at the time of collecting data. At the same time, data is normally collected in various environments and managed by different signatories. The management of such personal data created in a large amount in different environments can be a great challenge to the users. The companies and individuals tasked with implementing IoT systems face a lot of challenges with regard to preserving privacy and maintaining the security of the data collected. New secure techniques will be used in collecting IoT data from different environments, transfer the data through the internet and lastly get to store the data and have them analyzed over the cloud. Consequently, the new access control mechanisms will have to be applied to make sure that everybody gets informed on the type of data being gathered and allows the user to explicitly give their consent. Additionally, the companies will also have to apply the new services to enable the users to manage their gathered data in a usable, secure and privacy-friendly manner.

Even though there have been several attempts to have IoT secured from both internal and external threats, the success of having it fully deployed is strongly dependent on standardization and depth elaboration of various security protocols. Taking into consideration the heterogeneity and diversity of various IoT devices, applications, and systems, many open security issues stand in different sectors like cryptographic and authentication network protocols, identity and data management, trusted architectures and self-assessment. At the same time, there does not exist any single mechanism of defense which can be used effectively for each area of application and can totally overcome all the threats to security. Nevertheless, even though the IoT applications are different, some of them might share common measures of security and mechanisms of defense against cyber threats.

Of the many ways existing in ensuring privacy and security in IoT systems, one of the major ways is developing and designing a privacy-friendly and secure IoT system. However, a challenge stands on how experts will formulate strategies to mitigate the security threats. The strategies will, in turn, be applied to creating various privacy and security requirements. Ensuring that the requirements are fulfilled will make sure that such threats are abated. Nevertheless, the greatest challenge is designing a system capable of fulfilling all the requirements. With such challenges in mind, there are great chances of research opening up and can be taken up for future projects and scholars interested in the area.

The main concerns that could be summarized from this survey are that today it seems important to take into account the inadequate security culture. Many companies and individuals tend to undermine the issue of cybersecurity. That leaves their employees unaware of the impending danger that they face. However, if the culture of security is implemented in companies, it is very easy to deal with the majority of the threats. Lack of security skills and lack of knowledge present a significant vulnerability which may be exploited by malicious third parties. The security behavior of the managers and employees of authorities and businesses is vital to achieving an adequate level of protection.
An increasing number of devices are connected via the Internet. This provides new opportunities but also increases vulnerability to attacks due to the potential for more rapid spread of security incidents. The ready availability of hacking tools on the Internet means that anyone who wishes to hack a system can do so relatively easily and cheaply. There is also a high dependency on digital infrastructure. Vital digital infrastructure is a precondition for carrying out activities in the public and private sectors. Lack of accessibility, integrity, and confidentiality in digital infrastructure can have significant repercussions for society.

One of the best ways to prevent such attacks is taking extra measures and precautions while performing sensitive operations. That can be attained by applying software inventory tools and whitelisting. Ensuring strong scanning and documentation channels also help prevent cyber threats by a greater deal. There is a need to ensure secure configurations for software and hardware on mobile devices, workstations, laptops as well as servers. That helps in setting a baseline for security which will enable more accurate and better alerting and monitoring. Continuous vulnerability evaluation and remediation confirms the first two controls and prompts for identification and remediation as vulnerabilities become known. There exist several tools that can be used in scanning for vulnerability available. It is advisable that companies scan their networks internally and externally.

Secondly, this document outlines the CHARIOT methodology as an output of sub-task 1.4.2 (‘Consolidated Chariot Design Method’). Rather than a methodology per se, this is a methodological framework that prescribes key high-level activities and tasks. This is necessary, given the very diverse range of IoT technologies, installation methods and targeted industrial systems. Indeed, a methodology intended for IoT in personal healthcare, for example, will likely have very different features, steps and goals to a methodology targeting factory automation (for example, Industry 4.0). The CHARIOT Methodological framework therefore allows its adopters to fit their own methods or techniques within the overall framework context to match the characteristics of specific IoT technologies they use and unique requirements of their industrial domain.

The main tenets of the CHARIOT Methodological framework are as follows:

- A system of systems approach used for modelling and understanding the IoT and Industrial systems, as well as their interdependencies and dynamics.
- A risk-based approach to IoT related safety, security and privacy. IoT introduces new types of risks, very hard to detect or foresee by using conventional system engineering approaches.
- A logical top-down approach that starts with industrial level risks and proceeds to prescribing controls for managing them, both at an architectural level but also at a component level.
- A continuous engineering philosophy. This is essential as it is unlikely that IoT, the Industrial System or their environments will remain static for too long. New threats for example emerge frequently in IoT as well as new technologies. Each of them represents a risk that must be managed. The CHARIOT Platform with its continuous evolution must keep one step ahead of such threats.

A revised version of the CHARIOT methodological framework (v2) will be made available in Month 33, reflecting on experience gained from the development of the CHARIOT Platform and its deployment in the Project’s Living Labs.

Moreover, this document highlights the work has been done for the market research and the implementation of the initial version of a simulation tool in order to benefit the project and support IoT applications modelling, network topology design and IoT data generation. This will showcase how the dashboard displays the real time readings (row data and alerts) from the sensors and mitigate the risk where the use cases cannot provide data early enough. The next version of the Simulation Tool will also perform Privacy, Security, Safety Threat Vulnerability Analysis using multiple methods of assessment such as agent and network-based methods utilizing existing tools from CORE.

Addressing subtask 1.4.4 and 1.4.5, this document describes the web-based Search Index portal that has been implemented containing an index of IoT Threats, Protection Technologies and Governance Models. The results of the survey performed in the Industrial IoT security threats for rail, airports and smart buildings along with the data obtained, helps in the grouping and categorization of the Search Index and it’s continues update with
content. These results will also help on the continuously update of portal’s content, throughout and beyond the lifecycle of the project and also be used for subsequent architectural and design tasks in WP2 and WP3 and capacity building planning in WP5.
8 References


[10] The Internet of Things: A New Path to European Prosperity. https://www.atkearney.com/documents/10192/7125406/The+Internet+of+Things+A+New+Path+to+European+Prosperity.pdf/e5ad6a65-84e5-4c92-b468-200fa4e0b7bc


[31] ENISA. (2017). EU strategies to secure the EU cyber space and critical infrastructure against hackers. Speech by ENISA’s Executive Director, Prof. Dr. Udo Helmbrecht - AECA Round-Table Conference-Luncheon.


9 Bibliography


URVASHI BABARIA Applying DevOps to Improve the Effectiveness and ROI of IoT Testing. www.einfochips.com. MARCH 21, 2018

### Annex 1: Search index research

<table>
<thead>
<tr>
<th>#</th>
<th>Portal</th>
<th>Access Link</th>
<th>#</th>
<th>Portal</th>
<th>Access Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Aplus</td>
<td><a href="http://aplus.com/">http://aplus.com/</a></td>
<td>33</td>
<td>Know All</td>
<td><a href="http://demo.herothemes.com/knowall/?ref=2">http://demo.herothemes.com/knowall/?ref=2</a></td>
</tr>
<tr>
<td>14</td>
<td>Twenty two words</td>
<td><a href="http://twentytwowords.com/">http://twentytwowords.com/</a></td>
<td>34</td>
<td>Know How</td>
<td><a href="http://demo.herothemes.com/#knowhow">http://demo.herothemes.com/#knowhow</a></td>
</tr>
<tr>
<td>15</td>
<td>TechDesk</td>
<td><a href="https://themeforest.net/item/techdesk-responsive-knowledge-basefaq-theme/5564344">https://themeforest.net/item/techdesk-responsive-knowledge-basefaq-theme/5564344</a></td>
<td>35</td>
<td>Buy Base</td>
<td><a href="http://demo.themebeans.com/?theme=Base">http://demo.themebeans.com/?theme=Base</a></td>
</tr>
<tr>
<td>18</td>
<td>Mimosa</td>
<td><a href="http://ap.help.mimosa.co/home">http://ap.help.mimosa.co/home</a></td>
<td>38</td>
<td>Ticketrama</td>
<td><a href="http://preview.themeforest.net/item/ticketrama-wordpress-helpdesk-ticket-">http://preview.themeforest.net/item/ticketrama-wordpress-helpdesk-ticket-</a></td>
</tr>
<tr>
<td>---</td>
<td>-----------------</td>
<td>-----------------------------------</td>
<td>----</td>
<td>----------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>19</td>
<td>ITS Observatory</td>
<td><a href="http://itsobservatory.redhost.dk/">http://itsobservatory.redhost.dk/</a></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Annex 2: IoT search index categorization

<table>
<thead>
<tr>
<th>Categories</th>
<th>Sub-Categories</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sectors and Stakeholders</strong></td>
<td></td>
</tr>
<tr>
<td>Shippers</td>
<td></td>
</tr>
<tr>
<td>Retailers</td>
<td></td>
</tr>
<tr>
<td>Freight Forwarders</td>
<td></td>
</tr>
<tr>
<td>Ports and terminals</td>
<td></td>
</tr>
<tr>
<td>Shipping</td>
<td></td>
</tr>
<tr>
<td>Road Transport</td>
<td></td>
</tr>
<tr>
<td>Airports and Air Transport</td>
<td></td>
</tr>
<tr>
<td>Railway</td>
<td></td>
</tr>
<tr>
<td>Smart Buildings</td>
<td></td>
</tr>
<tr>
<td>Facilities, Warehouses</td>
<td></td>
</tr>
<tr>
<td>Inland waterways</td>
<td></td>
</tr>
<tr>
<td>Multimodal operators</td>
<td></td>
</tr>
<tr>
<td>Custom Authorities</td>
<td></td>
</tr>
<tr>
<td>Trusties and other Intermediary Organizations</td>
<td></td>
</tr>
<tr>
<td>Banks, investors and other funding providers</td>
<td></td>
</tr>
<tr>
<td>Urban and Countryside Logistics</td>
<td></td>
</tr>
<tr>
<td><strong>Collaborative Classification and Models</strong></td>
<td></td>
</tr>
<tr>
<td>Collaborative Planning and Synchronomodality</td>
<td></td>
</tr>
<tr>
<td>Optimisation</td>
<td></td>
</tr>
<tr>
<td>Collaboration Risk and Value Sharing</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Visibility</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Corrective and Preventive actions (CAPA)</td>
<td></td>
</tr>
<tr>
<td>Supply Chain Financing</td>
<td></td>
</tr>
<tr>
<td>Environmental Performance Management</td>
<td></td>
</tr>
<tr>
<td>Business Models</td>
<td></td>
</tr>
<tr>
<td>Contract Management</td>
<td></td>
</tr>
<tr>
<td>Process Improvements and Benchmarking Indexes</td>
<td></td>
</tr>
<tr>
<td>Customs &amp; Regulatory Compliance</td>
<td></td>
</tr>
<tr>
<td><strong>Digitisation Frameworks</strong></td>
<td></td>
</tr>
<tr>
<td>e-Freight</td>
<td></td>
</tr>
<tr>
<td>e-Maritime</td>
<td></td>
</tr>
<tr>
<td>National Single Windows</td>
<td></td>
</tr>
<tr>
<td>Data Pipelines</td>
<td></td>
</tr>
<tr>
<td>Control Towers</td>
<td></td>
</tr>
<tr>
<td>Port Community Systems</td>
<td></td>
</tr>
<tr>
<td><strong>Technologies</strong></td>
<td></td>
</tr>
<tr>
<td>Hybrid S/T Communication and Navigation Platforms</td>
<td></td>
</tr>
<tr>
<td>Physical Internet (PI)</td>
<td></td>
</tr>
<tr>
<td>Business Integration Patterns, Publish-Subscribe</td>
<td></td>
</tr>
<tr>
<td>Public key infrastructure (PKI)</td>
<td></td>
</tr>
<tr>
<td>Cognitive</td>
<td></td>
</tr>
<tr>
<td>Cloud Technologies/Computing, Services Virtualisation</td>
<td></td>
</tr>
<tr>
<td>Agile Deployment, Configuration Management</td>
<td></td>
</tr>
<tr>
<td>Business Applications</td>
<td></td>
</tr>
<tr>
<td>Data Management, Simulation and Dashboards</td>
<td>Data Governance, Integrity, Quality Management and Harmonization</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>Data Fusion</td>
</tr>
<tr>
<td></td>
<td>Event handling</td>
</tr>
<tr>
<td></td>
<td>Simulation</td>
</tr>
<tr>
<td></td>
<td>Statistics and Key Performance Indicators (KPIs)</td>
</tr>
<tr>
<td></td>
<td>Dashboards</td>
</tr>
<tr>
<td>Safety, Security and Privacy Systems</td>
<td>International Organisations</td>
</tr>
<tr>
<td></td>
<td>Safety and Security Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
</tr>
<tr>
<td></td>
<td>Access management</td>
</tr>
<tr>
<td></td>
<td>Information security</td>
</tr>
<tr>
<td></td>
<td>International Organisations</td>
</tr>
<tr>
<td></td>
<td>Safety and Security Assessment</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment and Management</td>
</tr>
<tr>
<td></td>
<td>Coordinated Border Management</td>
</tr>
<tr>
<td></td>
<td>Source Code Analysis</td>
</tr>
<tr>
<td>Supply chain management</td>
<td>Supervision approach</td>
</tr>
<tr>
<td></td>
<td>Risk-Based controls</td>
</tr>
<tr>
<td></td>
<td>Screening and tracking</td>
</tr>
<tr>
<td>Common information objects</td>
<td>Transport service description</td>
</tr>
<tr>
<td></td>
<td>Booking</td>
</tr>
<tr>
<td></td>
<td>Transport status</td>
</tr>
<tr>
<td></td>
<td>Customs Declarations</td>
</tr>
<tr>
<td></td>
<td>Waybills</td>
</tr>
<tr>
<td>Standards</td>
<td>UN/CEFACT</td>
</tr>
<tr>
<td></td>
<td>World Customs Organization (WCO)</td>
</tr>
<tr>
<td></td>
<td>International Organization for Standardization (ISO)</td>
</tr>
<tr>
<td></td>
<td>Good Distribution Practices</td>
</tr>
<tr>
<td>Connectivity</td>
<td>Connectivity Interfaces</td>
</tr>
<tr>
<td></td>
<td>Blockchain</td>
</tr>
<tr>
<td></td>
<td>Bluetooth</td>
</tr>
<tr>
<td></td>
<td>Ethernet / Wired</td>
</tr>
<tr>
<td></td>
<td>Wi-Fi</td>
</tr>
<tr>
<td></td>
<td>Architecture</td>
</tr>
<tr>
<td>Devices</td>
<td>IoT Sensors</td>
</tr>
<tr>
<td></td>
<td>IoT Gateways</td>
</tr>
<tr>
<td></td>
<td>IoT Controllers</td>
</tr>
<tr>
<td></td>
<td>Tracking Sensors</td>
</tr>
<tr>
<td>Computing and Processing</td>
<td>Cloud</td>
</tr>
<tr>
<td></td>
<td>Fog</td>
</tr>
<tr>
<td>Edge</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td></td>
</tr>
<tr>
<td>MIST</td>
<td></td>
</tr>
<tr>
<td>Knowledge Graphs</td>
<td></td>
</tr>
<tr>
<td>Stream Processing</td>
<td></td>
</tr>
<tr>
<td>Machine Learning</td>
<td></td>
</tr>
<tr>
<td>Big Data Management and Analytics</td>
<td></td>
</tr>
</tbody>
</table>
Annex 3: IoT search index mockup designs

- Home Page
- Categories Page
- Subcategories Page
- Article Page
Annex 4: Welcome page screenshots
Annex 5: Category page screenshots
edx IoT Sensors and Devices

The Internet of Things (IoT) is expanding at a rapid rate, and it is becoming increasingly important for professionals to understand what it is, how it works, and how to harness its...

IoT-ready Industrial Controller with Enhanced Data Processing Functions

Hitachi has developed a new IoT-ready industrial controller, the HX Series Hybrid Model. In addition to executing control functions such as sequence control and motion control, this con...

Smart Sensor Technology for the IoT

Internet of Things (IoT) applications - whether for city infrastructures, factories, or wearable devices — use large arrays of sensors collecting data for transmission over the ...

Most Popular Articles

The Power of Low Noise in IoT Smart Sensors
Performance vs. power dissipation; it’s one of the most delicate trade-offs for those who are developing smart sensors for the emerging IoT-based application space. Within the broad ...

An experimental study of a reliable IoT gateway
The Internet of Things (IoT) will include new devices specifically designed for IoT compatibility and systems that are already in place today and operate outside of IoT networks...

An experimental study of a reliable IoT gateway
The Internet of Things (IoT) will include new devices specifically designed for IoT compatibility and systems that are already in place today and operate outside of IoT networks. However, the path...

IoT Sensors

Securing IoT Devices and Traffic between IoT Sensors and Cloud Analytics
It is well documented that IoT devices have introduced new security risks. Most IoT devices must interface to cloud-based management and analytics engines and therefore support a TC...

IoT sensor devices (internet of things devices)
IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled ...

Smart Sensor Technology for the IoT
Internet of Things (IoT) applications - whether for city infrastructures, factories, or wearable devices — use large arrays of sensors collecting data for transmission over the ...

IoT Gateways

IoT Controllers
Annex 6: Sub-category page screenshots

Devices > IoT Sensors

Latest Articles

edx IoT Sensors and Devices
The Internet of Things (IoT) is expanding at a rapid rate, and it is becoming increasingly important for professionals to understand what it is, how it works, and how to harness its ...

IoT sensors devices (internet of things devices)
IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled ...

Introduction to IoT Sensors
The Internet of Things is one of the most important and promising technological topics today. Some market researchers estimate that there are more than 20 billion connected ...

Smart Sensor Technology for the IoT
Internet of Things (IoT) applications - whether for city infrastructures, factories, or wearable devices — use large arrays of sensors collecting data for transmission over the ...

Importance of Sensors in the Internet of Things
Different types of applications require different types of sensors to collect data from environment. This article takes a look at some common IoT sensors, in an Internet of Things (IoT) ecosystem...
Sticky Articles

Securing IoT Devices and Traffic between IoT Sensors and Cloud Analytics
It is well documented that IoT devices have introduced new security risks. Most IoT devices must interface to cloud based management and analytics engines and therefore support a TC...

IoT sensor devices (Internet of things devices)
IoT involves extending internet connectivity beyond standard devices, such as desktops, laptops, smartphones and tablets, to any range of traditionally dumb or non-internet-enabled...

Smart Sensor Technology for the IoT
Internet of Things (IoT) applications - whether for city infrastructures, factories, or wearable devices — use large arrays of sensors collecting data for transmission over the...

Most Popular Articles

Importance of Sensors In the Internet of Things
Different types of applications require different types of sensors to collect data from environment. This article takes a look at some common IoT sensors. In an Internet of Things (IoT) ecosystem...

Securing IoT Devices and Traffic between IoT Sensors and Cloud Analytics
It is well documented that IoT devices have introduced new security risks. Most IoT devices must interface to cloud based management and analytics engines and therefore support a TC...

The Power of Low Noise in IoT Smart Sensors
Performance vs. power dissipation; it’s one of the most delicate trade-offs for those who are developing smart sensors for the emerging IoT-based application space. Within the broad...
Annex 7: Article page screenshots

When it comes to transportation, nothing frustrates passengers more than delays – especially unexpected ones. That’s why railway companies take every advantage possible to maximize their operations and keep customers happy. The key is using the data that you have – or the data that you can easily get – to find new ways to deliver better service. VR Group, the state-owned railway in Finland, turned to analytics and the Internet of Things (IoT) to keep its fleet of 1,500 trains on the rails and provide a better, safer experience for its customers.

In constant operation in all kinds of weather, trains endure harsh conditions. So it’s no surprise that a large portion of VR Group’s operational costs go toward maintenance. To reduce costs and maximize uptime, VR Group wanted to move from a traditional maintenance approach that focused on replacing parts as needed.

“Although we are the only service for passenger railway traffic in Finland, we are certainly competing with other means of transportation,” says Kimmo Soini, Senior Vice President for Maintenance at VR Group. “We also want to ensure our competitiveness when it comes to maintenance, because maintenance costs are included in ticket prices.”
In recent years, VR Group began fitting sensors on various systems and subsystems to monitor symptoms of wear and other failures. But the sensors themselves only collect the raw data. The real benefit comes in analyzing that data, often in real time, to allow engineers to take faster, more appropriate responses. To add this level of intelligence to their operations, VR Group turned to SAS Analytics.

Related Articles

The Internet of Things: A world of opportunity for railroads

The Internet of Things (IoT) is but one of the phrases bandied about to characterize advanced connectivity of devices, systems and services that goes beyond machine-to-machine (M2M) communications. It covers a variety of protocols, domains and applications.

Could data be the rail sector’s most valuable asset?

In an interview with Global Railway Review, Matt Miller, Transportation Industry Principal at CSM, a leading global supplier of application software for operational data management, explains that the analysis and use of data is the rail sector’s most...

Railway Management System Market to reach US$ 64 billion by 2024

According to a new research report by Global Market Insights, Inc. the Railway Management System Market will grow at a CAGR of over 10 per cent between 2018 and 2024. The research shows that the Passenger Information System (PIS) segment has the highest...
Annex 8: Search index administration platform