# IoT4CPS – Trustworthy IoT for CPS

FFG - ICT of the Future
Project No. 863129

# Deliverable D5.1

# Data Models for the IIoT and Industry 4.0, and in the Automotive Sector

**Deliverable number:** D5.1
**Dissemination level:** Public
**Delivery data:** 17. June 2018

**Editor:** Violeta Damjanovic-Behrendt

**Author(s):** Violeta Damjanovic-Behrendt (SRFG)
Michaela Mühlberger (SRFG)
Cristina de Luca (IFAT)
Thomos Christos (IFAT)

**Reviewers:** Heinz Weiskirchner (NOKIA)
Christoph Schmittner (AIT)
Edin Arnautovic (TTTech)

Bundesministerium für Verkehr, Innovation und Technologie

Österreichische Forschungsförderungsgesellschaft

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

The IoT4CPS Consortium:

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

Document Control

| | |
|---|---|
| **Title:** | Data Models for the IIoT and Industry 4.0, and in the Automotive Sector |
| **Type:** | Public |
| **Editor(s):** | Violeta Damjanovic-Behrendt |
| **Author(s):** | Violeta Damjanovic-Behrendt (SRFG), Michaela Mühlberger (SRFG), Cristina de Luca (IFAT), Thomos Christos (IFAT) |
| **Reviewers:** | Heinz Weiskirchner (NOKIA), Christoph Schmittner (AIT), Edin Arnautovic (TTTech) |
| **Doc ID:** | IoT4CPS-D5.1 |

© Copyright 2018, the Members of the IoT4CPS Consortium

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

## Document History

| Version | Date | Author | Description/Comments |
|---|---|---|---|
| V0.0 | 22.03.2018 | Violeta Damjanovic-Behrendt (SRFG) | State-of-the-art in Industry 4.0, CPS, smart CPS, Digital Twin; Standards, models and frameworks in Industry 4.0 (Section 3.1) |
| V0.1 | 22.03.2018 | Michaela Mühlberger (SRFG) | Standards in the automotive sector (Section 3.2) |
| V0.2 | 15.04.2018 | Violeta Damjanovic-Behrendt (SRFG) | A conceptual scenario design, identification of lifecycle phases in the automotive sector, and the creation of initial data collection forms for the Digital Twin demonstrator |
| V0.3 | 10.05.2018 | Violeta Damjanovic-Behrendt (SRFG) | Pre-final version of D5.1 |
| V0.4 | 17.05.2018 | Heinz Weiskirchner (NOKIA) | Quality assurance (QA) of D5.1 |
| V0.5 | 22.05.2018 | Cristina De Luca (IFAT)<br>Thomos Christos (IFAT) | Added: Figures 1 and 2; Table 2 with relevant ongoing EU ECSEL JU projects; Comments on Chapter 3. |
| V0.6 | 28.05.2018 | Cristina De Luca (IFAT), a project coordinator of the SemI40 Innovation Action project “Power Semiconductor and Electronics Manufacturing 4.0” (http://www.semi40.eu/) | We received an excerpt from the *SemI40 project (ECSEL-IA 692466-2, Call 2015-2, Innovation Action) D1.1 “Report on Holistic Concept for Cyber-Physical Production Systems”* as the exchange of know-how between the two projects (IoT4CPS and SemI40). The following sections of SemI40 D1.1 are included in Appendix 1, Appendix 2, and Appendix 3 of this report:<br>• section 5.3 (State of the Art in Security, Safety, Lifecycle Process Standards and Best Practices Guidelines),<br>• section 5.4 (State of the Art in Process Management Standards) and<br>• section 5.5. (State of the Art in Business Process Modelling Languages). |
| V0.7 | 29.05.2018 | Violeta Damjanovic-Behrendt (SRFG) | Resolving comments on D5.1 received from partners (Cristina De Luca, Thomos Christos) and from QA (Heinz Weiskirchner) |
| V0.8 | 29.05.2018 | Violeta Damjanovic-Behrendt (SRFG) | Added a short description of the COSSIM project in Table 1. COSSIM defines an open source CPS simulation framework. |
| V0.9 | 06.06.2018 | Violeta Damjanovic-Behrendt (SRFG) | D5.1 sent for a second round of review |
| V0.10 | 07.06.2018 | Christoph Schmittner (AIT) | Quality assurance (QA) of D5.1 |
| V0.11 | 08.06.2018 | Violeta Damjanovic-Behrendt (SRFG) | Resolving the comments from QA (Christoph Schmittner (AIT)): Section 2.3 addresses the interoperability efforts between RAMI 4.0 and IIRA; IEC 62443 moved from Section 3.2.2 to Section 3.1.2. |
| V0.12 | 13.06.2018 | Edin Arnautovic (TTTech) | Quality assurance (QA) of D5.1 |
| V1.0 | 17.06.2018 | Violeta Damjanovic-Behrendt (SRFG) | Final version of D5.1 published |

## Legal Notices

*The information in this document is subject to change without notice.*
*The Members of the IoT4CPS Consortium make no warranty of any kind with regard to this document, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. The Members of the IoT4CPS Consortium shall not be held liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.*
*The IoT4CPS proje4ct is partially funded by the "ICT of the Future" Program of the FFG and the BMVIT.*

## Abbreviations

| | |
|---|---|
| AE | Application Entity (in oneM2M) |
| AI | Artificial Intelligence |
| AIOTI | Alliance for Internet of Things Innovation |
| AMF | Additive Manufacturing File Format |
| ASIL | Automotive Safety Integrity Level |
| ASME | American Society of Mechanical Engineers |
| BoD | Bill of Disposal |
| BoM | Bill of Materials |
| BoP | Bill of Processes |
| BoS | Bill of Services |
| BPEL | Business Process Execution Language |
| BPM | Business Process Management |
| BPMN | Business Process Modelling Notation |
| BSMD | Bounded Secured Managed Domain |
| BSS | Basic Safety Standard |
| C-ITS | Cooperative Intelligent Transport System |
| CALM | Communication Access for Land Mobiles |
| CBM | Condition Based Maintenance |
| CIM | Computer Integrated Manufacturing |
| CMSD | Core Manufacturing Simulation Data |
| CoAP | Constrained Application Protocol |
| CPPS | Cyber Physical Production System |
| CPSs | Cyber Physical Systems |
| CRM | Customer Relationship Management |
| CSC | Cloud Service Customer |
| CSE | Common Service Entity (in oneM2M) |
| CSP | Cloud Service Provider |
| DCS | Distributed Control Systems |
| DEI | Digitising European Industry |
| DTE | Digital Twin Environment |
| DTI | Digital Twin Instance |
| DTP | Digital Twin Prototype |
| E/E | Electrical and/or Electronic systems |
| ebXML | Electronic Business XML |
| EDDL | Electronic Device Description Language |
| EDI | Electronic Data Interchange |
| ERP | Enterprise Resource Planning |
| FB | Function Blocks |
| FoF | Factories of the Future |
| GCMA | Global Classification and Management of ITS Applications |
| GD&T | General Dimensioning & Tolerances |
| GPS | Geometrical Product Specification |
| HMI | Human Machine Interface |
| I2V | Infrastructure to Vehicle |
| IACS | Industrial Automation Control Systems |
| ICS | Industrial Control System |
| IFC | Industry Foundation Class |
| IIC | Industrial Internet Consortium |
| IIoT | Industrial Internet of Things |
| IIRA | Industrial Internet Reference Architecture |
| IoT | Internet of Things |

| | |
|---|---|
| ISA/IEC | International Society of Automation/ Internat. Electrotechnical Commission |
| ISMS | Information Security Management Systems |
| ISO | International Organization for Standardization |
| IVI | In-Vehicle Information |
| KPI | Key Performance Indicators |
| LDMs | Local Dynamic Map |
| M2M | Machine to Machine |
| MES | Manufacturing Execution Systems |
| MQTT | Message Queue Telemetry Transport |
| NIS | Network and Information Systems |
| NIST | National Institute of Standards and Technologies |
| O-DF | Open Data Format |
| O-MI | Open Messaging Interface |
| O&M | Operation & Maintenance |
| OAGIS | Open Applications Group Integration Specification |
| OMG | Object Management Group |
| OPC UA | OPC Unified Architecture |
| OSA-EAI | Open Systems Architecture for Enterprise Application Integration |
| PDCA | Plan-Do-Check-Act |
| PLC | Programmable Logic Control |
| PLCS | Product Life Cycle Support |
| PLM | Product Lifecycle Management |
| PPMP | Production Performance Management Protocol |
| PPP | Public Private Partnership |
| PRC | Product Representation Compact |
| PRM | Process Reference Model |
| PSL | Process Specification Language |
| RAMI 4.0 | Reference Architecture Model Industrie 4.0 |
| RFID | Radio Frequency Identification |
| RMS | Reconfigurable Manufacturing Systems |
| SCADA | Supervisory Control And Data Acquisition |
| SCC | Supply Chain Council |
| SCM | Supply Chain Management |
| SCOR | Supply Chain Operations Reference |
| SGAM | Smart Grid Architecture Model |
| SIL | Safety Integrity Levels |
| SISO | Simulation Interoperability Standards Organization |
| SysML | Systems Modelling Language |
| TPD | Technical Product Documentation |
| UBL | Unified Business Language |
| V2I | Vehicle to Infrastructure |
| V2X | Vehicle to everything |
| W3C | World Wide Web Consortium |
| WfMC | Workflow Management Coalition |
| WSDL | Web Service Definition Language |
| WSN | Wireless Sensor Networks |
| XPDL | XML Process Definition Language |

# 1. Introduction

The objective of this report is to explore the current state of technology progress that impacts lifecycle data models and methods for data capturing and data management in the Industrial Internet of Things (IIoT) and Industry 4.0, and in the automotive sector. The report overviews a set of the most popular standards and data models with the potential to further enhance ongoing developments in these two sectors. The identified standards and models serve as a basis for the conceptual model of the Digital Twin demonstrator, which will be designed and implemented in a later phase of the project, with the aim to simulate and validate physical processes and their lifecycle phases in domains central to IoT4CPS: Industry 4.0 and Automotive Driving.

This report is organized as follows. Section 1 describes our motivation to explore lifecycle data models supporting new digital manufacturing initiatives across Europe and relying on Industry 4.0 technologies, e.g. Internet of Things (IoT), Cyber Physical Systems (CPSs), Smart CPSs, Smart Data and Smart Factory. Section 2 briefly presents two technical reference architectures: the Reference Architecture Model for Industry 4.0 (RAMI 4.0) and the Industrial Internet Reference Architecture (IIRA), which role is to serve as the technical blueprint for interoperation and standardization in Industry 4.0. Section 3 overviews standards and recommendations for Industry 4.0, including Smart Manufacturing standards related to product development, production system, business process and supply chain lifecycle phases; automotive standards for Intelligent Transport Systems and their functional safety, and the oneM2M open standard for IoT interoperation. In addition to a set of related standards explored in IoT4CPS, we received an additional overview of standards as the **exchange of know-how between IoT4CPS and the European SemI40 project** (ECSEL-IA 692466-2, Call 2015-2, Innovation Action) and SemI40 D1.1 "Report on Holistic Concept for Cyber-Physical Production Systems". The know-how transfer includes the following state-of-the-art sections presented in Appendix 1, Appendix 2, and Appendix 3 of this report, respectively:

- Appendix 1: State of the Art in Security, Safety, Lifecycle Process Standards and Best Practices Guidelines (c.f. SemI40 D1.1, Section 5.3);
- Appendix 2: State of the Art in Process Management Standards (c.f. SemI40 D1.1, Section 5.4);
- Appendix 3: State of the Art in Business Process Modelling Languages (c.f. SemI40 D1.1, Section 5.5).

Section 4 presents an exemplary scenario created to capture lifecycle data models in the automotive industry. The scenario firstly identifies assets in the automotive sector. Secondly, we model assets and create lifecycle data models (note Appendix 4 and Appendix 5 contain data lifecycle models related to production phases (e.g. design, operation and maintenance) and product data, respectively). Section 5 concludes the report.

## 1.1 Motivation

In April 2016, the European Commission presented a set of measures to support the digitization of industry across multiple domains. These measures are known as the **Digitising European Industry (DEI) initiative** and include a set of national and international initiatives and standards, reference architectures and interaction protocols designed to support and interconnect the digital industrial platforms of the future [ECDSM16] (see Figure 1 and Figure 2). The DEI initiative emphasizes the need of the future digitized platform infrastructures to interact with each other and be trustworthy, i.e. to present high degree of trade-offs between safety, security and availability, as well as monitoring and supervision capabilities in run-time.

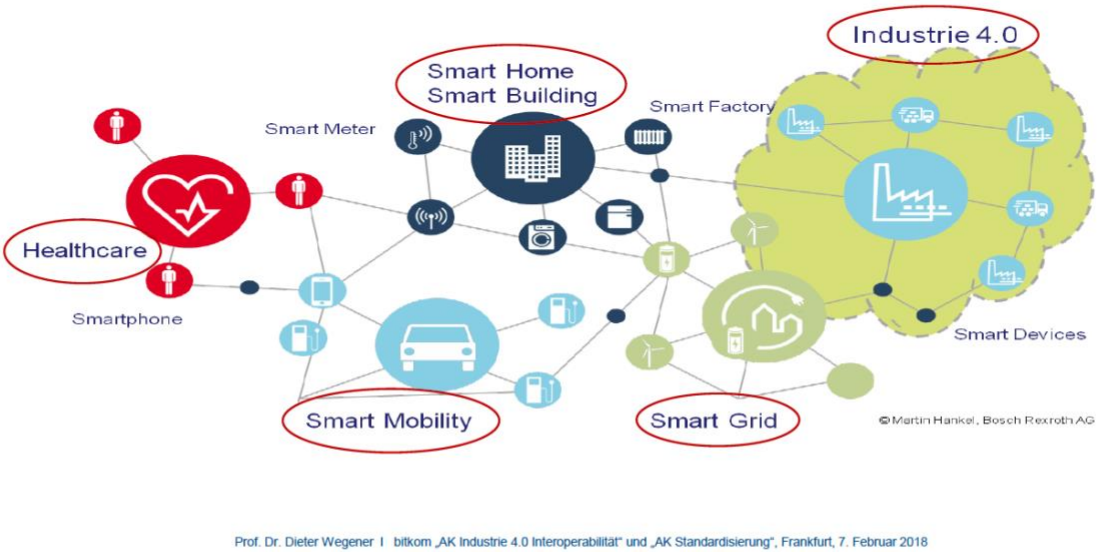



**Figure 1.** Building a connected world through digital economy (source: [WEGE17]).

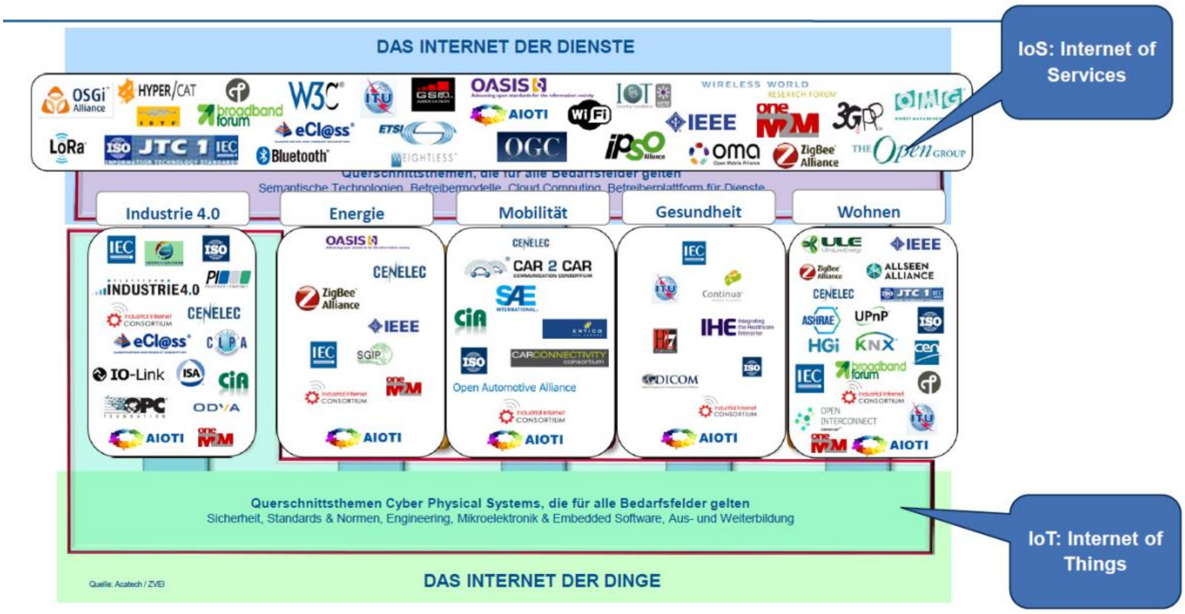



**Figure 2.** Standardization landscape (source: [WEGE17]).

The focus of work package WP5 in IoT4CPS, is to design and implement a digital monitoring and decision-making demonstrator for the validation of the IoT4CPS tools in Industry 4.0 and Automotive Driving domains. With respect to the DEI initiative, the main aim of WP5 is to design an open source demonstrator that could be interfaced with the European industrial platforms of the future. The design and development of such a demonstrator (**IoT4CPS Digital Twin** in the rest of the document) is expected to deliver scientifically relevant results and industry focused solutions.

This report overviews the existing lifecycle data models, standards and initiatives in two domains of interest. To identify components and services that are of relevance for the IoT4CPS Digital Twin, this report explores a set of existing digital platforms and experimentation testbeds that are developed (or are currently under the development) under the EU programmes: IoT-01-2016, FoF-11-2016 (Factories of the Future (FoF)) on Digital Automation, and EU H2020 ECSEL JU projects (Electronics Components and Systems for European Leadership/ Joint Undertaking) which address capabilities of essential systemic and strategic importance in Europe). The design and development of the IoT4CPS Digital Twin include two use case-based validation environments, and will be tested within complex industrial regulatory environments incorporating sectoral governance models, security policies, GDPR (General Data Protection Regulation), and other guidelines, e.g. Article 29 Data Protection Working

Party: WP29 Guidelines on Automated Individual Decision-Making and Profiling for the Purpose of Regulation 2016/679, that has been revised and adopted in February 2018.

## 1.2 Industry 4.0 Enabling Technologies

The Industry 4.0 term is coined by “Industrie 4.0” Working Group and “Plattform Industrie 4.0” initiative. It is “*a collective term for technologies and concepts of value chain organization*” [HEPO15]. Over the course of time, the concept of Industry 4.0 has evolved from mass production to mass customization, dynamic supply networks, adaptive workspaces and economy based on self-reconfiguring machines, predictive maintenance, etc. The authors in [PEAA18] propose the following technology classification scheme for Industry 4.0, including features that characterize Industry 4.0: virtualization/ digitization, interoperability/ network collaboration, automatization/ decentralization, real-time availability/ remote monitoring and mobility, flexibility/ mass-customization, service orientation/ service sharing, and energy efficiency;

The core technologies of the Industry 4.0 include:

- **CPSs technologies** such as Machine to Machine (M2M), embedded systems, Mobile Computing, Communication Interfaces, Manufacturing Execution Systems (MES), Monitoring Application, Multidimensional data correlation, Smart Analytics, Clustering for similarity in data mining, standards for data transfer, standards in security procedures, cybersecurity, telecommunications and the cloud, etc.
- **IoT technologies** such as sensors, RFID, mobile technologies, actuators, smart phones, standardized software, hardware interfaces, smart objects, smart networks, data acquisition systems, connecting the machines and equipment to suppliers, smart and sensor-based human-machine interfaces, ubiquitous computing, crowdsourcing, etc.
- **Smart Data technologies** such as Cloud Computing, Big Data, storing and analysing data, traceability and conditions of devices, simulation models, production status, energy consumption behaviour, customer orders and feedback suppliers’ data, sensor data, etc.
- **Smart Factory technologies** such as Smart Product, Smart Logistics, Smart Machines, Smart Devices and Processes, decentralized intelligence, self-optimization and reconfiguration machines, automatic solutions, adjusted production schedules, optimized capacity, 3D-printing, autonomous vehicle, small and autonomous manufacturing cells, self-organizing, adaptive logistics, complex and intertwined manufacturing networks, transparency and traceability of the products during lifecycle, and more.

**CPSs.** The first Industry 4.0 reference model is presented in [KAWJ13]. It introduces the CPS as the key technology for Industry 4.0, and enhances traditional production processes by adding intelligence to them [LEE08] [LEBK15][JAZD14]. CPS integrates computational paradigms with the physical processes [LEE08], and creates capabilities of the intelligent manufacturing systems, such as reliability, self-organizations, self-repair, predictability, interoperability and tracking [MONO14]. A comprehensive review of the existing middleware solutions for integrating heterogeneous computing and communication devices and for supporting interoperability within the diverse applications and services is given in [RMJP16]. It addresses middleware for Wireless Sensor Networks (WSN), RF identification (RFID), M2M, and Supervisory Control And Data Acquisition (SCADA). Monostori defined the concept of **Cyber Physical Production System (CPPS)** as a group of “autonomous and cooperative elements and subsystems that are getting into connection with each other in situation dependent ways, on and across all levels of production, from processes through machines up to production and logistics networks” [MONO14].

**Smart CPSs.** Smart CPSs are complex engineering systems built to support reasoning, learning, adapting, and evolving of the systems. To fully exploit the potentials of CPSs and IoT, advanced data models should be employed, such as ontologies, that represent semantic and formal conceptualizations of concepts in a domain [GAFN15]. The semantic data management for the development and continuous reconfiguration of smart products and Digital Twins is explored in [ABGD16]. The authors in [TAHO18] analyse the current understanding and state of advancement in designing smart CPSs for run-time, in the context of advanced manufacturing systems. Smart CPSs belong to the category of complex and non-linear systems, with a set of features designed to provide reasoning capabilities and the adaptation freedom of systems. For example, the authors in [TAHO18] introduce four levels of CPSs, i.e. (1) the CPS that is designed to support conventional control mechanisms and can regulate parameters to a known degree, (2) the CPS that is designed to support alternative known modes of control and to select the optimal mode of control during run-time, (3) the self-learning CPS with the ability to adapt predefined control algorithms during the exploitation period, and (4) the CPS with largely unknown changes.

**Twin.** The concept of *twins* was firstly used in NASA's Apollo program for building two identical space vehicles: the one to be sent in space, and the other one to mirror the conditions and performances of the vehicle in space, during the flight mission [BORO16]. The twin concept has been used in aircraft industries as a core for the optimization and validation technology of aircraft systems based on the integration of sensor data, historical maintenance data and other available historical/fleet data [SHAF10][SHAF12].

**Digital Twin.** The term Digital Twin has been created by M. Grieves in 2002 and has evolved over time from "conceptual ideal for PLM (Product Lifecycle Management)", "the mirrored space model", "the information mirroring model", up to nowadays concept of the Digital Twin. Practically, the term Digital Twin is in wide use from 2011, defined as "a set of virtual information constructs that fully describes a potential or actual physical manufactured product from the micro atomic level to the macro geometrical level'' [GRIE14][GRVI17]. The evolution of ''microchip, sensor and IT technologies'' opened the way for the creation of smart products that can track product models along their lifecycle phases, merge and analyse the acquired sensor data and communicate their production and operating conditions [ABGD16][SAMW17]. Such technology evolution shifted the concept of twins from the aerospace industry into Industry 4.0 [RHOM15], ensuring information exchange throughout the entire manufacturing lifecycle phases [ABGD16][ROWL15], virtualization of manufacturing systems [SCRO16], decision support and system behaviour-based predictions [KRAF16], as some of the major features of the Digital Twin.

The full overview of the Digital Twin definitions from the literature is given in [NEFM17], defining the Digital Twin as a "product digital counterpart of a physical product" [RHOM15] that is used for its simulation in a virtual world to predict future states of the system" [GABK16]. The Digital Twin need to be supported by a proper data model that structures information about the system design, production, operation, its history, its behaviour and current state. Finally, the following types of the Digital Twin can be currently find in the literature [GRVI17]:

- Digital Twin Prototype (DTP): it includes information related to requirements of a physical object, its 3D model, Bill of Materials (BoM) and material specification, Bill of Processes (BoP), Bill of Services (BoS) and Bill of Disposal (BoD);
- Digital Twin Instance (DTI): it includes information such as 3D model with General Dimensioning & Tolerances (GD&T) describing geometry of the physical object and its components, a BoM that lists the object's components, a BoP that lists operations performed on the object an Industrial Internet of Things d related measurements, operational states captured from sensor data;
- Digital Twin Environment (DTE): it enables operations on the Digital Twin to support either prediction of the future behaviour and performances, or interrogation for the histories and data correlation.

## 1.3 Industry 4.0 and Automotive Driving Technologies

Industry 4.0 (or Smart Manufacturing) has evolved from the following concepts: the Computer Integrated Manufacturing (CIM) in the 1980's, the Reconfigurable Manufacturing Systems (RMS) [KHJM99][KOSH10], the Smart Factory initiative based on the IoT and embedded intelligence [ZUEH10], the Ubiquitous Factory concept and its reference architecture encompassing the following four layers: the shop floor, the application system, the information infrastructure, and the lifecycle layer [YOSS12].

The role of IoT in Industry 4.0 is to create and collect real-time sensor data that can be exchanged through the Internet [SABA00]. As such, IoT can be used to control sensor devices remotely and across network infrastructures, which results in higher efficiency and accuracy of industrial systems. Edge, fog and cloud computing technologies enable the analysis and correlation of data; Artificial Intelligence (AI) technologies enable data mining and the creation of added value through knowledge discovery, while Big Data technologies provide systematic analyses of a variety of data generated along the entire product lifecycle (product design, manufacturing, testing, operation, maintenance, disposal), supporting a rapid decision making and improving productivity of manufacturing systems [DEPB12][LEKY14].

Manufacturing models based on CPS can be classified into the following groups:

- the Lee's 5C CPS conceptual architecture for industry 4.0 manufacturing systems, which supports plug & play smart connection. The 5C CPS architecture provides smart analytics for subsystem health; enables Digital Twin model for components and machines; adds cognition for decision making, and self-configuration for resilience. It is composed of five layers: (i) smart connection, (ii) data-to-information conversation, (iii) cyber, (iv) cognition, and (v) configuration layers [LEE15];
- the Virtual Engineering Object/Virtual Engineering Process (VEO/VEP) conceptual architecture presented in [SSST15] that can be considered as a predecessor of the Digital Twin concept, in which the manufacturing system is associated to its virtual representation and all real objects have their virtual counterpart in a virtual environment;
- the integration of cloud computing technologies into the 5C CPS's cyber layer, ensuring the scalability of storage, computation, and cross domain communication capabilities [ALSA17].

According to the literature review exploring the availability of simulations and simulation tools for the Digital Twin in Industry 4.0 sector (see [NEFM17], Table 2), simulations are mainly focused on complex behaviour of production or data exchange simulation, while simulations tools in manufacturing are currently not available. The authors in [HAAN18] define the Digital Twin as a comprehensive digital representation of an individual product, its properties, condition and behaviour. Its core functionality is to support design tasks and/or to validate system properties through the multi-domain and multi-level simulations along all lifecycle phases, including operation support [BORO16]. In other industrial practices, the Digital Twins are built to increase the manufacturing flexibility and competitiveness, improve the product design performance, forecasting the health and performance of smart products over lifetime (i.e. Predix by GE), improving efficiency and quality in manufacturing (i.e. Simcenter 3D by Siemens) or enabling synchronous data transmission between the product and the factory (i.e. Tesla) [SAMW17].

In Automotive Driving, the Digital Twins are defined as a life management and certification paradigm that incorporates models and simulations consisting of as-built vehicle states, loads and environments, and vehicle-specific history data [HOLN17]. The authors in [REMM13] look at the Digital Twin as a simulation that integrates an on-board health management system, maintenance history, historical vehicle and fleet data. Here, Digital Twin can mirror the entire lifecycle of a specific physical device, enabling significant gains in its safety and reliability.

# 2. Reference Models for Industry 4.0

There exist two reference models designed as a technology blueprint for interoperation and standardization in Industry 4.0. These are the Reference Architecture Model for Industry 4.0 (RAMI 4.0) and the Industrial Internet Reference Architecture (IIRA).

## 2.1 Reference Architecture Model for Industry 4.0 (RAMI 4.0)

The RAMI 4.0 is based on the Smart Grid Architecture Model (SGAM). Figure 3 illustrates the RAMI 4.0 architecture that is defined in a three-dimensional space. The first horizontal axis of the RAMI 4.0 architecture represents the value chain and the lifecycle, the second horizontal axis represents the different hierarchies of a production system (i.e. products, field devices, control devices, station, work centres, enterprise, connected world), and the vertical axis contains the following six layers: (1) physical world (asset), (2) integration of software and hardware components, (3) communication capabilities, (4) information creation through data, (5) functional properties and (6) business processes [RAMI4.0].

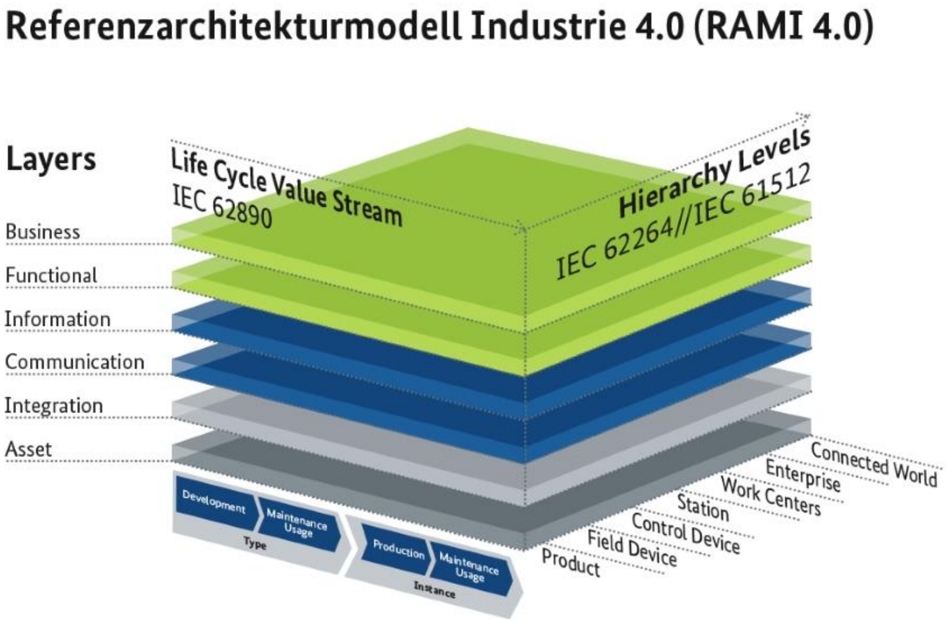



**Figure 3.** RAMI 4.0 Reference Architecture, source: [RAMI4.0]

## 2.2 Industrial Internet Reference Architecture (IIRA)

The Industrial Internet Consortium created the IIRA architecture model, based on ISO/IEC/IEEE 42010:2011 standard [IIRA17]. The IIRA has a focus on various perspectives (business, usage, functional and implementation viewpoints) of various stakeholders acting in the system, i.e. users, operators, owners, vendors, developers and the technician who maintain the system. Figure 4 illustrates the five functional domains defined in IIRA: control, operation, information, application and business domains, which are compared against system characteristics (e.g. safety, security, privacy, resilience, scalability, reliability) and cross-cutting functions (e.g. connectivity, distributed data management, industrial analytics, intelligent and resilient control).

In sum, all Industry 4.0 technical systems should be designed and implemented by referring on RAMI 4.0 and IIRA reference architectures.

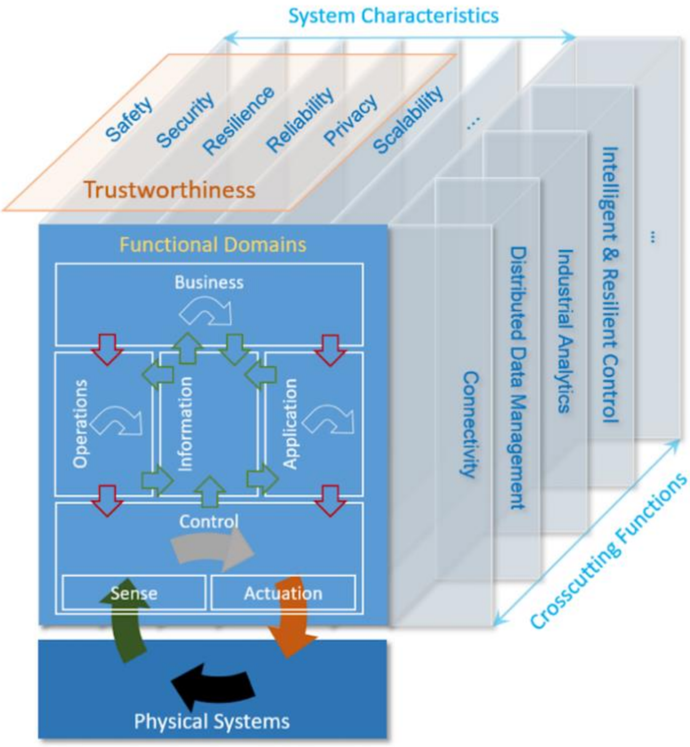



**Figure 4.** IIRA - Functional Domains, Crosscutting Functions and System Characteristics [IIRA17]

## 2.3 Interoperability Between RAMI 4.0 and IIRA

In a recent joint whitepaper by the Industrial Internet Consortium (IIC) and the Plattform Industrie 4.0 [IIRA-RAMI17], the authors conclude that the two architectures have good complementarity: while IIRA has a broader scope, RAMI is deeper when it comes to IoT in manufacturing and to shop-floor connectivity. The whitepaper shows a sound foundation for these two organizations to further collaborate to enrich each reference architecture and to further drive interoperability of IIoT systems. The following quote from the whitepaper illustrates the current understanding (p14).

> *"**CORRESPONDENCE BETWEEN IICF AND RAMI 4.0 COMMUNICATION LAYER***
>
> *To enable interoperability in one or cross industry domains, IIC and Plattform Industrie 4.0 understand the need to harmonize and improve the connectivity standard(s) including the lingua franca for IIoT.*
> *In the manufacturing environment, RAMI 4.0 specifies OPC UA as the core connectivity standard (using the IICF terminology) for connecting manufacturing product, equipment and process software. Furthermore, RAMI4.0 specifies TCP/UDP/IP communication with a possible future extension to TSN and 5G.*
> *In IICF there are 4 core standards specified. One of them is OPC UA for manufacturing. Additionally, TCP/UDP/IP, TSN and wireless technologies are described in IICF.*
> *This common ground is a good starting point for the collaboration between IIC and Plattform Industrie 4.0."*

In the future, this collaboration will focus on (i) addressing the semantic interoperability between the two models and (ii) leveraging data analytics (from IIRA for RAMI 4.0) and Industrie 4.0 components (from RAMI 4.0 for smart components and devices in IIRA) [IIRA-RAMI17].

# 3. Overview of Standards and Recommendations for Industry 4.0

This Section summarizes sets of existing and emerging standards, recommendations and initiatives in the two sectors of interest in IoT4CPS: Industry 4.0 and Automotive Driving. It underlines the importance of using standards, which enables clear interfaces, allows for system functionalities to be reused, reduces complexity and increases productivity.

## 3.1 Industry 4.0 Standards and Recommendations

Industry 4.0 extends the traditional business and manufacturing models and enables easier integration of smart products and their corresponding smart Supply Chain Management (SCM). In 2016, the EU H2020 FoF-11-2016 programme emphasized the need for adopting advanced value- and supply chain-centric communication and collaboration schemes for manufacturing and logistics, enabling machine, human and organizational aspects to be merged and supporting higher integration of SMEs into production supply chains. The FoF-11-2016 funded projects exploit CPS, IoT, cloud computing, robotics, Machine-to-Machine (M2M) communication, modelling and simulation, AI, data analytics, as well as security by design. Hence, in the rest of this section we firstly identify relevant and ongoing FoF-11-2016 projects (Table 1). Secondly, we identify relevant EU H2020 ECSEL JU projects (Table 2).

**Table 1. Relevant ongoing EU H2020 FoF-11-2016 research and innovation action projects**

| Project name and URL | Project short description |
|---|---|
| **MAYA**<br>The Future of Manufacturing<br>URL: http://www.maya-euproject.com/ | The MAYA project aims at developing a plant Digital Twin to support activities along all factory lifecycle phases: from the design, through the optimization of the operational life, to the dismissal phase. |
| **Deadalus**<br>(Distributed control and simulAtion platform to support an Ecosystem of DigitAL aUtomation developerS)<br>URL:<br>https://cordis.europa.eu/project/rcn/205469_en.html | It delivers distributed control and simulation capabilities to support an ecosystem of digital automation developers. It is based on the CPS concept of virtualized intelligence, fostering the creation of a Digital Ecosystem that goes beyond the current limits of manufacturing control systems. |
| **vf-OS**<br>(Virtual Factory Open Operating System)<br>URL:<br>https://cordis.europa.eu/project/rcn/205550_en.html<br>http://www.vf-os.eu/ | It implements the Virtual Factory Platform that includes the manufacturing Virtual Store (vf-Store), integrated factory assets and legacy systems, integration and processing of data sources, an application for optimisation of communication and collaboration among supply chain networks, and an Open Applications Development Kit for integrating external industrial platforms. |
| **COMPOSITION**<br>(Ecosystem for Collaborative Manufacturing Processes – Intra- and Interfactory Integration and Automation)<br>URL:<br>https://cordis.europa.eu/project/rcn/205593_en.html | COMPOSITION develops a data sharing ecosystem supporting the connection of data and services between factories and their suppliers and supporting the optimization of the manufacturing and logistics processes and decision-making. It extends the existing FI-WARE and FITMAN catalogues and LINKSmart® Middleware and adapts the concept of Industrial Data Space (IDS). |
| **DIGICOR**<br>(Decentralised Agile Coordination Across Supply Chains)<br>URL:<br>https://www.digicor-project.eu/ | DIGICOR develops a collaboration platform, tools, and services for the setup and coordination of production networks for planning and control of the collaborative production, logistics and risk management. The platform allows manufacturing companies and service providers to |

| | |
|---|---|
| | create and operate collaborative networks across the value chain. |
| **DISRUPT**<br>(Decentralised architectures for optimised operations via virtualised processes and manufacturing ecosystem collaboration)<br>URL: http://disrupt-project.eu/ | The DISRUPT platform facilitates data collection, orchestration and analytics to handle disruptions across complex manufacturing ecosystems at critical time scales. Within DISRUPT, the data collected is analysed to detect complex events that trigger automated actions. |
| **FAR-EDGE**<br>(Factory Automation Edge Computing Operating System Reference Implementation)<br>URL: https://cordis.europa.eu/project/rcn/205577_en.html | It develops a factory automation platform based on edge computing architectures and IoT/CPS technologies. It aims to provide a reference implementation of emerging standard-based solutions for industrial automation, along with simulation services for validating automation architectures and production scheduling scenarios. |
| **COSSIM**<br>(A Novel, Comprehensible, Ultra-Fast, Security-Aware CPS Simulator)<br>URL: http://www.cossim.org/ | COSSIM provides an open-source framework for simulating the networking and the processing parts of the CPS, performing the simulations, providing analytics on power consumption and security of the CPS. |

**Table 2. Relevant ongoing EU H2020 ECSEL JU projects**

| **Project name and URL** | **Project short description** |
|---|---|
| **PRODUCTIVE4.0**<br>Productive 4.0 is an European co-funded innovation and lighthouse program<br>URL: http://productive40.eu/ | Productive4.0 tackles theoretical and conceptual approaches in the field of Industry 4.0 (Digital Industry). Its focus is on practical implementations involving pilots, test beds, zones of full scale testing in all industries in Europe. The reference implementations such as 3D printer farms, customized production or self-learning robot systems will benefit from specific technological and conceptual approaches in fields like service-oriented architecture (SOA), IOT components & infrastructures, process virtualisation or standardisation.<br>The implementation focuses on the three pillars: digital production (DP), supply chain networks (SCN) and the entire product lifecycle management (PLM). |
| **SemI40**<br>Power semiconductor and electronics manufacturing 4.0<br>URL: http://www.semi40.eu/ | Competitive production in Europe will be leveraged by a well-focused approach of automation and smart production system integration in the domains of technologies, tools and methodologies which are complemented by innovations in the area of secure communication, knowledge management, automated decision-making and smart production execution. The technological challenges in order to link the digital with the real world, new technologies and solutions, new standards, are not fully understood and developed. Hence, the SemI40 project will demonstrate how to apply these new technologies and solutions in real Industrial use cases. Technical and socio-economic impact is also an essential aspect assessing the smart factory technologies. |

Table 3 summarizes other international Industry 4.0 projects, initiatives and coalitions with relevance to the IoT4CPS project.

**Table 3. Other projects, initiatives and coalitions related to Industry 4.0 sector.**

| **Project name and URL** | **Project short description** |
|---|---|
| **FIWARE for Industry**<br>URL: http://www.fiware4industry.com/ | FIWARE for Industry is the European community and two-sided digital platform that emerged from the FITMAN EU project (Future Internet Technologies for MANufacturing industries; see www.fitman-fi.eu). It offers manufacturing industry its FIWARE-enabled reference implementations of Industry 4.0 business processes. |
| **Open Platform for Smart Manufacturing**<br>URL:<br>https://smartmanufacturingcoalition.org/open-platform-smart-manufacturing | It supports real-time, high value applications for manufacturers to optimize production systems and value chains. The major R&D challenges include technical integration and cross industry collaboration, and CPS intelligence addressing dynamic Supply Chain intelligence, physical and performance intelligence and metrics. |
| **AIOTI (Alliance for Internet of Things Innovation) Working Group WG11: Smart Manufacturing**<br>The report is available from [AIOTI15]<br><br>URL: https://aioti.eu/aioti-w11-report-on-smart-manufacturing/ | Created by the EU, AIOTI provides an overview of European research and demonstration activities in the field of digital manufacturing. At EU level, Smart Manufacturing is addressed in the FoF Public Private Partnership (PPP), ARTEMIS/ESCEL domain (Electronic Components and Systems for European Leadership; see: http://www.ecsel.eu/), the IERC cluster (European Research Cluster on the Internet of Things; see: http://www.internet-of-things-research.eu/) and the Digital Business Innovation Community. |
| **OPC-UA**<br><br>URL: https://opcfoundation.org/ | The OPC Foundation originally developed standards that allow device providers to integrate their products into a Microsoft-based platform. OPC Foundation has evolved into an independent standards organization with its own certification and testing program [NIST-8107]. |
| **MTConnect** | MTConnect is an open-source, read-only, extensible data-exchange standard for manufacturing, originally designed to transform process-related information from proprietary to structured-XML formats accessible for monitoring applications [MTConnect-1] [MTConnect-2]. The standard is based on HTTP and provides information models and communication protocols for enhancing the data-acquisition capabilities of manufacturing equipment, systems, and applications and enabling a plug-and-play environment. It includes four information models: Devices, Streams, Assets, and Errors. These models represent common vocabulary and structure for manufacturing equipment data. |

Despite the ongoing EU projects and international Industry 4.0 initiatives and coalitions, there exist other standards and initiatives in the IIoT field, including those with the potential to provide platform interoperability at data and model levels, and to support data aggregation, processing, managing and storing the data from heterogeneous data sources. In sum, the standards around IIoT can be classified according to their applicability level (see: http://www.inter-iot-project.eu/approach):

- at the device level, providing seamless inclusion of novel IoT devices and their interoperation with existing, heterogeneous devices (objects);
- at the networking level, providing seamless support for smart objects mobility and information routing;

- at the middleware level, providing seamless service discovery and management system for smart objects and their basic services;
- at the application service level, providing reuse and exchange (import/export) of heterogeneous services between different IoT platforms;
- at the data and semantics level, providing common interpretation of data and information based on global shared ontology in order to achieve semantic interoperability;
- at the integrated IoT platform level, providing rapid prototyping of cross-platform IoT applications;
- at the business level, providing faster introduction of IoT technology and applications across multiple application domains.

Several European and international IoT research projects have emphasized a strong need for the semantic interoperability at data level. Standard development organizations such as W3C (World Wide Web Consortium), oneM2M, and AIOTI WG3 design standards to boost the acceptance and adoption of semantic technologies by the IoT-based platforms. Another set of references comes from Platform 4.0 (RAMI 4.0) and IIC (Industrial Internet Consortium) (IIRA 2.0 Reference Architectures). In addition, we looked at the existing communication protocols such as Production Performance Management Protocol (PPMP) which is a basis for the Industry 4.0 platform from BOSCH, and the cloud OPC-UA (OPC Unified Architecture) communication standard that is exploited by the MINDSPHERE platform from SIEMENS.

Finally, the National Institute of Standards and Technologies (NIST) organization differs among the following three major groups of Smart Manufacturing standards [NIST-8107]:

- Product development lifecycle,
- Production system lifecycle, and
- Business processes and supply chain lifecycle.

### 3.1.1. Product Development Lifecycle Standards

Standards related to the product development lifecycle enhance modelling accuracy and reduce product innovation cycles. These standards can be classified into the following five categories (for detailed overview of standards see [NIST-8107]):

- **Modelling Practice**, e.g. standards that define symbols and rules for dimensioning and tolerance, or standards for printed boards and assemblies:
    - **ASME** (American Society of Mechanical Engineers)
        - **Y14.5** GD&T (Geometric Dimensioning and Tolerancing)
        - **Y14.41** Digital Product Definition Data Practices
        - **Y14.36** Surface Texture Symbols
    - **ISO** (International Organization for Standardization)
        - **ISO/TC 213** GPS (Geometrical Product Specification) including ISO 1101 for geometrical tolerances of forms, ISO 5459 for geometrical tolerances of datums, ISO 14405 for dimensional tolerances, ISO 17863 for tolerancing of moveable assemblies, etc.;
        - **ISO/TC 10** TPD (Technical Product Documentation) including ISO 128 and ISO 7083 for technical drawings and ISO 16792 for technical product documentation;
        - the joint **IEC/ISO 81714** defines graphical symbols for use in the technical documentation of products;
        - **IPC-D-325** defines documentation requirements for printed boards, assemblies and support drawings.
- **Product Model and Data Exchange**, for capturing the representation of product and engineering information to enable data exchange between CAD software from different vendors:

  - **STEP ISO 10303** - addressing a broader range of information for CAD representations, e.g. 203 (in aerospace and defence), 214 (in automotive mechanical design processes), 210 (for printed circuit boards), etc.
  - **ISO 14306(JT)** - a visualization exchange format (CAD file)
  - **ISO 14739(PRC)** - Product Representation Compact (PRC) format exchange
  - **IGES** - an exchange format for sharing product design data, adopted by ANSI since 1976;
  - **STL** (Stereolithography) used for rapid prototyping, 3D printing and additive manufacturing.
  - **ISO 52915 AMF** (Additive Manufacturing File Format) is an open standard proposed to describe colour, materials, lattices, and constellations of a 3D object allowing for more complex descriptions of products, beyond basic geometry;
  - **MIL Standard 31000A**, for sharing product model information & product lifecycle [MIL-STD-31000A].
- **<u>Manufacturing Model Data</u>** defines the data needed to manufacture a product from a design:
  - **ISO 6983 (G-Code)** is widely used for Numerical Control (NC) of machines;
  - **ISO 14649** defines a data model to enable a link between manufacturing operations and the original CAD geometry data.
  - **ISO 10303 - 238 (STEP)** is designed to extend ISO 14649 in order to integrate more tightly with product design definitions.
  - **ISO 10303 - 207** provides sheet metal die planning and design.
- **<u>Product Catalogue Data</u>**, support the description of particular instances of products or product parts:
  - **ISO 13584** specifies the principles to be used for defining characterization classes of parts and properties of parts independent from any particular supplier-defined identification;
  - **ISO 15926-Part 4** represents a specific domain and defines the engineering terms required to design, build, and operate an oil and gas production facility;
  - **ISO 22745** provides guidelines for the development of terminology for open technical dictionaries and inventory and catalogue systems.
- **<u>Product Lifecycle Data Management</u>**, focuses on the needs of long-term retention and access to data consistently throughout the product lifecycle.
  - **ISO 10303 AP239, also known as Product Life Cycle Support (PLCS)**, designed for the exchange of complex-product for life-long support, i.e., the information needed and created during the use and maintenance of products.
  - **PLM XML** is an emerging open format from Siemens for facilitating PLM [CHEL08]
  - **LOTAR (LOng Term Archiving and Retrieval)** project focuses on long-term access to digital product and technical information through the development of standards-based archival and retrieval mechanisms. The results of that effort are recommended practices on how standards can be applied to long-term archiving of products and associated design information.

### 3.1.2. Production System Lifecycle Standards

Production system lifecycle refers to collections of machines, equipment, and auxiliary systems organized to create goods and services from various resources [NIST-8107]. These standards support various perspectives such as complex system design and modelling, automation engineering, and operation and maintenance (O&M), which is defined through the following categories of standards:

- **<u>Production System Model Data & Practice</u>**, provide information models for factory and production system design, enhancing information exchange among stakeholders, manufacturing agility and reducing manufacturing cost.
  - **Standards for manufacturing resource and process**, including

        - **ISO 10303 AP 214** for representing different aspects of a manufacturing system in development,
        - **ISO 10303 AP 221** for defining functional data for, and schematic representation of, process plants,
        - **ISO 18629** that defines a Process Specification Language (PSL) aimed at formally defining and structuring the semantic concepts intrinsic to the capture and exchange of process information related to discrete manufacturing,
        - **IEC 62832 (Digital Factory)** that defines a comprehensive network of digital models, methods, and tools to represent the basic elements and automation assets, as well as the behaviour and relationships between these elements/assets.
        - **ISO 17506** that defines an open standard XML schema for exchanging digital assets among various graphics software applications for plant geometry representation and kinetics simulation.
        - **CMSD (Core Manufacturing Simulation Data)** Information Model developed by NIST and standardized by the Simulation Interoperability Standards Organization (SISO) to define a data-interface specification for efficient exchange of manufacturing lifecycle data in a simulation environment.
        - **PLC Open XML** provides standards to represent Programmable Logic Control (PLC) including sequences of actions, internal behaviour of objects, and Input/Output (I/O) connections.
        - **IEC 62337** defines specific phases and milestones in the commissioning of electrical, instrumentation, and control systems in the process industry.
        - **IEC 61987** defines a standard to facilitate understanding of process measurement and control equipment descriptions when transferred from one party to another.
    - **Standards for building/facility modelling**
        - ISO 10303 - 225 for building elements using explicit shape representation
        - ISO 10303 - 227 for plant spatial configuration
        - ISO 16739, IFC (Industry Foundation Class) to facilitate interoperability in architecture, engineering and construction industry.
- **<u>Production System Engineering</u>**, can be used to interconnect engineering tools from different disciplines, e.g., system engineering, electrical design, process engineering, process control engineering, Human Machine Interface (HMI) development, robotic programming, etc.
    - **SysML (Systems Modelling Language)**, OMG's general-purpose modelling language for systems engineering applications, particularly useful for production systems;
    - **Modelica** (see https://www.modelica.org/) is an object-oriented modelling language, widely used in applications that model complex physical systems and subcomponents of production systems;
    - **IEC 61131** standard for programmable controller;
    - **IEC 61499** is an open standard for distributed control and automation, upon which entire applications can be built from Function Blocks (FB) with event triggers;
    - **IEC 61804** defines FB for process control;
    - **IEC 62714 (AutomationML**) interconnects engineering tools from different disciplines, e.g., mechanical plant engineering, electrical design, process engineering, process control engineering, HMI development, PLC programming, robotic programming, etc. [FNMM12];
    - **IEC 62453-2** for modelling and configuring production equipment (for field device tool interface specification)
    - **IEC 61804-3** for specifying Electronic Device Description Language (EDDL);

- **IEC 61508** for electrical, electronic, and programmable electronic safety-related systems. It specifies requirements to ensure that systems are designed, implemented, operated, and maintained to standards for safety integrity levels (SIL);
- **IEC 61511** for specifying practices in the engineering of systems that ensure the safety of an industrial process through the use of instrumentation;
- **ISA/IEC 62443 (Industrial Automation and Control Systems Security),** created to improve safety, availability, integrity, confidentiality of components, to provide criteria for procuring and implementing secure Industrial Automation Control Systems (IACS), improve electronic security, reduce risk of compromising confidential information, risk of causing degradation or failure of equipment of processes under control, etc. (see: http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf). For more information on ISA/IEC 62443, see Appendix 1 "State of the Art in Security, Safety, Lifecycle Process Standards and Best Practices Guidelines";
- **ISO 13849** provides safety requirements and guidance on the principles for the design and integration of safety-related parts of control systems, including the design of software.

- **Production Lifecycle Data Management** standards define general models of data integration, sharing, exchange, and hand-over for lifecycle support of production facilities:
  - **ISO 10303 - 239 (PLCS)** has the most potential to model a manufacturing system and its lifecycle;
  - **ISO 15926** is the most widely used production lifecycle data management standard in the process industry. It defines a reference data model in Part 4 providing more useful entities for representing process plants;
  - **ISO 15926 -1** defines a class structure of various phenomena or occurrences that exist in time and space in that industry;
  - **ISO 16739 (IFC)** defines a common data model for building lifecycle support that can be applied to manufacturing facilities;
  - **IEC 62890** defines standards for lifecycle management for systems and products used in industrial process measurement, control and automation.
- **Production System Operation and Maintenance (O&M)** standards define data processing, communication, and presentation standards for condition monitoring and diagnostics of machines, for maintaining the adequate performance of the system, and for searching ways to improve performance. These standards include:
  - **MIMOSA Open Systems Architecture for Enterprise Application Integration (OSA-EAI)** specifications (widely used in the oil and gas industry);
  - **MIMOSA Condition Based Maintenance (CBM)** specifications (widely used in the oil and gas industry);
  - **ISO 13374** defines data processing, communication, and presentation standards for condition monitoring and diagnostics of machines;
  - **ASME B5.59-2** addresses performance and capabilities of machine tools at any time in their lifecycle phases, e.g., during specification, after acceptance testing, or during operation. It does not include process-related information [CHEL08].

### 3.1.3. Business Processes and Supply Chain Lifecycle Standards

There are several standards for the interaction among manufacturers, suppliers, customers, partners and competitors. These standards are the key to enhance the supply chain efficiency and manufacturing agility [NIST-8107]:

- General standards for business modelling and executing business processes; and
- Manufacturing specific modelling standards (and corresponding message protocols).

The main manufacturing-specific standards supporting the integration are presented in [NIST-8107]:

- **APICS SCOR** (Supply Chain Operations Reference) is a text-based process reference model from Supply Chain Council (SCC). It is considered de facto standard for identification and promotion of best practices in the management and the operation of supply chain activities. SCOR is a tool for managing the supply chain “from supplier’s suppliers to customer’s customers” and describes business activities for all phases of satisfying the customer’s demand. It is based on three pillars: Process modelling and reengineering, Performance measurements and Best practices.

- **OAGIS** (Open Applications Group Integration Specification) describes a suite of engineering and business message specifications and defines common content models as well as messages for communication between business applications and guides for implementation. Some industries and functions, which are spanned by OAGIS, include e-Commerce, manufacturing, logistics, Customer Relationship Management (CRM) and Enterprise Resource Planning (ERP). It contains specific formats for common types of messages as well as mechanisms for extending and customizing standards for specific needs.
- **MESA B2MML** is an implementation well adopted of ISA 95 data models, which facilitates the integration of ERP as well as supply chain management systems with different manufacturing systems.

Other examples of standards for modelling and execution of business processes include (see Appendix 3 for more details):

- **BPMN (Business Process Modelling Notation)** by OMG, is a standardized graphical notation for drawing business processes, which also defines metamodel and interchange format;
- **XPDL (XML Process Definition Language)** by the Workflow Management Coalition (WfMC), defines business process models that addresses the graphics and the semantics, and can be executed, stored, exchanged;
- **ebXML (Electronic Business XML)** by OASIS, standardizes the secure exchange of business data;
- **BPEL (Business Process Execution Language)** by OASIS, specifies business process behaviour based on web services, XML-based, and models can be executed, stored, exchanged;
- **UBL (Unified Business Language)**, OASIS, is a generic XML interchange format, which can be customized (in order to meet the requirements of industries);
- **WSDL (Web Service Definition Language)** by W3C, is an XML format that describes network services as set of endpoints operating on messages, contains document- oriented or procedure- oriented information;
- **ANSI X12** by ASC X12, is one of the most widely adopted Electronic Data Interchange (EDI) document standards;
- **EDIFACT**, UN/CEFACT, an international EDI standard for Administration, Commerce, Transport.

## 3.2 Automotive Driving Standards and Recommendations

The automotive industry is currently going through significant changes: there are already electric and connected vehicles on the road, and autonomous vehicles are tested around the globe, and will enter mainstream in a few years. Today’s electric and autonomous vehicles are designed with lots of computer-assisted technologies, including sensors, in-vehicle operating systems, analytics, smart navigation, and more. Therefore, it is necessary to find a way to ensure technological interoperability and to support the communication and interaction among vehicles and their environment. The information gathered from vehicles (e.g. in-vehicle operations, occupants, planned journeys, environment, etc.) can be used to make the journey more efficient, reduce the costs or even contribute to safety. For this to become real, the vehicle has to communicate with a range of other systems, like traffic management, weather monitoring, pollution control, emergency response, fuel supply. If this is enabled, it could also improve road utilization, e.g. traffic lights could be turned off as computers in vehicles and traffic management system could interweave.

Standards are needed to ensure that different technologies in Automotive Driving communicate effectively, but because manufacturers have been developing intelligent devices for 40+ years, various protocols are currently in use in various industries. They were not designed specifically for IoT and there is no consensus on which standards to be adopted for a specific purpose. For the automotive industry, this means that multiple manufacturers use multiple systems, which leads to smart vehicles not being able to communicate with each other. To create an efficient smart road infrastructure, best practice standards are needed to ensure the transmission of operational and environmental information between smart vehicles. For example, the bIoTope project (http://www.biotope-project.eu/) aims to establish a marketplace for services provided by intelligent systems. These services should be able to communicate with each other using open standards, e.g.:

- O-DF (Open Data Format), Open Group: similar to HTML, way of encoding and describing information (https://publications.opengroup.org/c14a)
- O-MI (Open Messaging Interface), Open Group: similar to HTTP, format for exchanging information (https://publications.opengroup.org/c14b)

One of the bIoTope's use cases is described as follows: "*A car arrives in a smart city. It is able to make contact with other smart devices in its environment, so it can deliver useful information to the driver, like the quickest route, location of a free parking space or the availability of an electric charging point.*" Here, standards are the key in the world of electric and autonomous cars to ensure interoperability of various technologies [HAJO17].

### 3.2.1 ISO Standards for Intelligent Transport Systems

An overview of standards in Cooperative Intelligent Transport System (C-ITS) field is given in [ITS 278]. The overall objective of C-ITS is to improve safety, sustainability, efficiency, comfort in the automotive sector. It includes the following standards (see Figure 5):

- **ISO/TS 19091:2017** (ITS – Cooperative ITS – Using V2I and I2V communications for applications related to signalized intersections): message, data structures and data elements to support information exchange between roadside equipment and vehicles, to improve safety, mobility, environmental efficiency (see: https://www.iso.org/standard/69897.html);
- **ISO/TS 17429:2017** (ITS – Cooperative ITS – ITS station facilities for the transfer of information between ITS station): generic mechanisms to enable information exchange between ITS stations, conform to ITS station reference architecture (ISO/TS 21217);
- **ISO 21217:2014** (ITS – Communication Access for Land Mobiles (CALM) – Architecture): communications reference architecture of nodes (ITS station units), designed to support the deployment in ITS communication networks, describes various communication modes between ITS communication nodes (see: https://www.iso.org/standard/61570.html):
- **ISO/TS 19321:2015** (ITS – Cooperative ITS – Dictionary of In-Vehicle Information (IVI) data structures): IVI data structures required by different ITS services for information exchange between ITS stations, general extensible data structure, containers for current-day information, divided into data frames and data elements (see: https://www.iso.org/standard/64606.html)
- **ISO/TS 17419:2014** (ITS – Cooperative systems – Classification and management of ITS applications in a global context): specifies GCMA (Global Classification and Management of ITS Applications), based on ISO 21217, specifies globally unique addresses and identifiers (internal and external of ITS station) and how they are used for classification, registration and management of ITS applications (see: https://www.iso.org/standard/59720.html)
- **ISO/TS 18750:2015** (ITS – Cooperative systems – Definition of a global concept for Local Dynamic Maps (LDMs)): describes functionality of LDMs, in context of Bounded Secured Managed Domain (BSMD) (see: https://www.iso.org/standard/63273.html)
- **ISO/TS 17425:2016** (ITS – Cooperative systems – Data exchange specification for in-vehicle presentation of external road and traffic related data): In-vehicle signage service and application about road and traffic conditions (qualified by road authorities/operators).

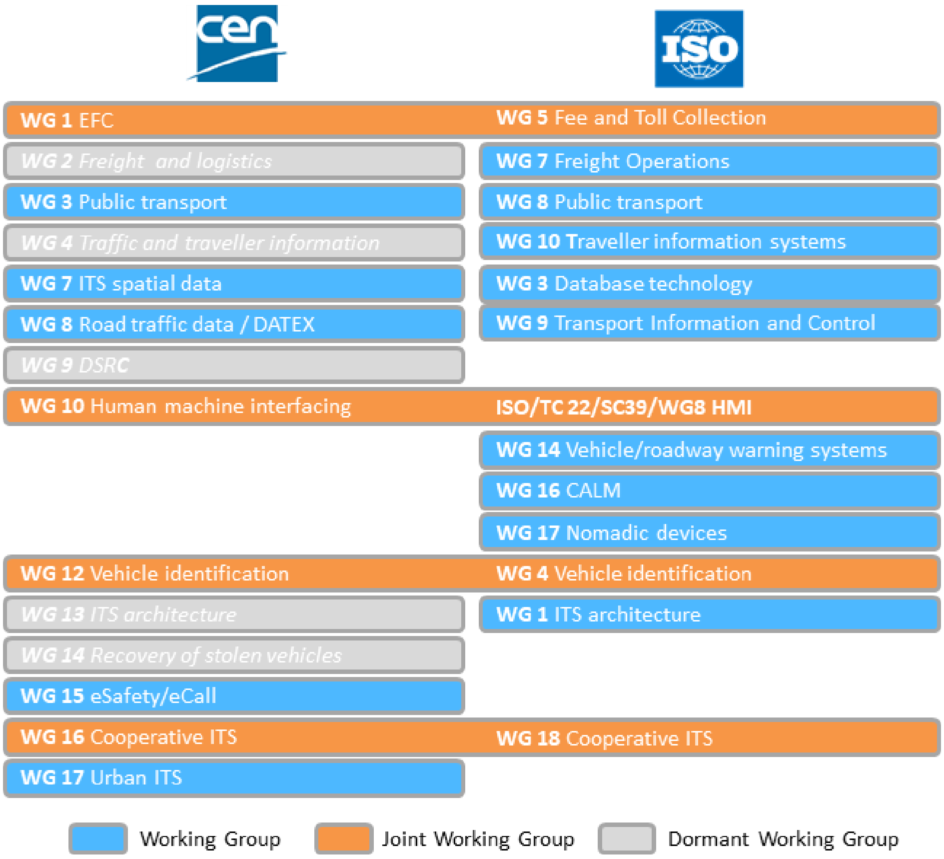



**Figure 5.** C-ITS Working Groups, Joint Working Groups, and Dormant Working Groups [ITS 278].

### 3.2.2 ISO Standards for Functional Safety

- **ISO 26262-10:2012** (Guideline on ISO 26262): overview and the description of general concepts of ISO 26262 (see: https://www.iso.org/standard/54591.html)
- **ISO 26262:2011** (Road Vehicles – Functional Safety): standards applied to safety-related systems that include one or more Electrical and/or Electronic (E/E) systems, not addressing E/E systems in special purpose vehicle (e.g. vehicle for driver with disabilities), not addressing hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy (unless directly caused by malfunctioning behaviour of E/E safety-related systems)
- **ISO 26262-1:2011** (Vocabulary): terms, definitions, abbreviated terms (see: https://www.iso.org/standard/43464.html)
- **ISO 26262-2:2011** (Management of functional safety): requirements for functional safety management for applications, project-specific requirements addressing management activities in safety lifecycle (see: https://www.iso.org/standard/51356.html)
- **ISO 26262-3:2011** (Concept phase): requirements for concept phase of Automotive Driving applications, such as item definition, initialization of safety lifecycle, hazard analysis and risk assessment, functional safety concept (see: https://www.iso.org/standard/51358.html)
- **ISO 26262-4:2011** (Product development at the system level): requirements for product development at system level for Automotive Driving applications, such as requirements for initiation of product development at system level, technical safety concept, system design, item integration and testing, safety validation, functional safety assessment, product release (see: https://www.iso.org/standard/51359.html)
- **ISO 26262-5:2011** (Product development at the hardware level): requirements for product development at hardware level for Automotive Driving applications, requirements for initiation of product development at hardware level, specification of hardware safety

requirements, hardware architectural metrics, evaluation of violation of safety goal due to random hardware failures, testing (see: https://www.iso.org/standard/51360.html)
- **ISO 26262-6:2011** (Product development at the software level): requirements for product development at software level for Automotive Driving applications, requirements for initiation of product development at software level, software safety requirements, software architectural design, software integration and testing, verification of software safety requirements (see: https://www.iso.org/standard/51362.html)
- **ISO 26262-7:2011** (Production and operation): requirements for production, operation, device decommissioning (see: https://www.iso.org/standard/51363.html)
- **ISO 26262-8:2011** (Supporting processes): requirements for supporting processes, interfaces between distributed developments, configuration management, change management, verification and documentation (see: https://www.iso.org/standard/51364.html)
- **ISO 26262-9:2011** (Automotive Safety Integrity Level (ASIL)-oriented and safety-oriented analyses): requirements for ASIL-oriented and safety-oriented analysis, requirements decomposition with respect to ASIL tailoring, criteria for coexistence of elements, analysis of dependent failures, safety analyses (see: https://www.iso.org/standard/51365.html)
- **ISO 26262-10:2012** (Guideline on ISO 26262): overview of ISO 26262, additional explanations, general concepts of ISO 26262 (for more details, see: https://www.iso.org/standard/54591.html)
- **ISO/SAE AWI 21434 (Road Vehicles - Cybersecurity engineering):** Currently under development (see: https://www.iso.org/standard/70918.html)

## 3.3 oneM2M Open Standard for IoT Interoperation

**OneM2M** (see: http://www.onem2m.org/) is a global standard for IoT applications, created to reduce the diversity of devices and legacy systems, which at present cause huge complexity for IoT development. IoT platform convergence requires horizontal integration and strong interoperability features, which should be achieved through adoption of a wide range of well-established IoT communication protocols, e.g. CoAP (Constrained Application Protocol), MQTT (Message Queue Telemetry Transport), Websockets and HTTP. The two major objectives of oneM2M are (i) to reduce the market fragmentation caused by mutually incompatible IoT platforms, and (ii) to support sharing of service resources (with different resource formats) across domains and reuse of available tools and functionalities of integrated platforms, e.g. data analytics modules, security software, optimization methods, etc. [oneM2M17].

The oneM2M architecture contains the oneM2M Common Service Layer and the oneM2M Application Layer (Figure 6) [oneM2M-REQ16]. All IoT-related services are captured by the Common Service Entity (CSE), while IoT-related applications are within the Application Entity (AE). The oneM2M Application Layer supports flexibility of the IoT application, e.g. it enables an IoT security application to set its own security policies, while reusing applications from different providers [oneM2M16]. The oneM2M Common Service Layer is based on the **oneM2M Base Ontology** (data model for knowledge specification). Semantic interoperability between oneM2M and external open platforms can be achieved through ontology mapping, either by linking (mapping) classes and properties of oneM2M Base Ontology to external ontology, or by using semantic annotation across ontologies [oneM2M-BaseOntology].

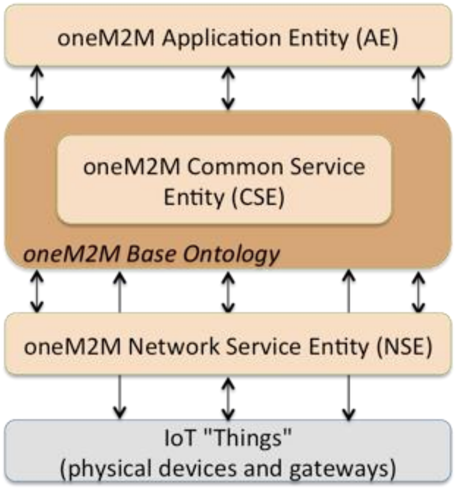



**Figure 6.** oneM2M high level architecture

**oneM2M BENEFITS FOR ADOPTERS.** oneM2M is designed to support semantic interoperability, resource distribution and reuse, and security features: platform registration; secure data management; access control including identification, authentication and authorization; identity management; security administration; sensitive data handling. This allows external developers to adopt basic security services and focus on value added services [oneM2M16].

# 4. Scenario Design for Capturing Lifecycle Data Models in Automotive Driving

Smart autonomous vehicles are designed to assist their owners in a variety of ways, from enhancing the driver's user experience (e.g. lane changing, parking assistance, night vision, traffic sign and traffic light recognition, map navigation support, etc.) to reducing driver's distraction and improving the safety [NAKR15][ENISA16]. However, Cloud Computing and cloud-based applications and technologies in the automotive sector, are exposed to a vast attack surface, in which every asset is a potential target for compromising its security, privacy, and safety. Specifically, in task T5.1 of IoT4CPS, we have created a conceptual scenario to help us capture basic lifecycle data models in the automotive sector. Note our basic lifecycle data models will be extended in task T5.4 of IoT4CPS to address security, privacy, and safety.

The validation of the tools and services to be developed in the project, will be performed based on the Digital Twin demonstrator. Therefore, our scenario includes a Digital Twin-based functionality to simulate Smart Car's operational lifecycle. We firstly define the operational process to be simulated, and secondly, we identify scope of data that are necessary to support simulation phases and analytics mechanisms related to operational lifecycle (see Appendix 4 and Appendix 5 for details).

Figure 7 illustrates the current state of play in the automotive sector. covering the following phases:

- *initial phase* - collecting data about the vehicle model, vehicle design information, on-board sensors, tyre surface, etc.), data about the connectivity to external systems and services (e.g. retailer, insurance, road services, etc.), driver's perception data (e.g. environmental cues);
- *operational/ driving phase* - collecting data from various operational assets, environmental statistics data, authority reports (government and regulations);
- *analytics phase* – requiring manual data processing and assessments reports, information about the threat identification and mitigation;
- *reporting phase* – manually creating the reports about operational features and sending these reports to stakeholders for further decisions.

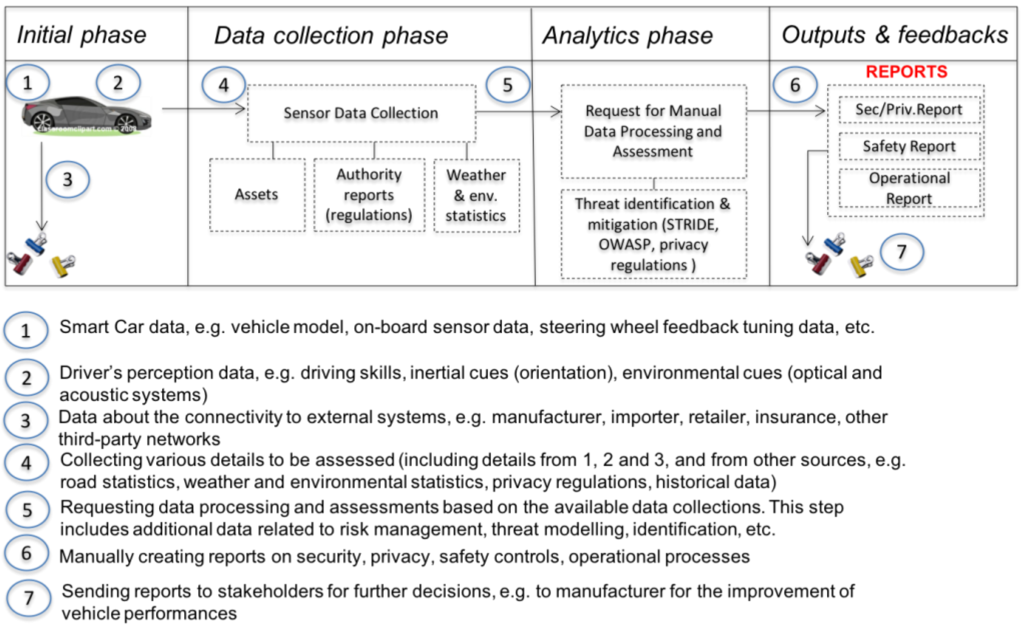



**Figure 7.** Current state in the automotive sector: data analytics, reporting and decision making are performed under control of human actors.

In IoT4CPS, the process of simulating and measuring operational behaviour and performances of Smart Cars is envisioned to be supported by the Digital Twin, replacing currently manually performed data analytics and reporting (as shown in Figure 7) with automated decision-making based on (near) real-time measurement and data (see Figure 8). Currently, the decisions on how to improve operative procedures that may affect user experience, are under control of human engineers. With the evolution of digital manufacturing, more intelligence and automation need to be brought to business processes and lifecycle phases, along the entire lifecycle, e.g. from the product design, manufacturing, operational, to administrative processes in the Smart Car ecosystem.

Figure 8 illustrates a scenario with a Digital Twin, supporting the simulation of Smart Car operational lifecycle based on the driver's perception data (e.g. inertial cues, environmental cues), sensor-based assessment, analytics and decisions. The collection of (near) real-time sensor (assets) data and data obtained from external sources, including environmental statistics and government regulations, will be sent to the Digital Twin for analyses, e.g. location- and temporal behavioural analyses, correlation of captured behaviour and performances through Machine Learning (ML) and Deep Learning algorithms (e.g. Deep Neural Networks). In that way, the Digital Twin and its intelligent methods correlate dynamic sensor data to KPIs and historical data, perform security, safety and operational analyses, predict insights and create analytics-based decisions that could be automatically sent to stakeholders, either suggesting operational changes or performing operational decisions with or without human interventions.

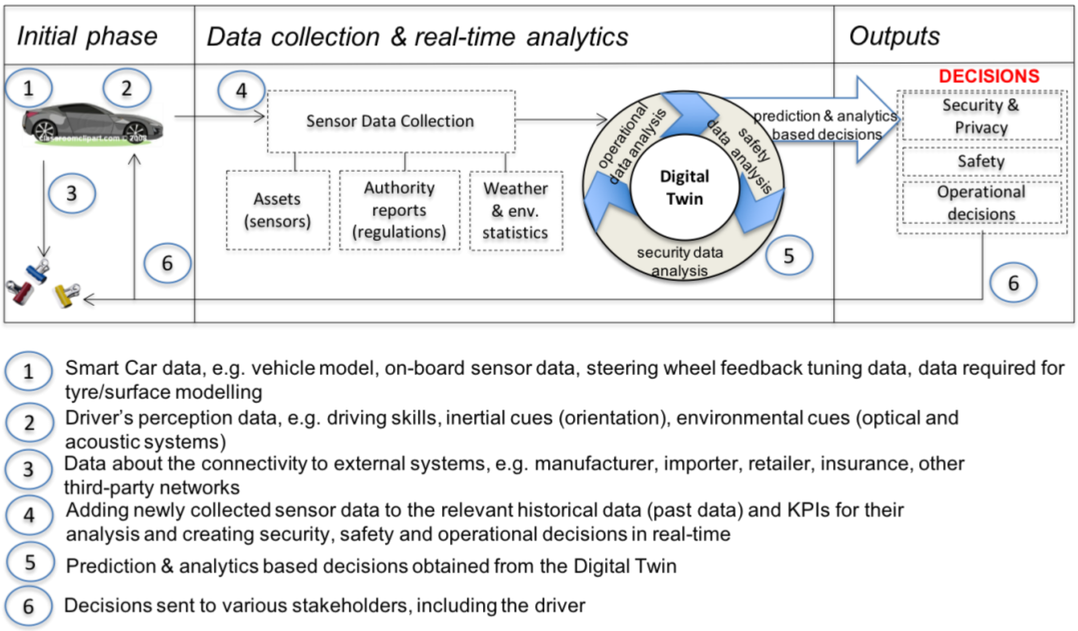



**Figure 8.** Future state in Smart Car driving: the assessment of driving conditions is based on the Digital Twin.

Both the collected data and data processed by the Digital Twin can contain privacy data. AI & ML methods combine, correlate and link privacy data that can affects the subject's privacy in unexpected, unintended ways. Therefore, the Digital Twin toolset can be designed to support e.g. GDPR enforcement, privacy anomalies detection, security and safety issue detection and mitigation mechanisms. The pre-requisite for the implementation of such a toolset is to have defined data models with various stakeholders and assets, in order to effectively support lifecycle data management. Note that the identification of multi stakeholders in the automotive sector and the analysis of their interests to consume lifecycle data will be a topic of task T5.2 (D5.2 "Data Model for Multiple Stakeholder Lifecycle Data Management").

## 4.1 Identifying Assets in Automotive Driving Systems

Automotive Driving systems are designed to augment user experience through information exchange amongst various stakeholders that can open numerous security, privacy and safety issues leading to reputational damage for the users, car manufacturers, suppliers, garages, network service providers, software and application providers, Smart Cities. In this section, we identify sensitive assets in the operational lifecycle of the automotive sector, e.g. the driver's smartphone.

Table 4 lists assets identified in a Smart Car's lifecycle, their core functionality and associated security, privacy and safety concerns and risks to data.

**Table 4. Assets in the Smart Car Driving Scenario (analysis partly based on [ENISA16]).**

| **Sensitive Asset** | **Asset Functionality** | **Security, Privacy & Safety Concerns & Mitigations** |
|---|---|---|
| Infotainment controls | Navigation services and maps, entertainment services (audio/video), geo-fencing, cameras, traffic information, external media, etc. | Revealing information about user's current location and navigation history, call history, geo-fencing data related to driving and working routines, heart rate and pulse, health data, banking accounts, etc. |
| Body controls | Door/ window locking, seat belts, heating seats, | Revealing information about user's driving patterns and preferences, information about the functionality of assets leading towards safety issues. |
| Chassis controls | Alerts sent to drivers via ADAS (Advanced Driver Assistance Systems) | Revealing sensitive information linked with GPS data and traffic warnings, connected smartphone data, blind spots, audio alerts, etc. |
| Power Train controls | Speed control | Security breaches; Driving patterns and preferences; speed and safety. |
| Communications controls | Authentication features; Connectivity with external services through an embedded GSM module or driver's smart phone;<br>Stolen vehicle tracking; emote engine start; etc. | Security breaches; Revealing privacy data stored on smartphones; Sharing security and privacy data via smartphone with: service providers, developers, criminals hacking physical access to device, behavioural marketing; government; geotags GPS capabilities to embed exact location into posts or photos, etc. |
| Smartphones | Authentication features; Connectivity with Smart Car services and applications using e.g. tethered connections, etc. | Security breaches; Unauthorized access and manipulation of information stored on smartphone, e.g. e-mails, text, instant messenger apps, online accounts and passwords typed into phone, location data and history, call history, photos, etc. |

## 4.2 Asset Modelling and Designing Lifecycle Data Models

Asset modelling is the crucial step in defining of the technical architecture of the Digital Twin. Asset modelling is about designing the structure of product's or system's assets (physical things) and components, measurable physical parameters and other digital manufacturing information that describe the assets, e.g. manufacturing date, maintenance history. Asset modelling adds value to the connected sensor data and contributes to a range of new insights, e.g. obtaining an information on health of sensors, which could be performed through inferring, correlation and transformation of measured sensor values and asset states, conditions and maintenance records [KUAB17]. It may also include a different presentation (visualization) forms for different user groups, e.g. one group of users may require the insight in only operational data, while the others could be more focused on individual devices. Finally, by adding information such as metadata, nearby environmental conditions, maintenance data, service history, configuration and production data, external data, enterprise web services etc., enhance a digital representation of the physical things (device/system) and further augments the Digital Twin.

The functionality of a Digital Twin improves over time as more data is accumulated and processed through effective algorithms correlating asset lifecycle data (e.g. time-series sensor data), inferred and historical data. According to the size of the data and knowledge base in the Digital Twin, the authors in [KUAB17] differentiate between:

- *partial* Digital Twin, with a small number of data sources that can be effectively combined to infer data (derivative data);
- *clone* Digital Twin, with a larger amount of meaningful and measurable data sources; and
- *augmented* Digital Twin that enhances connected asset data with derivative data and correlated data obtained from analytics tools.

A partial Digital Twin is built on top of simplistic device models that could be implemented as JSON documents, including a set of observed and reported attributes (e.g. speed of a machine) and a set of desired values (e.g. an application is setting the speed of a machine), which can be further correlated to detect operational abnormalities and instantly generate alerts. A clone and augmented Digital Twins are typically needed in industry. They are built on top of the product design and manufacturing information, reflect physical properties of the physical system and often use real-time data.

For the purpose of creating lifecycle data models to cover the above presented scenario in the automotive sector, we have created the initial forms for data acquisition. These forms relate to product design and operation lifecycle in the automotive sector. Note the form for data acquisition about multiple stakeholders and their motivations to have insights into smart driving data, will be presented in D5.2.

# 5. Conclusion

The evolution of the traditional industrial systems towards Industry 4.0 [WWLZ16] and Smart Manufacturing [KLCK16] is helping manufacturing systems to become more adaptive, by creating flexible decision-making mechanisms, self-adjustment and self-optimization features supporting core business process components, lifecycle phases and services [LFKF14][MOEL16]. For example, the Digital Twin is a virtual representation of the real-world manufacturing, operational, logistic, maintenance, even administrative processes in a company, designed with the aim to improve real-world products and processes based on simulated data and AI & Machine Learning supported decisions. Designing the Digital Twin demonstrator for Automotive Driving is expected to augment overall functionality of vehicles, including their security and safety, while privacy data should be kept secure in the cloud and comply with various regulations at the European level and relevant national data protection laws, e.g. privacy policies, procedures and regulations such as the GDPR, the NIS Directive on security of Network and Information Systems (NIS), and the eCall alarm system, etc.

# APPENDIX 1: State-of-the-art in security, safety, lifecycle process standards and best practices guidelines (Know-how transfer from SemI40 D1.1, Section 5.3)

**IEC 61508**

IEC 61508 "Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES)" is a Basic Safety Standard (BSS), and is used as a template to develop domain specific safety standards.

**IEC 62443**

IEC 62443 was developed by the ISA99 committee and IEC Technical Committee 65 Working Group 10 (TC65WG10) to address the need to design cybersecurity robustness and resilience into Industrial Automation Control Systems (IACS). Its scope includes all types of plants, facilities, and systems in all industries including, but not limited to systems like:

- hardware and software systems such as DCS, PLC, SCADA, networked electronic sensing, and monitoring and diagnostic systems.
- associated internal, human, network, or machine interfaces used to provide control, safety, and manufacturing operations functionality to continuous, batch, discrete, and other processes.

IEC 62443 is organized in four groups with multiple publications per group (Figure 9).

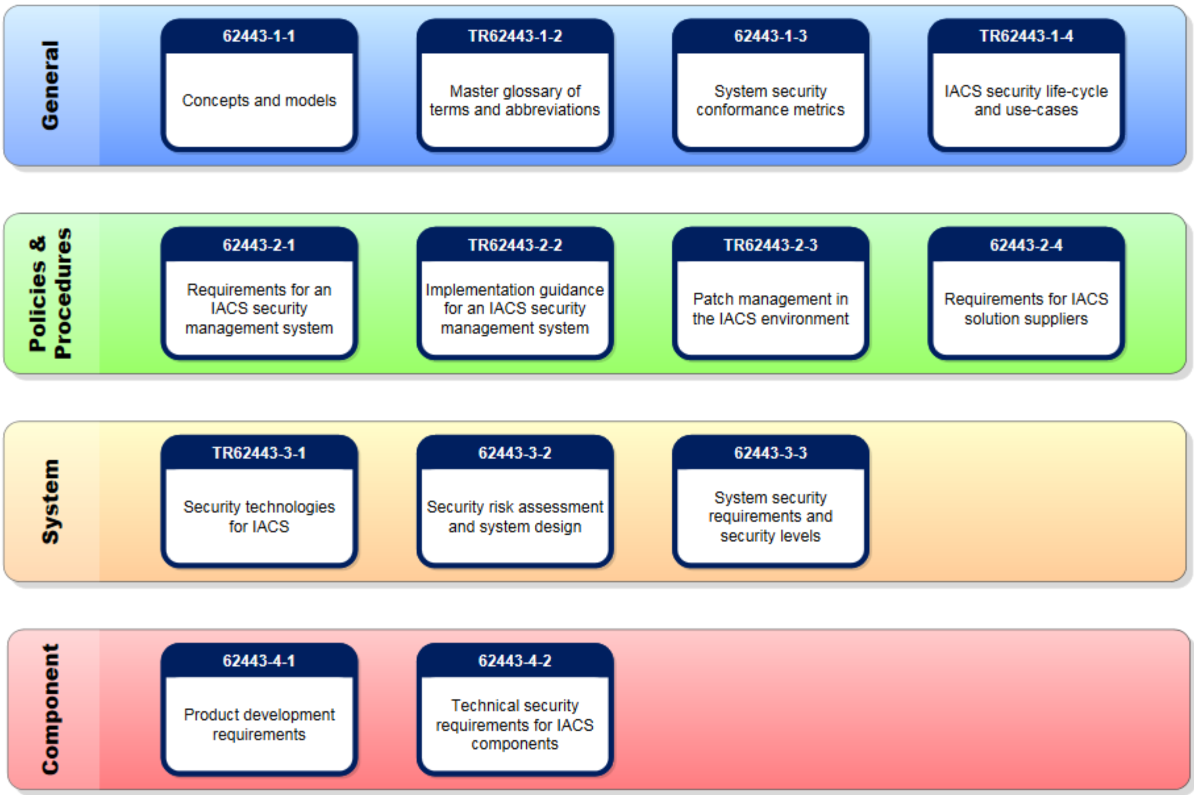



**Figure 9:** IEC 62443 elements [62443-15]

**ISO 2700X**

ISO/IEC 2700x family gives an overview and explains the Information Security Management Systems (ISMS), referring to ISMS family of standards with related terms and definitions. The standards ISO/IEC 27000, 27001, 27002, 27005 and 27017 are international standards, which have been adopted from different organizations around the world.

**ISO 27001**

**ISO/IEC 27001:2013** – *Information Technology – Security Techniques – Information Security Management systems – Requirements* **[**BREW13**]** defines the requirements to establish, operate, implement, maintain, monitor and improve the effectiveness of information security for an organization. This standard is a risk-based guideline with the purpose to ensure the information security in accordance with organization, information security, legal and operational procedures and responsibilities. It is built to assure the selection of the suitable security controls to protect information assets based on the Plan-Do-Check-Act (PDCA) process model and requirements for continuous improvement to improve the effectiveness. ISO 27001:2013 is not focused only on information technology, but also on business assets, resources and processes. This standard is an updated version of BS7799 by integrating the process-based approach of ISO 9001:2000 and ISO 14001:2004. The requirements in ISO 27001:2013 are generic and applicable to all kinds of organizations (public and private or commercial and nonprofit), regardless of type, size or nature.

**ISO/IEC 27002**

**ISO/IEC 27002:2013** – *Information Technology – Security Techniques – Code of Practice for Information Security Controls* [ISO27002-13] standard is designed to be used as a reference for (i) selecting controls within the process of implementing an ISMS based on ISO 27001, (ii) implementing information security controls and (iii) developing the organization own information security management guidelines. It has a well-structured set of controls to protect information assets against threats considering confidentiality, integrity and availability aspects. This standard is also intended to be used in developing industry and organization specific information security management guidelines taking in consideration their specific information security risk environment. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met.

The current version contains 114 security controls grouped in 14 security controls clauses. ISO 27002:2013 is a broadly applicable standard, since it leaves to the organization the decision to select and implement controls which are suitable for their security by providing flexibility in the implementation.

**ISO/IEC 27005**

**ISO/IEC 27005:2011** – *Information Technology – Security Techniques - Information Security Risk Management* [ISO27005-11] is a generic standard used for all types of organizations dealing with risk management, as an important approach to identify organizational needs regarding information security requirements and to create an effective information security management system. The focus of this standard is to provide guidelines for information security risk management by including risk assessment, threat and vulnerability identification, risk treatment, risk acceptance and risk monitoring.

**ISO/IEC 27017**

**ISO/IEC 27017:2015 –** *Security Techniques – Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services* [ISO27017-15]. The guidelines in this standard are in addition to and complement the guidelines given in ISO/IEC 27002 with the implementation of cloud based specific information security controls. The standard provides very useful recommendations and advices for both, the cloud service customer (CSC) by educating them what they should request from the cloud host and the cloud service provider (CSP) controls by defining the security controls that should be implemented to reduce the barriers to cloud mitigation. ISO 27017 is designed to help the organizations to manage the adoption of cloud services in a secure and compliant manner while preserving the advantages that these kind of IT services bring.

**ISO/IEC 15408**

**ISO/IEC 15408:2009 – Common Criteria** – *Information technology – Security techniques – Evaluation criteria for IT security* [ISO15408-09] is composed of three main parts. The first part of the standard establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation. The second part of the standard defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408 general model. It contains a comprehensive catalogue of predefined security functional components, which are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. The third part of the standard defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance.

**NIST SP 800 series**

The National Institute of Standards and Technology (NIST) 800 series is a set of publications developed as outcome of research for optimizing the security of IT systems and networks.

**NIST SP 800-82**

**NIST SP 800-82 –** *Guide to Industrial Control Systems (ICS) Security* [STOU11]. This standard provides guideline for implementing and establishing secure Industrial Control System (ICS) by including SP 800-53 controls for SCADA systems, Distributed Control Systems (DCS), and control system configuration such as Programmable Logic Controllers (PLC) in the industrial sector. NIST SP 800-82 gives an overview of ICS and also what makes it different and unique from traditional IT systems by providing, (i) ICS risk management and assessment, (ii) how to develop and deploy an ICS specific cyber security program, (iii) different ways for architecting the industrial control system for security, and (iv) applying security controls to ICS. The document has several appendices including: (a) ICS threats, vulnerabilities and incidents, (b) Activities in industrial control systems security, and (c) ICS security capabilities and tools.

**NIST SP 800-184**

**NIST SP 800-184** – *Guide for Cybersecurity Event Recovery* [BCSS16] . The purpose of this document is to support organizations in a technology-neutral way in improving their cyber event recovery plans, processes, and procedures. This guideline provides tactical and strategic guidance regarding the planning, playbook developing, testing, and improvement of recovery planning. It also provides an example scenario that demonstrates guidance and informative metrics that may be helpful for improving resilience of the information systems.

**NIST CSF**

**NIST Cybersecurity Framework - CSF** [NIST-CSF-14] is built on industry standards and best practices to help and identify cybersecurity risks. The framework provides a common language to manage internal and external cybersecurity risks for different organizations or within an organization. Since it is not industry-specific and is not designed to replace existing solutions, gives the possibility to apply and integrate this framework to the overall risk management process (i.e., Critical Infrastructure services). CSF can be adapted without replacing the existing risk management program but using it to improve and have a stronger cybersecurity management.

**ENISA**

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU with the aim to develop advice and recommendations on good practice in information security, providing technical advice about cloud computing security and resilience. ENISA investigates coordinates the development of best practices and advice for business, industry, institutions for EU member states.

**ENISA -** *Information Security and Privacy standards for Small and Medium Enterprises (SMEs)* [ENISA-15]. This document is a recommendation to improve the adoption of information security and privacy standards in small and medium enterprises (SMEs) by providing a set of relevant recommendations regarding how to increase the adoption of information security and privacy standards and the main existing barriers to adopt security standards. To understand the information security and privacy, ENISA evaluate existing international and European standards for SMEs in three domains: (i) professional and industry associations (e.g., ISO/TR 13569:2005[1], ISO/IEC TR 27019:2013[2], ISO 27799:2008[3], etc.), (ii) specific standards targeting SMEs (e.g., ISO/IEC 27036-3:2013[4]), (iii) standards, guidelines and best practices for securing business processes, products and compliance (e.g., ISO/IEC 27005:2011[5], ISO/IEC 27031:2011[6], BSI 100-4[7], CWA 16113:2010[8], etc.).

**ENISA** - *Procure Secure - A guide to monitoring of security service levels in cloud contracts*. This guideline published by ENISA addresses the contractual relationship of cloud services providers and cloud service customers by providing advices on questions to ask about the monitoring of security including service availability and continuous monitoring of security service levels. The main goal is to provide applicable transparency to the public-sector customer to understand the security of cloud services by providing real time information, reporting, alerting and the parameters that should be included in a monitoring framework to be able to verify if the security requirements are being met during the lifetime of the contract. The security metrics that should be measured presented in this document are based on the ENISA reports, Resilience Metrics and Measurements[9] and Survey and analysis of security parameters in cloud SLAs across the European public sector[10].

[1] http://www.iso.org/iso/catalogue_detail.htm?csnumber=37245
[2] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=43759
[3] http://www.iso.org/iso/catalogue_detail?csnumber=41298
[4] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=59688
[5] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=56742
[6] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374
[7] https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html
[8] https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT,FSP_ORG_ID:34912,413610&cs=
[9] https://www.enisa.europa.eu/publications/metrics-tech-report
[10] https://www.enisa.europa.eu/publications/survey-and-analysis-of-security-parameters-in-cloud-slas-across-the-european-public-sector

# APPENDIX 2: State-of-the-art in process management standards (Know-how transfer from SemI40 D1.1, Section 5.4)

The demand for better quality products at lower costs and the need to achieve strategic goals faster have urged the development and implementation of business processes. By using Key-Performance-Indicators (KPIs), business processes are convenient control mechanisms as one can quantify and measure them, even adapt them if appropriate. Managing these processes can be summarized under the term "Business Process Management (BPM)", which is defined as the activity undertaken by businesses to identify, evaluate, and improve business processes [BPM-16]. BPM can be managed with appropriate software, which is customized based on metrics and policies, to improve business process performance related issues.

**ISO 9001**

**ISO 9001:2015** - *Quality management systems – Requirements* [ISO9001-15]. This standard specifies the requirements for a quality management system, which can help an organization to improve its overall performance and provide a sound basis for sustainable development initiatives. The quality management system can help an organization in terms of: (i) the ability to consistently provide products and services that meet customer and applicable statutory and regulatory requirements; (ii) facilitating opportunities to enhance customer satisfaction, (iii) addressing risks and opportunities associated with its context and objectives, and (iv) the ability to demonstrate conformity to specified quality management system requirements. This International Standard is based on the quality management principles described in ISO 9000, including customer focus, leadership, engagement of people, process approach, improvement, evidence-based decision making, and relationship management. The process approach involves the systematic definition and management of processes, and their interactions, to achieve the intended results in accordance with the quality policy and strategic direction of the organization. Management of the processes and the system as a whole can be achieved using the PDCA (Plan-Do-Check-Act cycle) cycle with an overall focus on risk-based thinking aimed at taking advantage of opportunities and preventing undesirable results. All the requirements of ISO 9001:2015 are generic and are intended to be applicable to any organization, regardless of its type or size, or the products and services it provides.

**ISO 18404**

**ISO 18404:2015** - *Quantitative methods in process improvement -- Six Sigma -- Competencies for key personnel and their organizations in relation to Six Sigma and Lean implementation* [ISO18404-15]. This standard is used to define what is required in an organization that deploys applications such as, Six Sigma, Lean, and "Lean & Six Sigma". Since between these applications there are noticeable commonality and differences, e.g., in process improvement Lean focuses on reducing 'chronic' waste whilst Six Sigma focuses on reducing the variation and thereby its adverse effects, this standard defines the separate competency requirements for Six Sigma and Lean implementation; it also defines a combined competency framework for "Lean & Six Sigma". In so doing, it focuses on the competencies (skills and abilities) to deliver benefits to an organization rather than defining the specific educational level required for each role.

**ISO/IEC TS 33052**

**ISO/IEC TS 33052:2016** - *Information technology -- Process reference model (PRM) for information security management* [ISO33052-16]. The purpose of this Technical Specification (TS) is to define a Process Reference Model (PRM) for the domain of information security management. The PRM is a model comprising definitions of processes described in terms of process purpose and outcomes, together with an architecture describing the relationships between the processes. This standard is linked with other relevant standards, see Figure 10, such as ISO/IEC TR 24774, ISO/IEC 27001, ISO/IEC 33004, ISO/IEC 33002, ISO/IEC 33020, and ISO/IEC TS 33072. ISO/IEC 27001 and ISO/IEC 33004 provide the needed requirements for this standard, whereas ISO/IEC TR 24774 provides the guidelines for the description of processes by identifying descriptive elements and rules for their formulation. This TS standard provides then the description of processes assessed by ISO/IEC TS 33072. Using the PRM in practical applications may require additional elements suited to the environment and circumstances.

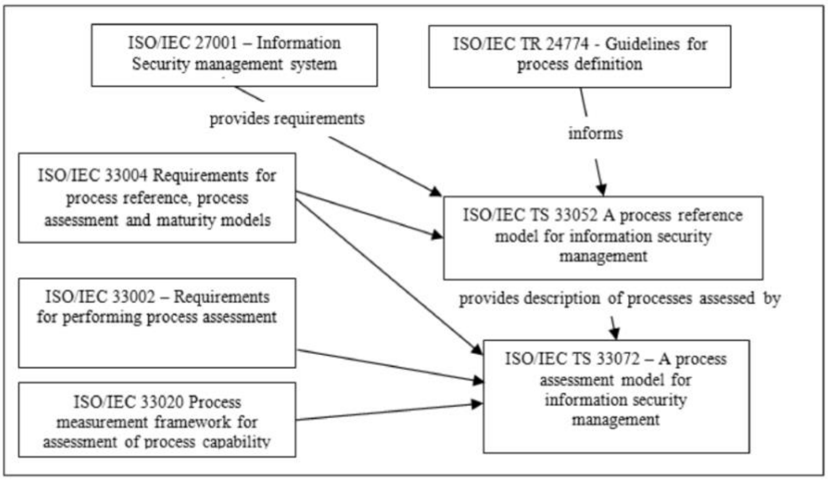



**Figure 10.** Relationships between relevant standards.

**ISO/IEC 29169**

**ISO/IEC 29169:2016** - *Information technology -- Process assessment -- Application of conformity assessment methodology to the assessment to process quality characteristics and organizational maturity* [ISO29169-16]. The purpose of this standard is the development of a conformity assessment methodology used to assess process quality characteristics and organizational process maturity. This standard support JTC1's objectives of mutual recognition of accreditation, test reports, certification, registration, and recognition of a supplier's declaration of conformity and follows the approach of ISO/IEC 17020. Thus, the overall framework for conformity assessment mainly includes the examination of processes, determination of their conformity using requirements defined in ISO/IEC 33001, and the subsequent reporting of results of these activities to clients and, when required, to supervisory authorities.

**ISO/IEC/IEEE 15288**

**ISO/IEC/IEEE 15288:2015** - *Systems and software engineering -- System life cycle processes* [ISO15288-15]. ISO/IEC/IEEE 15288 provides a common framework, defining a set of processes and associated terminology, to describe the life cycle of systems created by humans. These processes can be applied at any level in the hierarchy of a system's structure. Selected sets of these processes can be applied throughout the life cycle for managing and performing the stages of a system's life cycle. This is accomplished through the involvement of all stakeholders, with the ultimate goal of achieving customer satisfaction. This standard addresses those systems that include human-in-the-loop and can be configured with one or more of the following system elements: hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials and naturally occurring entities.

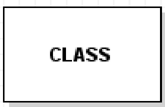
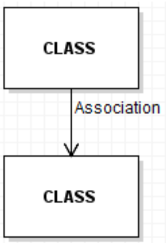
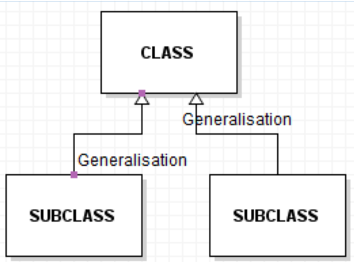
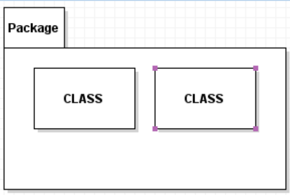
# APPENDIX 3: State-of-the-art in business process modelling languages (Know-how transfer from SemI40 D1.1, Section 5.5)

A business process model is a sequential representation of all functions associated with a specific business activity [BPM-16]. Examples of the most relevant business process modeling standards are listed in this section.

**ÖNORM A 9009** - *Prozesse in Managementsystemen*[11]. This Austrian standard provides guidance and requirements for processes in management systems and is designed for any organization, regardless of its type, size and the nature of the products and services provided. It focuses on the life cycle and the maturity level of a process.

**UML 3.0** *Unified Modeling Language (UML)*[12] is developed by the Object Management Group (OMG) with the main goal to provide system architects, software engineers, and software developers with tools for analysis, design, and implementation of software-based systems as well as for process modelling. Table 5 gives an example of a class diagram with the corresponding elements. This diagram shows the structure of the system at the level of classes and interfaces, their features, constraints and relationships, e.g. associations, generalizations, dependencies, etc.

**Table 5. UML symbols**

| Element | | Purpose |
|---|---|---|
| **Class** |   | Shows structure of the designed system, subsystem or component as related classes and interfaces, with their features, constraints and relationships - associations, generalizations, dependencies, etc. |
| **Association** |   | A relationship between classifiers, which is used to show that instances of classifiers could be either linked to each other or combined logically or physically into some aggregation. |
| **Generalization** |   | Directed relationship between a more general classifier (superclass) and a more specific classifier (subclass). |
| **Package** |   | A package is used to group elements or to provide a namespace for the grouped elements. |

**BPMN 2.0** - *Business Process Model and Notation (BPMN)*[13] is developed by the Object Management Group (OMG) with the goal to provide a notation that is understandable by all business users, from

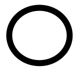
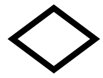
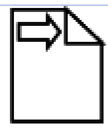
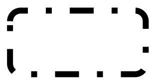
[11] http://prozesse.at/publikationen/oenorm-a9009.html
[12] http://www.uml.org/

[13] http://www.bpmn.org/

the business analysts that create the initial drafts of the processes, to the technical developers responsible for the implementation of the technology, and finally, to the business people who are responsible for the management and monitoring of processes. In BPMN, a process is depicted as a graph of flow elements, e.g. a set of Activities, Events, Gateways, and Sequence Flows that define finite execution semantics.

Table 6 displays a list of BPMN basics concepts that could be depicted through a business process modeling notation.

**Table 6. BPMN elements and notations.**

| Element | Description | Notation |
|---|---|---|
| **Event** | An Event is something that "happens" during the course of a Process, a cause or an impact, affecting the flow of the model. |  |
| **Activity** | An Activity is used to describe different types of tasks performed during a Process. |  |
| **Gateway** | A Gateway is used to control the flow in a process, by determining branching, forking, merging, and joining of paths in a Process. |  |
| **Sequence Flow** | A Sequence Flow is used to show the order that Activities will be performed in a Process. |  |
| **Data** | A Data object represents information flowing through the process such as business documents, emails, etc. |  |
| **Artifact** | Artifacts represent information relevant to the model but not to individual elements within the process |  |
| **Swimlane** | Swimlanes are used to organize aspects of a process. Swimlanes visually group objects into lanes, with each aspect of the process added to a separate lane |  |

Other conventions used in BPMN include operators, such as,
<none> — exactly once
[0..1] — 0 or 1
[0..*] — 0 or more
[1..*] — 1 or more

and attributes separated by | and grouped within { and } — alternative values
<value> — default value
<type> — the type of the attribute

## APPENDIX 4: Production lifecycle data model (the first draft)

(The objective of this data model is to identify production lifecycle phases, including design, operational and maintenance).

| Lifecycle Data | Description | Security/ safety measures | Data & connectivity standards | Comment |
|---|---|---|---|---|
| **PRODUCTION LIFECYCLE DATA** | | | | Information about the processes that would be observed in the use case/ scenario, and later on, simulated through the IoT4CPS demonstrator |
| *LC Design Processes* | | | | Data type, e.g. production data, transactional data |
| *Process 1 Name* | e.g. Data Product Catalogue Specification | | | Product catalogue design and definition |
| • *Input data*<br>• *Data format* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| *Process 2 Name* | e.g. Specification of Manufacturing Processes and Resources | | | Data for manufacturing a product from a design; Data for interconnecting various engineering tools, e.g. SysML, Modelica; implement. guidances, Device data |
| • *Input data*<br>• *Data format* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| *Process 3 Name* | E.g. Specification of Data Integration, Data Exchange & Connectivity Details | | | Models of data integration & interoperability; Data exchange and connectivity details for software from different vendors (e.g. visualization exchange formats, or standard for describing color, materials) |
| • *Input data*<br>• *Data format* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| ... | | | | Please add the description of other design processes of |

| | | | | |
|---|---|---|---|---|
| | | | | importance for the use case |
| *LC Operational Processes* | | | | Data type, e.g. operational sensor data, aggregated sensor data, environ. data |
| *Process 1 Name* | e.g. Data processing | | | |
| • *Input data*<br>• *Data format*<br>• *Process start time* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format*<br>• *Process end time* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| *Process 2 Name* | e.g. Data sharing | | | Data sharing between enterprise systems |
| • *Input data*<br>• *Data format*<br>• *Process start time* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format*<br>• *Process end time* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| ... | | | | Please add the description of other operational processes of importance for the use case |
| *LC Maintenance Processes* | | | | Data type, e.g. calibration data, maintenance data |
| *Process 1 Name* | Condition monitoring | | | |
| • *Input data*<br>• *Data format*<br>• *Process start time* | | | | |
| • *Output data*<br>• *Data type*<br>• *Data format*<br>• *Process end time* | | | | |
| • *Data and process dependencies* | | | | Does the process require the interaction of heterogeneous sub-systems or sub-processes? |
| ... | | | | Please add the description of other processes of importance for the use case |

# APPENDIX 5: Product lifecycle data model (the first draft)

(The objective of this data model is to identify the core product data related to the use case e.g. smart car)

| Lifecycle Data | Description | Security/ safety measures | Data & connectivity standards | Comment |
|---|---|---|---|---|
| **PRODUCT DATA** | | | | Information about the product that is involved in the use case/ scenario |
| *Name* | e.g. Connected Car FCA | - | - | |
| *Model* | e.g. Fiat Chrysler | - | - | |
| *Technology* | e.g. Telematics Control Unit (TCU) | | | |
| *Product design data* | e.g. assembly | Security methods? | | 2D, 3D model, specification, assemblies ... |
| *On-board sensor 1 /component* | e.g. steering wheel sensor-1 | | | |
| ● *Input data*<br>● *Data format* | e.g. steering wheel input data | Data integrity | | |
| ● *Output data*<br>● *Data type*<br>● *Data format* | e.g. steering wheel tuning data | Data integrity | | |
| *On-board sensor 2 /component* | e.g. tyre sensor-2 | | | 2D, 3D model, specification, assemblies ... |
| ● *Input data*<br>● *Data format* | e.g. tyre input data | Data integrity | | |
| ● *Output data*<br>● *Data type*<br>● *Data format* | e.g. tyre output modelling data | Data integrity | | |
| **…** | | | | Please add the description of more sensors/ components/ elements that constitute the Product. |

## References


[62443-15] Industrial Automation and Control Systems Security, "Overview The 62443 series of standards," 2015.

[ABGD16] Abramovici, M., Göbel, J.C., Dang, H.B. Semantic Data Management for the Development and Continuous Reconfiguration of Smart Products and Systems. CIRP Ann 2016;65(1):185–8. 2016.

[AIOTI15] AIOTI (2015). AIOTI WG11, „Report on Smart Manufacturing." Online available: https://aioti.eu/aiotiw11-report-on-smart-manufacturing. Last accessed March 2018.

[ALSA17] Alam, K.M. and Saddik, A.E. C2PS: A Digital Twin Architecture Reference Model for the Cloud-Based Cyber-Physical Systems. In: IEEE Access. Vol. 5 (2017)

[BCSS16] M. Bartock, J. Cichonski, M. Souppaya, M. Smith, G. Witte and K. Scarfone, "Cybersecurity Event Recovery," NIST Special Publication 800-184, 2016.

[BORO16] Boschert S, Rosen R (2016) Digital Twin – The Simulation Aspect. in Hehen- berger P, Bradley D, (Eds.) Mechatronic Futures: Challenges and Solutions for Mechatronic Systems and their Designers, Springer International Publishing 2016, pp. 59–74.

[BORO16] Boschert, S., Rosen R. Digital Twin – The Simulation Aspect. In: Hehenberger P, Bradley D, editors. Mechatronic Futures. Cham: Springer International Publishing; 2016.

[BPM-16] "Business Dictionary," 2016. Available: http://www.businessdictionary.com/definition/business-process-management-BPM.html.

[BREW13] Brewer, D., *An introduction to ISO/IEC 27001,* BIS British Standards Institution, 2013.

[CHEL08] A.V. Euler-Chelpin, Information modelling for the manufacturing system life cycle, Doctoral Thesis, KTH Royal Institute of Technology, Stockholm, Sweden, 2008

[DEPB12] Davis, J., Edgar, T., Porter, J., Bernaden, J., Sarli, M. Smart Manufacturing, Manufacturing Intelligence and Demand-Dynamic Performance, Comput. Chem. Eng. 47 (2012) 145–156.

[ECDSM16] EC Digital Single Market, Press release. "Commission sets out path to Digitize European Industry". Online available: https://ec.europa.eu/digital-single-market/en/news/commission-sets-out-path-digitise-european-industry, Last accessed: February 2018

[ENISA-15] ENISA, *Information Security and Privacy Standards for SMEs,* 2015.

[ENISA16] ENISA. Cyber Security and Resilience of Smart Cars: Good Practices and Recommendations (2016)

[FNMM12] S. Faltinski, O. Niggemann, N. Moriz, A. Mankowski, AutomationML: From Data Exchange to System Planning and Simulation, 2012 IEEE International Conference on Industrial Technology (ICIT), Athens, Greek.

[GABK16] Gabor, T., Belzner, L., Kiermeier, M. A Simulation-Based Architecture for Smart Cyber-Physical Systems. IEEE International Conference on Autonomic Computing (ICAC) 2016:374–379. (2016)

[GAFN15] Garetti, M., Fumagalli, L., Negri, E. Role of Ontologies for CPS Implementation in Manufacturing, MPER-Manag. Prod. Eng. Rev.6, 26–32. (2015)

[GRIE14] M. Grieves. Digital Twin: Manufacturing Excellence through Virtual Factory Replication, 2014.

[GRVI17] Grieves, M., Vickers, J. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. in Kahlen F-J. Flumerfelt, S., Alves, A., (Eds.) Transdisciplinary Perspectives on Complex Systems: New Findings and Approaches, Springer International Publishing, pp. 85–113. (2017)

[HAAN18] Haag, S. and Anderl, R. Digital Twin - Proof of Concept. Manufacturing Letters, (2018) Online: https://doi.org/10.1016/j.mfglet.2018.02.00

[HAJO17] Hardin, C., Josey, A. Standards to Unlock Smart Automotive Potentials. (2017) Online: http://www.newelectronics.co.uk/electronics-technology/standards-to-unlock-smart-automotive-potential/153291/

[HEPO15] Herman, M., Pentek, T., Otto, B. Design Principles for Industrie 4.0 Scenarios: A Literature Review. Technische Universität Dortmund. Audi Stiftungslehrstuhl Supply Net Order Management (2015).

[HOLN17] Hochhalter, J., Leser, W.P., Newman, J.A. Coupling Damage-Sensing Particles to the Digital Twin Concept. NASA Center for AeroSpace Information. (2014)

[IIRA-RAMI17] Shi-Wan Lin, Brett Murphy, Erich Clauer, Ulrich Loewen, Ralf Neubert, Gerd Bachmann, Madhusudan Pai, Martin Hankel, 2017. "Architecture Alignment and Interoperability: An Industrial Internet Consortium and Plattform Industrie 4.0 Joint Whitepaper," IIC:WHT:IN3:V1.0:PB:20171205. Online available: https://www.plattform-i40.de/I40/Redaktion/DE/Downloads/Publikation/whitepaper-iic-pi40.html

[IIRA17] Industrial Internet Consortium. The Industrial Internet of Things. Volume G1: Reference Architecture. IIC:PUB:G1:V1.80:20170131. Online available: https://www.iiconsortium.org/IIC_PUB_G1_V1.80_2017-01-31.pdf (2017)

[ISO15288-15] ISO15288, "Systems and software engineering -- System life cycle processes," ISO/IEC/IEEE, 2015.

[ISO15408-09] ISO15408, "Common Criteria for Information Technology Security Evaluation," Common Criteria, 2009.

[ISO18404-15] ISO18404, "Quantitative methods in process improvement – Six Sigma – Competencies for key personnel and their organizations in relation to Six Sigma and Lean implementation," ISO, 2015.

[ISO27002-13] ISO27002, "ISO 27002 Information technology - Security techniques - Code of practice," ISO/IEC, 2013.

[ISO27005-11] ISO27005, "Information Technology–Security Techniques–Information Security Risk Management," ISO/IEC, 2011.

[ISO27017-15] ISO27017, "ISO 27017 Information technology - Security techniques," ISO/IEC, 2015.

[ISO29169-16] ISO29169, "Information technology -- Process assessment -- Application of conformity assessment methodology to the assessment to process quality characteristics and organizational maturity," ISO/IEC, 2016.

[ISO33052-16] ISO33052, "Information technology -- Process reference model (PRM) for information security management," ISO/IEC TS, 2016.

[ISO9001-15] ISO9001, "Quality management systems -- Requirements," ISO, 2015.

[ITS 278] CEN/TC 278 ITS Standardization. Online: http://www.itsstandards.eu/cits

[JAZD14] Jazdi, N. Cyber Physical Systems in the Context of Industry 4.0, In: Autom. Qual. Testing, Robot. 2014 IEEE Int. Conf., 2014: pp. 1–4.

[KAWJ13] Kagermann, H., Wahlster, W., Johannes, H. Recommendations for Implementing the Strategic Initiative Industrie 4.0. (2013).

[KHJM99] Koren, Y., Heisel, U., Jovane, F., Moriwaki, T., Pritschow, G., Ulsoy, G., Van Brussel, H.. Reconfigurable Manufacturing Systems, Annals of the CIRP, 48 (2), 527-540, (1999).

[KLCK16] Kang, H.S., Lee, J.Y., Choi, S., Kim, H., Park, J.H., Son, J.Y., Kim, B.H., Noh, S.D. Smart Manufacturing: Past Research, Present Findings, and Future Directions. International Journal of Precision Engineering and Manufacturing-Green Technology, 3, pp. 111–128 (2016)

[KOSH10] Koren, Y., Shpitalni, M. Design of Reconfigurable Manufacturing Systems. Journal of Manufacturing Systems, 29(4), 130-141. (2010)

[KRAF16] Kraft, E.M. The Air Force Digital Thread/Digital Twin - Life Cycle Integration and Use of Computational and Experimental Knowledge, in: 54th AIAA Aerospace Sciences Meeting, AIAA SciTech Forum, 2016.

[KUAB17] Kucera, R., Aanenson, M. and Benson, M.: The Augmented Digital Twin: Combining Physical and Virtual Data to Unlock the Value of IoT. White paper (2017)

[LEBK15] Lee, J., Bagheri, B., Kao, H. A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems, Manuf. Lett. 3, 18–23. (2015)

[LEE08] Lee, E.A. Cyber Physical Systems: Design Challenges. In 2008 11th IEEE International Symposium on Object and Component-Oriented Real-Time Distributed Computing, 363–369. (2008)

[LEE15] Lee, J. Smart Factory Systems. Informatik-Spektrum 38, 230–235. (2015)

[LEKY14] Lee, J., Kao, H., Yang, S. Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. In: Procedia CIRP, Elsevier B.V., 2014: pp. 3–8.

[LFKF14] Lasi, H., Fettke, P., Kemper, H. G., Feld, T., Hoffmann, M. Industry 4.0. Business & Information Systems Engineering, 6(4), 239. (2014)

[MIL-STD-31000A] MIL standard. Online available from: http://23.96.237.142/wp-content/uploads/2015/10/MIL-STD-31000A-released-on-ASSIST-3-13-2013.pdf Last accessed: March 2018.

[MOEL16] Möller, D.P. Digital Manufacturing/Industry 4.0. In: Guide to Computing Fundamentals in Cyber-Physical Systems, 307-375. Springer International Publishing. (2016).

[MONO14] Monostori, L. Cyber-Physical Production Systems: Roots, Expectations and R&D Challenges. In Variety Management in Manufacturing Proceedings of the 47th CIRP Conference on Manufacturing Systems 17, 9–13. (2014)

[MTConnect-1] MTConnect Institute, 2014. MTConnect Standard, Version 1.3, Standard. URL http://www.mtconnect.org/standard-documents. (Last accessed June 2017)

[MTConnect-2] MTConnect Institute, 2017. Reference MTConnect Schemas, Standard. URL http://schemas.mtconnect.org/ (Last accessed June 2017)
[NAKR15] Nakrani, P.K.: Smart Car Technologies: A Comprehensive Study of the State of the Art with Analysis and Trends. A MSc Thesis, Arizona State University (2015)
[NEFM17] Negri, E., Fumagalli, L., Macchi, M. A Review of the Roles of Digital Twin in CPS-based Production Systems. In Proceedings of the 27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy. Procedia Manuf 2017; 11:939–48. 2017.
[NIST-8107] Y. Lu, K.C. Morris, S. Frechette, 2016. NISTIR 8107 Current Standards Landscape for Smart Manufacturing Systems. Online available from: http://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8107.pdf Last accessed: March 2018.
[NIST-CSF-14] NIST-CSF, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2014.
[oneM2M-BaseOntology] oneM2M Base Ontology. Online available from: https://git.onem2m.org/MAS/BaseOntology and from: http://onem2m.org/technical/onem2m-ontologies
[oneM2M-REQ16] oneM2M Technical Specification: Requirements. August 2016. Online: http://www.onem2m.org/images/files/deliverables/Release2/TS-0002-Requirements-V2_7_1.pdf (last accessed March 2017)
[oneM2M16] F. Ennesser and Y. Shah, 2016. Security solutions and services for the IoT. IoThink Thought Leader Series. February 2016. Online available at: http://bit.ly/2mZuDte (last accessed March 2017)
[oneM2M17] oneM2M, 2017. Smart Cities done Smarter. White paper, February 2017. Online: http://www.onem2m.org/images/files/oneM2M_WhitePaper_SmartCitiesDoneSmarter.pdf (last accessed March 2017.
[PEAA18] Perales, D.P, Alarcón, F., Boza, A. Industry 4.0: A Classification Scheme. Closing the Gap Between Practice and Research in Industrial Engineering. pp. 343-350. (2018)
[RAMI4.0] ZVEI. Reference Architectural Model Industrie 4.0 (RAMI 4.0), Status report. 2015. https://www.vdi.de/fileadmin/vdi_de/redakteur_dateien/gma_dateien/6092_PUB_E_TW_GMA_Status_Report_ZVEI_-_Industrie_4_0_-_Technical_Assets_Internet.pdf
[REMM13] Reifsnider, K., Majumdar, P., Multiphysics Stimulated Simulation Digital Twin Methods for Fleet Management. 54th AIAA/ASME/ ASCE/AHS/ASC Structures, Structural Dynamics, and Materials Conference 1578. (2013)
[RHOM15] Rios,, J., Hernandez,, J.C., Oliva,, M., and Masb, F. Product Avatar as Digital Counterpart of a Physical Individual Product: Literature Review and Implications in an Aircraft System. In: ISPE CE: pp. 657–666. (2015).
[RMJP16] Razzaque, M.A., Milojevic-Jevric, M., Palade, A. and Clarke, S. Middleware for Internet of Things: A Survey. In IEEE Internet of Things Journal, Vol. 3, No. 1 (2016)
[ROWL15] Rosen, R., von Wichert, G., Lo, G., Bettenhausen, K.D. About the Importance of Autonomy and Digital Twins for the Future of Manufacturing. IFAC- PapersOnLine 2015;48(3):567–72. 2015.
[SABA00] Sarma, S., Brock, D.L., Ashton, K. The Networked Physical World, 2000.
[SAMW17] Schleich, B., Anwer, N., Mathieu, L., Wartzack, S. Shaping the Digital Twin for Design and Production Engineering. In CIRP Annals - Manufacturing Technology. Pp. 141-144. (2017)
[SAMW17] Schleich, B., Anwer, N., Mathieu, L., Wartzack, S. Shaping the Digital Twin for Design and Production Engineering. In CIRP Annals - Manufacturing Technology. Pp. 141-144. (2017)
[SCRO16] Schluse, M. , Rossmann, J. From Simulation to Experimentable Digital Twins - Simulation-based Development and Operation of Complex Technical Systems. In: Second IEEE International Symposium on Systems Engineering (ISSE 2016), October 3–5, Edinburgh, Scotland, pp. 273–278, IEEE, 2016.
[SHAF10] Shafto, M., Conroy, M., Doyle, R., Glaessgen, E., Kemp, C., LeMoigne, J., Wang, L. NASA Technology Roadmap: DRAFT Modeling, Simulation, Information Technology & Processing Roadmap Technology Area. (2010)
[SHAF12] Shafto, M., Conroy, M., Doyle, R., Glaessgen, E., Kemp, C., LeMoigne, J., Wang, L. NASA Technology Roadmap: Modeling, Simulation, Information Technology & Processing Roadmap Technology Area. (2012)

[SSST15] Shafiq, S.I., Sanin, C., Szczerbicki, E., Toro, C. Virtual Engineering Object / Virtual Engineering Process: A Specialized Form of Cyber Physical System for Industrie 4.0. In Procedia Computer Science, Vol. 60, 2015.

[STOU11] K. F. J. a. S. K. Stouffer, *Sp 800-82. Guide to industrial control systems (ics) security: Supervisory control and data acquisition (scada) systems, distributed control systems (dcs), and other control system configurations such as programmable logic controllers (plc),* 2011.

[TAHO18] Tavčar, J. and Horváth, I. A Review of the Principles of Designing Smart Cyber-Physical Systems for Run-Time Adaptation: Learned Lessons and Open Issues. In IEEE Transactions on Systems, Man, and Cybernetics: Systems. (2018) Online available: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8329014&isnumber=6376248

[WEGE17] Wegener, D. "Industrie 4.0" bedeutet die Verschmelzung von Office Floor mit Shop Floor. Zvei Die Elektoindustrie. (2017)

[WWLZ16] Wang, S., Wan, J., Li, D., Zhang, C. Implementing Smart Factory of Industrie 4.0: An Outlook. International Journal of Distributed Sensor Networks, 7. (2016)

[YOSS12] Yoon, J. S., Shin, S. J., & Suh, S. H. A Conceptual Framework for the Ubiquitous Factory. International Journal of Production Research, 50(8), 2174-2189. (2012)

[ZUEH10] Zuehlke, D. SmartFactory - Towards a Factory-of-Things. In Annual Review in Control. (2010). Online: http://foresight.ifmo.ru/ict/shared/files/201311/1_124.pdf