Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P0372-cd

IEC common data dictionary for functional safety in the process industries

Shenae Lee

Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: shenae.lee@sintef.no

Mary Ann Lundteigen

Dept. of Engineering Cybernetics, NTNU, Norway. E-mail: mary.a.lundteigen@ntnu.no

Solfrid Håbrekke

Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: solfrid.habrekke@sintef.no

Maria Vatshaug Ottermo

Software Engineering, Safety and Security, SINTEF Digital, Norway. E-mail: maria.v.ottermo@sintef.no

Andreas Schueller

Automation Engineering, YNCORIS GmbH & Co. KG, Germany. E-mail: andreas.schueller@yncoris.com

A key aspect of Industry 4.0 is machine-to-machine data sharing, facilitated by emerging technologies like the asset administration shell (AAS) and OPC UA. However, the exchange of domain-specific data can be impeded if a standardized semantic for the domain is not established. For this reason, standardized data repositories for multiple industrial domains have been under development, and the most common examples are IEC Common Data Dictionary (CDD) and ECLASS. IEC CDD is designed to provide standardized data in a machine-readable format for the IEC and ISO standards. However, the current version of IEC CDD, as of 2024, has not fully integrated domain-specific terms related to functional safety in the process industries, including only a very short list of such terms. This represents a significant limitation for information exchange in this sector. As a response to this, the ongoing research project called Automated Process for Follow-up of Safety Instrumented Systems (APOS) has taken the initiative to integrate the functional safety domain into IEC CDD, focusing on key concepts in functional safety for the process industries. This paper reports the groundwork needed to incorporate two key standards in functional safety for process industries, IEC 61508 and 61511.

Keywords: IEC common data dictionary, Machine-readable, functional safety, IEC 61511, IEC 61508, Industry 4.0, Interoperability

1. Introduction

With Industry 4.0 significantly evolving over the past decade, digital twin technologies have been increasingly adopted in several industrial sectors (Khan 2024). A digital twin can, as a digital representation of an asset, be realized by the asset administration shell (AAS), a framework developed by the companies engaged in the Platform Industrie 4.0. The AAS enables standardized and interoperable information models such that the data contained in the AAS can be exchanged for any asset and between different stakeholders (PlattformI4.0 2020). An AAS organizes data into submodels, which are defined for a specific domain or specific subject matter (Schnicke et al. 2022). A submodel consists of submodel elements, which refers to elements that provide description and differentiation of assets (PlattformI4.0 2020). Numerous applications of the AAS are currently under development in different sectors (Attaran and Celik 2023), as demonstrated by the AAS submodel templates published by the industrial digital twin association (IDTA) (IDTA 2024).

The ongoing research project, Digital lifecycle management of interoperable safety systems (APOS 2.0), aims to establish AAS submodel templates for functional safety in the

process industries. As part of this project, a collaboration has been established with the User Association of Automation Technology in Process Industries (NAMUR) working groups on digitalization and tools, who share the same interest and effort. Together with NAMUR, the APOS 2.0 project has proposed a dedicated working group (WG) within the IDTA, which was officially approved in July 2024. This WG involves experts from the process industry, covering manufacturers as well as end users. The primary focus is to agree on relevant data, along with the data structures for the AAS submodel templates designed for safety instrumented systems (SIS).

The choice to focus on SIS stems from its critical importance in ensuring safety. A SIS is used to protect process equipment against dangerous process situations (e.g. high pressure) that can possibly result in severe safety consequences. It is, therefore, important to ensure that the SIS can achieve the desired performance and to monitor SIS performance throughout its lifecycle. SIS performance management requires a large amount of technical and operational data, which involves a substantial load of manual work today. For this reason, the APOS 2.0 project defined an AAS use case for SIS that contains essential design and operational information related to SIS lifecycle performance management, as illustrated in Fig. 1. The APOS 2.0 project runs several pilots where the new templates are tested for exchange of data between existing digital tools for SIS design requirements, reliability analysis, and maintenance management.

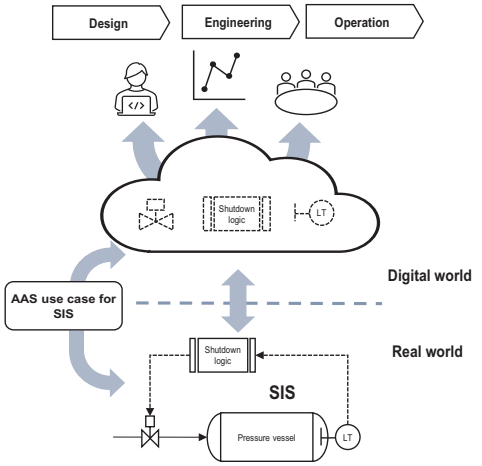

Fig. 1. Uses case of the AAS applied for SIS related information.

1.1 Data repositories for AAS submodels

An important feature of any AAS is its capability to reference external data repositories that contain domain-specific terms. A repository can be understood as a compilation of data dictionaries of different domains and standards. A data dictionary provides semantic definitions of terms and associated semantic attributes like unique machine-readable codes, data types, and value lists. Submodel elements can directly refer to an object in a data dictionary so that different AAS submodels can have global reference to external and interpret data in a consistent manner.

There are several publishers of such data repositories, with representative examples like the IEC common data dictionary (CDD) (IEC CDD, n.d.) and ECLASS (ECLASS, n.d.), and CFIHOS (CFIHOS 2020). IEC CDD is aimed at providing data models for all IEC and ISO standards, while the current version as of November 2024 includes a few selected IEC standards, such as IEC 61987 (IEC 61987 2009) and IEC 62683 (IEC 62683 2017). ECLASS is designed to provide product classifications and descriptions for different industry sectors, publishing a new version annually. The latest version, Release 15.0 from 2024 integrates thirty-nine sectors.

1.2 Data repositories for functional safety in the process industry

The IDTA submodel template for functional safety in the process industry will encompass the concepts and terms in IEC 61511 (IEC 61511 2016), the primary standard on functional safety in the process industry domain, as well as IEC 61508 (IEC 61508 2010), the standard on general functional safety across all sectors. For this reason, this submodel template will contain numerous properties that are defined in the scope of IEC 61508 and IEC 61511, in other words, properties related to SIS and safety instrumented functions (SIF), specific functions implemented by the SIS. Especially, it is crucial that the template contains information from the safety requirement specification (SRS), a document collecting information required by IEC 61511.

However, the current versions of IEC CDD and ECLASS includes only a limited subset of terms in IEC 61508 and has not incorporated specific terms from IEC 61511. Although a few recent amendments into IEC CDD organized under

the standard IEC 61987 series (IEC 61987 2009) integrates functional safety terms related to machinery safety, these amendments are not sufficiently comprehensive to cover a vast array of widely used terms in the scope of IEC 61508 and IEC 61511. Therefore, the APOS 2.0 project has initiated a specific activity to integrate terms and concepts from these standards, and this is a crucial part of developing he submodels for the SIS and SIF.

The main objective of this paper is to give a brief overview of IEC CDD to introduce the way forward to incorporate terms and definitions from IEC 61508 and IEC 61511 into IEC CDD. In this paper, IEC CDD is considered as a preferred candidate over ECLASS for implementing a data dictionary for IEC 61508 and IEC 61511. The main reason is that even though ECLASS is extensive in its outreach and overlaps and complements in some areas with IEC CDD, IEC CDD is considered to secure a more formal and open process and wider adaptation of ISO and IEC standards. In addition, IEC CDD shares all the data openly, unlike ECLASS where a license is required for full access to its features.

2. IEC CDD information objects

The current version of the IEC CDD database (Version: V2.0018.0001) integrates six data dictionaries, as shown in Fig. 2. Each of these dictionaries integrates a specific IEC standard domain and has its own data model.

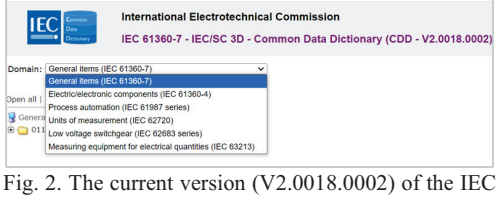

Fig. 2. The current version (V2.0018.0002) of the IEC CDD integrates six IEC domains as of November 2024.

IEC 61360-1 (IEC 61360-1 2017) defines different information objects in the IEC CDD and the relationship between them. Essential information objects in the IEC CDD are class, property, and attributes. A class is an abstraction of a set of similar products, and classes can be organized into a hierarchy. A property represents a characteristic for a class of elements or a data element. A property can have predefined values identified. Each piece of information about a class and a property in the IEC CDD data dictionaries is called an attribute. The attributes and their associated values for the property 'mean time between failures' is shown in Fig. 3.

Code:	0112/2///61987#ABB016
Version:	004
Revision:	01
IRDI:	0112/2///61987#ABB016#004
Preferred name:	mean time between failures
Synonymous name:	
Symbol:	
Synonymous symbol:	
Short name:	
Definition:	expectation of the operating time between failures
Note:	
Remark:	
Primary unit:	y
Alternative units:	
Level:	
Data type:	REAL_MEASURE_TYPE
Format:	
Property constraint:	
Definition source:	IEV 191-12-09 (modified)
Property data element type:	NON_DEPENDENT_P_DET
Drawing:	
Formula:	
Value list code:	
Value list:	
DET class:	
Applicable classes:	0112/2///61987#ABD877 - Functional safety and reliability [2] 0112/2///61987#ABC257 - Functional safety and reliability
Definition class:	0112/2///61987#ABA000
Code for unit:	0112/2///62720#UAB026 - year
Codes for alternative units:	
Code for unit list:	0112/2///61987#ABT511 - Time/time duration long
Status level:	Standard

Attributes

Fig. 3. A set of attributes for the property 'mean time between failure'.

3. Suggested amendments for IEC CDD for IEC 61511

The APOS 2.0 project conducted a detailed review of the existing contents related to functional safety within the current IEC CDD. This review concluded that the current contents are not complete when compared with the scope of IEC 61511. For this reason, the project has initiated the work to introduce an extended list of terms related to IEC 61511 in a consistent manner.

3.1. Existing *data relevant for the functional safety in the process industry*

IEC CDD already integrates terms and definitions from the standard IEC 61987 on the list of properties (LOP) for equipment in the process automation domain. Here, IEC 61987 defines a LOP as a 'predefined group of classes and properties with the purpose to characterize equipment'. LOP is split into two categories: Device list of properties (DLOP) and operating list of properties (OLOP), where the DLOP describes device characteristics, while the OLOP describes operational conditions for their use.

The IEC CDD for IEC 61987, therefore contains OLOPs and DLOPs for various automation equipment, including different types of actuated valves and transmitters. For instance, DLOPs for the equipment type 'differential pressure transmitter' in IEC CDD includes properties and classes like 'measuring principle', 'maximum output current', and 'type of device diagnostic'. Examples of OLOPs defined for the equipment type 'pressure measuring device' include 'maximum ambient temperature', 'phase type' and 'method of cleaning'.

The focus of IEC 61987 has been on general automation equipment properties and not safety aspects. Therefore, the APOS project (Automated process for follow-up of safety systems) (Hauge et al. 2023) proposed a set of DLOP and OLOP that are selected among the with the most influence on the reliability of SIS, referred to as reliability-influencing properties.

Such properties have been found useful for grouping of SIS equipment, also in an IEC CDD context. For instance, the value of the DLOP 'measuring principle' will influence the reliability of level transmitters and thus can be used for grouping level transmitters into detailed device types like 'capacitance level transmitter', 'displacer level transmitter', and 'ultrasonic level transmitter'. Unfortunately, the existing DLOPs and OLOPs in IEC CDD do not fully cover all the properties relevant to characterize the reliability performance of SIS. Besides such reliability influencing properties that are missing, the current IEC CDD also lacks properties normally included in the SRS.

The IDTA submodel template titled 'Functional safety', published in 2022, specifies the data models to be used for the safety-related control systems in the scope of machinery safety standards like IEC 62061(IEC 62061 2021). This submodel template includes a set of properties included in the class 'Functional safety and reliability', which currently is a part of IEC CDD for IEC 61987. However, the class 'Functional safety and reliability' is limited to twenty properties as shown in Fig. 4.

The APOS 2.0 project revealed that these were not well suited as a reference for the submodels for the SIS and SIF process industry. One main reason was that this class focused on machinery safety, meaning that a lot of properties relevant to the process industry were not represented. Examples of missing properties are 'SIF description', 'probability of failure on demand', 'maximum allowed spurious trip rate', and 'demand rate', which are typically included as a part of the SRS in the scope of IEC 61511. Hence, it is necessary to create a more extensive list of classes and properties related to SIS and SIF.

Fig. 4. Properties related to functional safety included in the current IEC CDD.

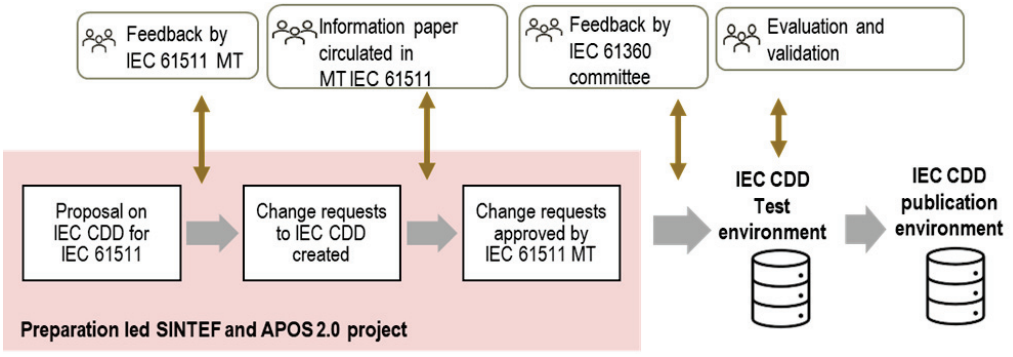

Fig. 5 Workflow for incorporating functional safety terms into IEC CDD.

3.2. *Initiative towards a new CDD by the APOS 2.0 project*

The APOS 2.0 project is currently working on preparing an extended list of classes and properties in the scope of IEC 61511 and IEC 61508 for their inclusion in the IEC CDD. The workflow of this process is illustrated in Fig. 5. The process involves preparatory phases to formulate formal change requests (CRs) to the IEC CDD. The submitted CRs will be subject to quality checks before entering into the IEC CDD test environment. Fig. 6 provides a simplified illustration of how the new proposed classes and properties can be organized in a structured manner within the IEC CDD repository environment. It should be noted that creating these CRs requires close collaboration with the maintenance team (MT) for IEC 61511, referred to as MT 61511. In addition, the coordination between MT 61511 and MT 61508 will be needed to ensure that the concepts from IEC 61508 and IEC 61511 are incorporated into the IEC CDD in a coherent manner, avoiding potential overlaps between terms and ambiguity. However, it is expected that the alignment and coordination process between MT 61511 and MT 61508 will require manual efforts by the members, which is resource-demanding in terms of man hours. Moreover, the agreement should be made on how the terms are organized into classes and properties in the IEC CDD. Such work will necessitate several iterations to minimize any repetitions of terms and to achieve the most reasonable data structure. For this reason, feedback and approval from MT 61511 and MT 61508 are prerequisites to ensure that proposed CRs align with the concepts and terms defined in the existing IEC 61508 and IEC 61511.

3.3. *Semi-formal ontology for SRS*

An important groundwork for creating a new IEC CDD for the functional safety domain is establishing a semi-formal "ontology" for the SRS. By semi-formal "ontology" for the SRS, we here mean a definition of terms and their relations in the understanding of the SRS requirements in IEC 61511. Considering that SRS documents written in the human-readable formats pose a major limitation for efficient digital exchange, the identification of terms within the SRS and their relations is considered essential for machine-to-machine data exchange of requirements among different stakeholders and across different lifecycle phases of the SIF.

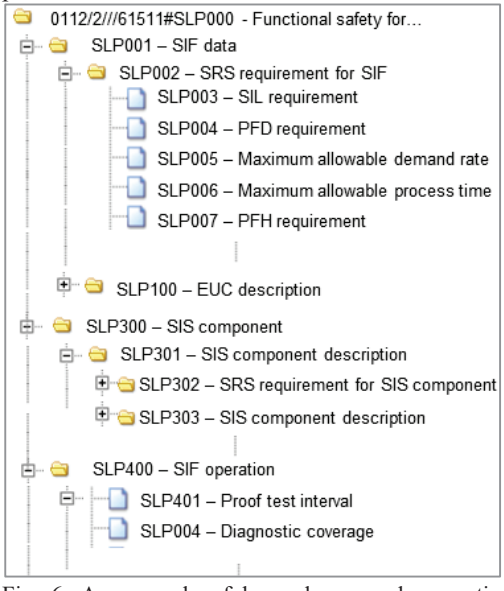

Fig. 6. An example of how classes and properties related 'functional safety for the process industry' can be incorporated into IED CDD.

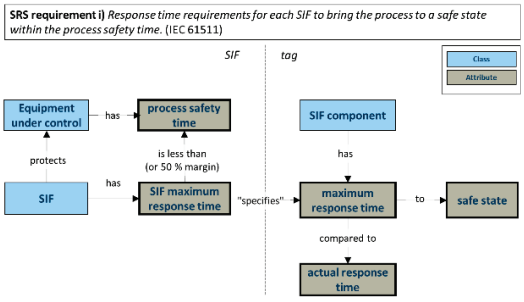

Fig. 7. An example of a semi-ontology map for SRS requirement i) from IEC 61511.

The APOS 2.0 project has established a semi-formal ontology for all the SRS requirements through several work meetings with representatives from oil and gas operators, vendors, engineering companies, contractors, consultants, and researchers. Compiling and integrating all the SRS requirements under some defined rules will form the basis for a more comprehensive information model for the SRS. Every term in the SRS semi-ontology will likely correspond to either a class, a property, or a value in both the IEC CDD and in the AAS submodels for functional safety.

An example of a semi-ontology map for one of the SRS requirements from IEC 61511 is shown in Fig. 7. This requirement (in prose) is broken down into possible classes such as equipment under control, SIF and SIF component, and attributes such as process safety time, and attributes such as process safety time, safe state and required response times. These are all classes and attributes representing known terms and are important to add to the IEC CDD with a proper definition and machine-readable code.

4. Concluding remarks

The integration of functional safety for the process industry domain into the IEC CDD will provide better alignment with IEC 61508 and 61511, enabling interoperable digital twins of the SIS and SIF in the process industry. This will promote a standardized way of using functional safety terms for different stakeholders in the SIS development projects, ranging from the manufacturer to the end-users. This work is not stand-alone, but part of a work to develop new AAS submodel templates for functional safety in the process industry.

The combination of submodel development for functional safety in the process industry with the development of the IEC CDD for IEC 61508 and IEC 61511 will play a key role to facilitate more seamless data exchange among different tools used in the industry and across the lifecycle of SIS. The reason is that the AAS submodels referencing IEC CDD dictionaries can facilitate the enhanced consistent use of terms in different software used in the process industry. This represents important steps in digitalizing the SIS performance management. It can also serve as groundwork to develop a formal ontology for the domain.

Acknowledgement

The paper presents results from APOS 2.0, a joint industry project on the digital lifecycle management of interoperable safety systems and the PDS forum. The APOS 2.0 project is supported by the Norwegian Research Council (Project no. 341194) and 9 industry partners representing oil companies, engineering, consultants, and vendors of control and safety systems. PDS forum is a co-operation between 30 participants representing oil companies, engineering companies, consultants, vendors, and researchers, with a special interest in safety instrumented systems. We also thank the members of the IDTA working group "Safety instrumented functions (SIF) for the process industries" and Klaus Dickmann from the IEC Subcommittee 3D, responsible for the development for IEC CDD, for valuable discussions.

References

Attaran, Mohsen, and Bilge Gokhan Celik. 2023. "Digital Twin: Benefits, Use Cases, Challenges, and Opportunities." *Decision Analytics Journal* 6 (March):100165. https://doi.org/10.1016/j.dajour.2023.100165.

CFIHOS. 2020. "CFIHOS - Specification Document." International Association of Oil & Gas Producers (IOGP).

ECLASS. n.d. ECLASS. Accessed May 27, 2024. https://eclass.eu/support/technical-specification/data-model/conceptual-data-model.

Hauge, Stein, Solfrid Håbrekke, Mary Ann Lundteigen, Shenae Lee, and Maria Vatshaug Ottermo. 2023. "Guidelines for Standardised Failure Reporting and Classification of Safety Equipment Failures in the Petroleum Industry, Ed. 1 (Open Version) (APOS H1)." SINTEF Report 2023:00108.

IDTA. 2024. “Industrial Digital Twin Association (IDTA).” IDTA. November 4, 2024. https://industrialdigitaltwin.org/en/.

IEC 61360-1. 2017. “IEC 61360-1. Standard Data Element Types with Associated Classification Scheme - Part 1: Definitions - Principles and Methods.” Geneva: International Electrotechnical Commission.

IEC 61508. 2010. “IEC 61508 - Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems.”

IEC 61511. 2016. *Functional Safety: Safety Instrumented Systems for the Process Industry Sector, Part 1-3.* Geneva: International Electrotechnical Commission.

IEC 61987. 2009. “IEC 61987-10. Industrial-Process Measurement and Control - Data Structures and Elements in Process Equipment Catalogues - Part 10: List of Properties (LOPs) for Industrial-Process Measurement and Control for Electronic Data Exchange - Fundamentals.” Geneva: International Electrotechnical Commission.

IEC 62061. 2021. “IEC 62061. Safety of Machinery - Functional Safety of Safety-Related Control Systems.”

IEC 62683. 2017. “IEC 62683-1:2017 Low-Voltage Switchgear and Controlgear - Product Data and Properties for Information Exchange - Part 1: Catalogue Data.”

IEC CDD. n.d. “IEC - Common Data Dictionary (CDD). Geneva: International Electrotechnical Commission.” Accessed November 27, 2024. https://cdd.iec.ch/cdd.

Khan, Tarique Hasan. 2024. “Redefining Value Creation: Assessing the Economic Impact of Digital Twin Technology Across Industries.”

PlattformI4.0. 2020. “Details of the Asset Administration Shell - Part 1: The Exchange of Information between Partners in the Value Chain of Industrie 4.0.” Version 3.0RC01. Plattform Industrie 4.0.

Schnicke, Frank, Thomas Kuhn, Tobias Klausmann, Sten Grüner, and Daniel Porta. 2022. “Architecture Blueprints for the Application of the Industry 4.0 Asset Administration Shell.” In *2022 IEEE 27th International Conference on Emerging Technologies and Factory Automation (ETFA)*, 1–8. https://doi.org/10.1109/ETFA52439.2022.9921694.