Digitalization of functional safety for Industrie 4.0 and Intelligent Manufacturing

IMS 国家智能制造标准化总体组
智能制造标准化
National Intelligent Manufacturing Standardisation Administration Group

STANDARDIZATION COUNCIL INDUSTRIE 4.0

GPQI

IMPRINT

Published by
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

Registered office
Bonn and Eschborn, Germany

Globalprojekt Qualitätsinfrastruktur
Tayuan Diplomatic Office Building
No. 14, Liangmahe Nanlu, Chaoyang
100600 Peking, VR China
info@gpqi.org I www.gpqi.org

Design
Oliver Hick-Schulz

Photos
Cover: gesrey/iStock

On behalf of
Bundesministerium für Wirtschaft und Energie (BMWE)
Berlin, Deutschland 2025
Peking, VR China 2025

Text
Global Project Quality Infrastructure

Authors and experts
TEG Functional Safety & Predictive Maintenance: **Peter Sieber**, HIMA, **Wenze Xiong**, ITEI,
Wang Chengcheng, ITEI, **Marco Turdo**, HIMA, **Michael Niehaus**, Lenze, **Volker Hirsch**, Siemens

The Federal Ministry for Economic Affairs and Energy (BMWE) has commissioned the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) to implement the Global Project on Quality Infrastructure.

Implemented by

Federal Ministry for Economic Affairs and Energy

giz Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH

CONTENTS

1 **INTRODUCTION** 4
2 **INTEROPERABILITY BETWEEN EXISTING TOOLS USING THE AAS FUNCTIONAL SAFETY REQUIREMENTS** 5
2.1 Safety Requirement Specification 5
2.2 The Verification of Safety Designs 5
2.3. Device Verification 5
2.4. The Performance Monitoring of Safety Functions Under Operation 6
3. **FUNCTIONAL SAFETY AND DIGITALIZATION** 7
4. **INFORMATION MODEL FOR FUNCTIONAL SAFETY** 9
4.1. Basics of the Asset Administration Shell for Functional Safety 9
4.2. Functional Safety Life Cycle Utilizing Administration Shells 10
5. **UTILIZATION OF THE ASSET MANAGEMENT SHELL** 11
5.1. Introducing SIF Performance Monitoring 11
5.2. Digitalized Safety Design 12
5.2.1. Digitalized Hazard and Risk Analysis (HARA) 12
5.2.2. Digitalized Safety Requirement Specification 12
5.2.3. Digitalized SIF Implementation 13
5.2.4. Digitalized Application Program Development 13
5.3. Digitalized Device Failure Data Handling 14
5.3.1. New Safety Data Handling Philosophy 15
5.4. Digitalized Functional Safety Life Cycle Management 16
5.4.1. Digitalized Operate and Maintain 16
5.4.2. Distribution of Test Results 17
5.5. Usage of Digital Twins 18
5.6. Safety Related Digital Twin 18
5.7. Concluding the Usage of Asset Administration Shells (AAS) 20
6. **SAFETY AND SECURITY** 21
6.1. General Consideration 21
6.2. Baseline for Communications 23
7. **CONCLUSION** 23

1 INTRODUCTION

This white paper aims to find the differences in the understanding of IEC standards between China and Germany by analyzing factors such as technology, use cases, culture, and legal framework, and based on that, to develop ideas on the potential content of future synchronized standards. Separate from this document, there are documents under preparation focusing on:

- Digitalization of predictive maintenance

- OT security in view of the digitalization of functional safety and predictive maintenance

Problem statement:
The motivation for this document is that, in terms of functional safety, the processes and procedures that we currently have in place were developed in times when engineering was organized using pencils and papers. In recent years, tools have been developed that have replaced pencils and paper, but there are other challenges that remain:

- Lack of qualified personnel
- Cost of functional safety
- Lack of flexibility of functional safety when it comes to adaptations to be tackled

When looking at targets and benefits for a digitalization of the functional safety life cycle, the different target areas mentioned above need to be seen separately, where functionalities may be separated or combined in line with the preference of the individual operating company. However, a holistic approach, incorporating more functionalities under the same digital framework, is generally the preferred choice.

Hypothesis:
In the event that functional safety and i4.0 should be seen as something that co-exist, the handling of functional safety needs to be made more cost effective and flexible, while maintaining the targeted risk reductions.

In the event that functional safety and i4.0 should be seen as something that co-exist, the handling of functional safety needs to be made more cost effective and flexible, while maintaining the targeted risk reductions.

2 INTEROPERABILITY BETWEEN EXISTING TOOLS USING THE AAS FUNCTIONAL SAFETY REQUIREMENTS

Typically, different suppliers are engaged, meaning that different procedures and tools are used for design, design reviews, and modifications of safety functions. In addition, different technological areas need to be included when considering all life cycle activities, including:

- Hazard and risk analysis (e.g., HAZOP)
- Determination of SIL (e.g., LOPA)
- Safety requirement specification
- Functional design and implementation
- SIL reviews including FMEDA on device level
- Commissioning support (incl. factory and site acceptance tests)
- Operational monitoring
- Decommissioning

2.1 Safety Requirement Specification

An individual analysis is done for each kind of safety function. The baseline of such analyses is the determination of the different hazards to be compensated for. This process is called "HAZOP" or "HARA." When the hazards to be compensated for are identified, technical and organizational countermeasures are defined. The technical countermeasures are grouped into different independent layers. This process is called the "Layer of protection analysis (LOPA)".." One of these layers are is the "Safety Instrumented Functions (SIF)." The results of such analyses are function-specific only. Combining different devices like the transmitter, the logic solver, and actuators into one function is the major tasks of safety engineering. The result of these activities is the "Safety Requirement Specification." Once this specification is identified, the individual devices are specified.

Currently, this is done function by function. The use of qualified standard templates may be of help following the objectives under chapter 1.

2.2 The Verification of Safety Designs

At present, the verification of safety designs is done manually function by function.

For each function, the data sheets and safety manuals of all devices engaged – each with a dedicated functionality – are analyzed and the functions are individualized to the extent that for each safety function a complete set of verification documents is prepared.

By doing so, the overall safety function of a plant is made up of as many individual functions as there are safety functions.

The baseline is to take the individually documented functional requirements of the different functions, mirror them at the device properties (technical data, safety manual, etc.), and cross check in a paper-based procedure under which conditions the devices are going to fulfill the requirements set. This critical step is called verification.

This step focuses on the verification of designs, either when safety systems are implemented or when such functions are being modified.

2.3 Device verification

So far, the verification of devices used in safety functions is performed based on technical manuals, describing the device's abilities, as well as, where available, so-called safety manuals describing the safety-relevant behavior of the individual devices including the systematic capabilities of the device, e.g., the software capabilities of the device. This selection process is seen as a supplement to a process called "Prior Use," where practical experiences in using the devices under investigation are reviewed. This process is very time-consuming, as gathering practical experiences needs time. In addition, having more and more complex software at the individual devices, "Prior Use" results are to be viewed critically, because it's almost impossible to test all different device settings in when complex software is present.

Currently, the Failure Mode Effect Diagnostic Analyses (FMEDA) for complex electrical circuitries are typically done using digital tools. This review strategy is opening completely new possibilities.

For further details, please also refer to chapter 5.3.

2.4 The Performance Monitoring of Safety Functions Under Operation

Digital technology can introduce objective safety indicators, data, and recommendations to reduce the possibility of human error and effectively reduce system safety risks. This is done by collecting and analyzing data from all relevant sources, and provides consolidated information in the form of dashboards. Based on this information, the time and effort for maintaining safety functions can be optimized. In addition, for example, augmented reality opens up new possibilities for effectively training maintenance personnel.

For further details, please refer to chapter 8.

In this document, a particular focus is placed on the digitalization of functional safety in a broader sense, covering aspects of streamlining traditional processes and procedures, but also on the new possibilities that are feasible when applying digitalization from the bottom up.

3 FUNCTIONAL SAFETY AND DIGITALIZATION

Traditionally, the safety life cycle is organized following the idea that any kind of technical setup is verified by humans that have a deep understanding of the technology under review and are able to fully test each dedicated setup. This, depending on how and at which level of test confidence the verification is performed, may either be time-consuming or costly or entail risks, which in the end can prove even more costly.

In order to master the complexity when considering all aspects of functional safety, the overall safety life cycle management is currently broken up into different parts, reflecting the different components of a Safety Instrumented Function (SIF), as well as its related design documentation. On the one hand, this is beneficial as it allows each individual component to be understood as a testable black box. On the other hand, this introduces a new layer of complexity, as each component (sensors, logic solvers, actuators, and their interfaces) has its own safety life cycle in addition to the SIF's safety life cycle, which is required to coordinate all individual life cycle activities.

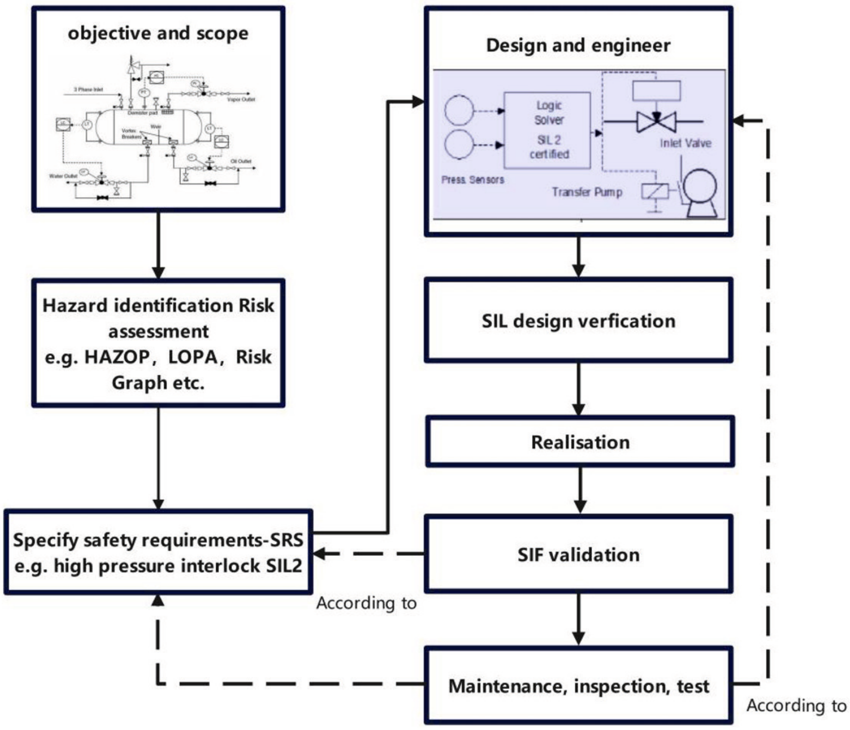

Figure 1: Functional Safety Life Cycle

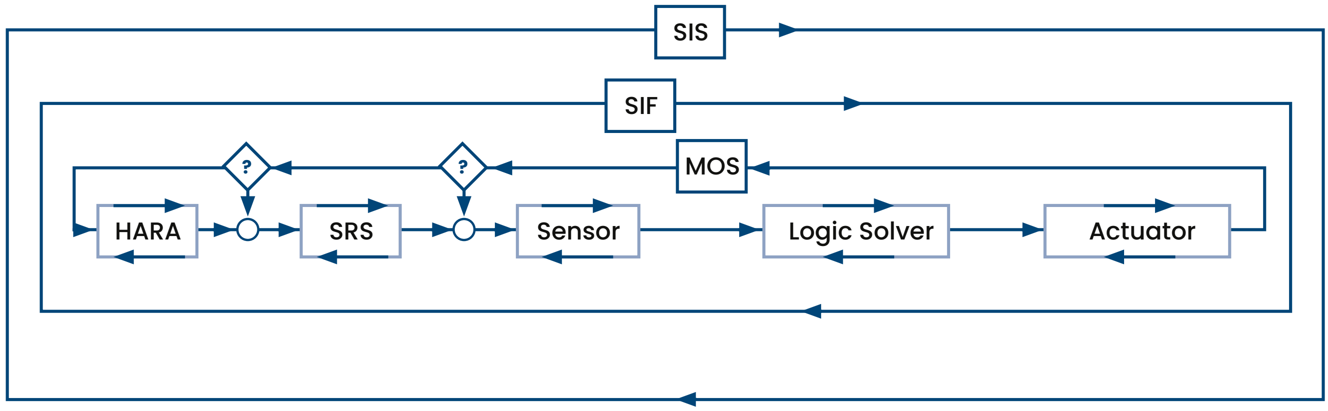

Figure 2: Traditional functional safety life cycle (simplified)

When using programmable Safety Instrumented Systems, there is another life cycle that we call SIS (see Figure 1), where aspects such as software updates and security aspects are handled. This is the traditional, but complex and costly way, to maintain function safety.

Digitalization, in principle, offers all that is needed to achieve this, but there are two important aspects to be considered:

1. Especially in brownfield situations, it's typically impossible to change all elements simultaneously, so a stepwise approach to introducing digitalization needs to be supported.

2. All benefits can be utilized when not only converting the existing data into the digital environment is done, but is requiring also reviewing the existing processes and procedures. When doing so, all life cycle phases, including the safety design phases and, of course, the management of change (MOC), need to be considered.

All this begins with modeling and handling the relevant data.

4 INFORMATION MODEL FOR FUNCTIONAL SAFETY

4.1. Basics of the Asset Administration Shell for Functional Safety

In parallel to the activities of the Sino-German Standardization Commission, other groups are also working on the definition of an information model (and subsequently a data model) for functional safety. Indeed, being that functional safety is a multidisciplinary topic that evolves during a predefined life cycle, its digitalization needs to be focused on the principles of interoperability, data exchange, scalability, and independency from technologies.

The clear aim is to ultimately create a digital twin that ensures functional safety through fully automated interaction between the digital representation and the actual system.

Even if the current document does not define a universally accepted information model for functional safety, this chapter provides key information to support this development, which aligns with the activities of other groups.

The most suitable way to define an interoperable information model for functional safety is through the Asset Administration Shell (AAS) philosophy: a standardized digital representation of assets parameters of different nature: physical (e.g., equipment), digital (e.g., documents), and intangible (e.g., software license). Working with AAS allows the user to decide the granularity of the information model for functional safety, which is not yet standardized; indeed, every SIF can be considered as being a composite AAS with a number sub-models to cover all the different asset categories.

Figure 3: Principle of an Asset Administration Shell

Figure 3 shows the principle of an Asset Administration Shell. The different parameters describing all the facets of a dedicated device (or function) are represented in a generic and unique way. The said information can be stored on the individual devices, but also on specific host devices (e.g., all transmitter parameters on a centralized data server). This allows effective storing of parameters that are identical to different devices of the same kind as well as making use of this data either at a digital twin of the physical set-up or to support functional safety life cycle activities.

4.2 Functional Safety Life Cycle Utilizing Administration Shells

Figure 4 shows the usage of Asset Administration Shells in the context of the functional safety life cycle. This concept represents the first phase of the digitalization of functional safety. Applying this concept means that the relevant data are transferred into a digital repository. This enables effective revision and change management of data related to functional safety; even though all other processes and procedures remain untouched.

The main benefit that is achievable is delivered by the standardized data repository allowing the data to be moved easily between different life cycle phases and the related tools.

Following this approach doesn't have any impact on the processes and procedures.

AAS: Asset Administration Shell

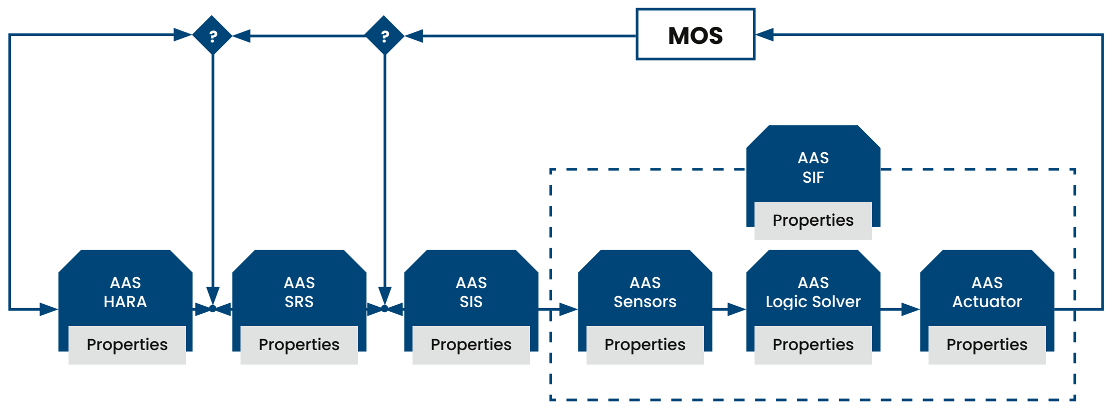

Figure 4: Asset Administration Shells in the context of the safety life cycle

5 UTILIZATION OF THE ASSET MANAGEMENT SHELL

5.1 Introducing SIF Performance Monitoring

Figure 5 shows the first evolutionary step of digitalization, reflecting on the operational challenge to have sufficient performance monitoring of the individual SIF. SIF-Performance dashboards several safety relevant aspects of the SIF in operation can be monitored.

Based on the current technical and safety considerations, this monitoring function is not meant to be interpreted as leading to an automated adaptation of the safety functions, but simply to provide information.

In case data of the Process Information Management Solution (PIMS) and data from the Enter-

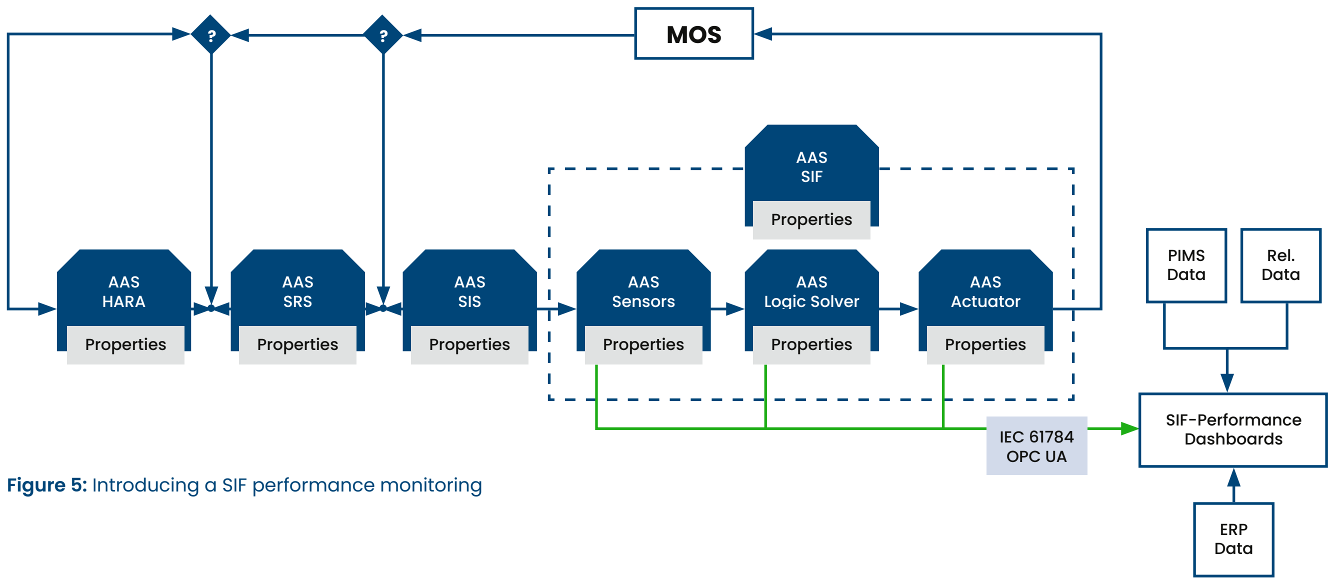

Figure 5: Introducing a SIF performance monitoring

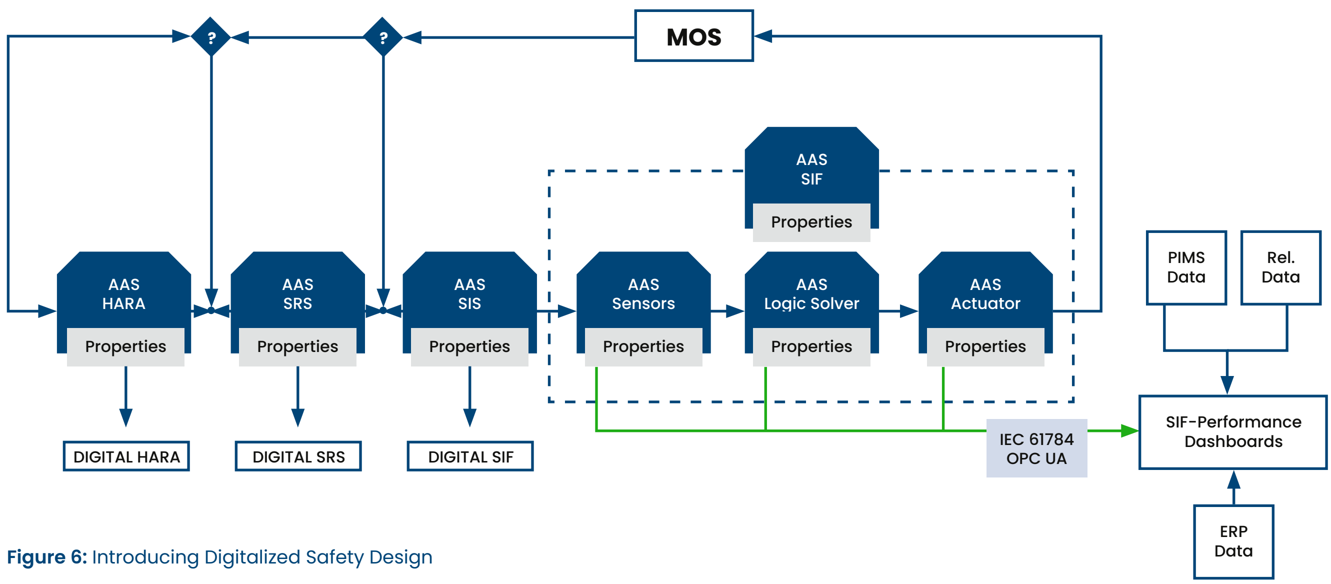

Figure 6: Introducing Digitalized Safety Design

prise Resource Planning (ERP) solution are added a complete SIF performance monitoring covering all recommendations and requirements arising from IEC 61508 and 61511 can be covered.

5.2 Digitalized Safety Design

Figure 6 shows the possibility of interconnecting digital tools supporting the safety design phases of the functional safety life cycle.

5.2.1. Digitalized Hazard and Risk Analysis (HARA)

Hazard and risk assessment (HARA) is an important phase in the functional safety life cycle, following which a safety requirements specification (SRS) is generated and system design and engineering takes place. However, for the past few decades, HARA has been independently conducted by safety analysts manually (e.g., brainstorming). Design and engineering engineers identify safety requirements based on their understanding of HARA reports, so misunderstandings are inevitable and frequent.

When we are using digitalized technical, this will bring the following conveniences to the execution of HARA

1. AI-based methods can be used to realize the automatic identification, import, and classification of HARA input materials, e.g., PID diagrams and related process flow information can be automatically converted into node division, parameters, and deviations for HAZOP.

2. Large language models (LLMs) can be used to inspect analytical models and automatically identify potential logical contradictions, inconsistencies, or similar issues in a large volume of analytical records.

3. Since the generated HARA records and reports are standardized digital information, they can be automatically converted into safety requirement specifications and safety engineering designs, and cross-verification can be performed (on them).

4. Digitalized HARA can also be used during the process online to achieve the dynamic risk assessment.

5.2.2 Digitalized Safety Requirement Specification

Today, safety requirements specifications are often documented as free-form text.

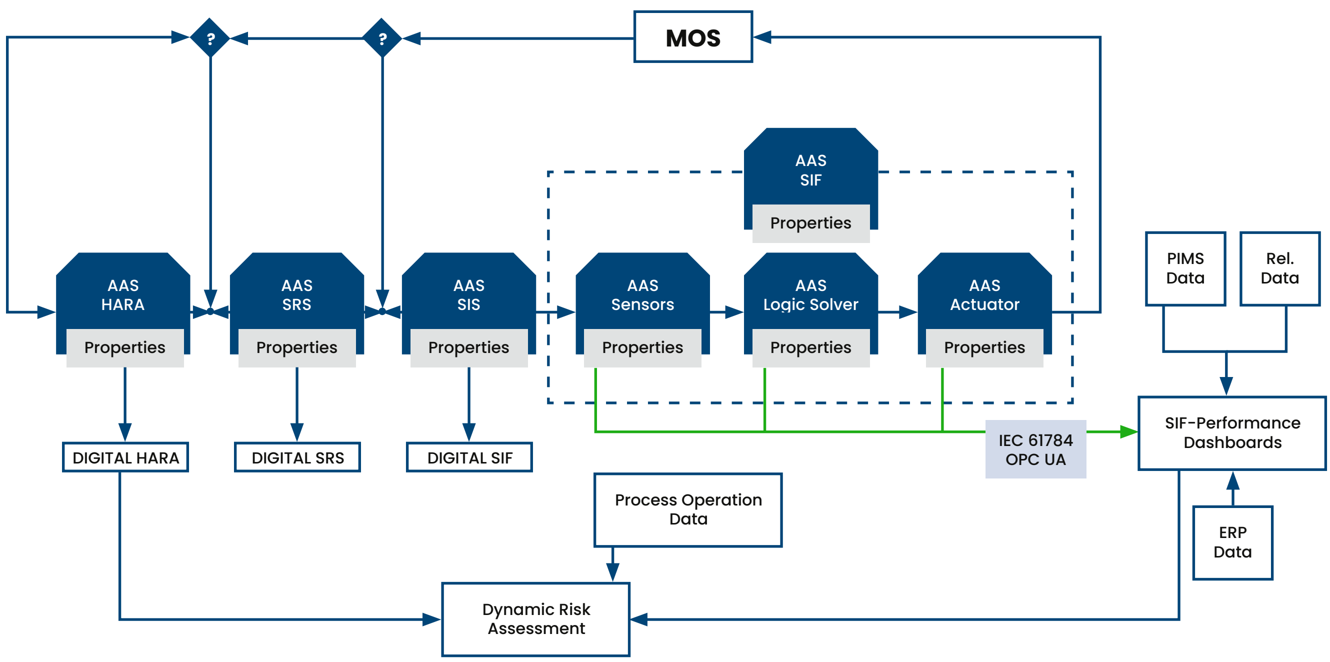

Figure 7: Digitalized Hazard and Risk Analysis

This way of handling is, even so this may sound difficult to believe, one of the major causes of accidents, because free text format documents hardly can be reviewed for completeness and correctness and the implementation of management of change processes are hard to achieve. • This prompted the authors of IEC 61508 Ed. 3 to require a formal description rather than a free-text description. In practice, there is a number of tools available at the market supporting such activity, but the data repository of such tools currently is not defined.

Here the introduction of AAS is a capable way of standardizing this.

5.2.3 Digitalized SIF Implementation

'These days, SIF implementation is often done by several specialists who take the SRS and start programming applications into a safety-related PLC, often without a functional specification.

- to create detail design specification for devices
- to engineer everything related to electrical and mechanical installations of safety related devices and components

'It clearly needs to be understood that in this way, it's difficult to create a standard-compliant safety implementation, especially when dealing with application software. Indeed, complying with the safety standards applicable requires at a minimum to make sure that:

- An SIF application program is clearly structured
- The structure allows to trace back which safety function is covered by which part of the logic
- A clear, structured test procedure reflecting the safety functions to be implemented

5.2.4. Digitalized Application Program Development

Looking at the engineering process, beginning with the completion of the safety requirement specification, the traditional process consists of multiple individual steps, for which different tools are used. While on the design side of the procedure, the use of semi-intelligent tools is the state of the art, most of the testing and related documentation are created manually.. Furthermore, the traditional implementation concept is product oriented, that means that the products to be used are defined and the related functions step by step are implemented and tested. To a certain extent type tests are undertaken especially for testing the interaction between different sub-systems. The handover from one phase to another is done after completion of all activities of the said phase.

This implementation strategy has 2 major disadvantages:

- Limited flexibility when changes occur in the project workflow (e.g., in case of delays in neighboring activities)
- The relative high probability that need for changes are identified only very late being pretty costly due to late implementation of changes

The digitalized workflow is based on the utilization of predefined instrument and functional typicals. The functions required by the safety requirement specification are reflected at the existing typicals and implemented making re-use of typicals as far as reasonably possible.

As part of the safety requirement specification, a test specification is created. This test specification describes on a High level what are the functional pass/fail conditions of each Safety instrumented function. This allows to automatically test the application software – even without the target hardware. In case IEC 61131 compliant controllers are used, the interface of Hard and Software is the name assigned to each signal processed by such controller. The correctness of the I/O wiring can be verified without requiring the complete safety

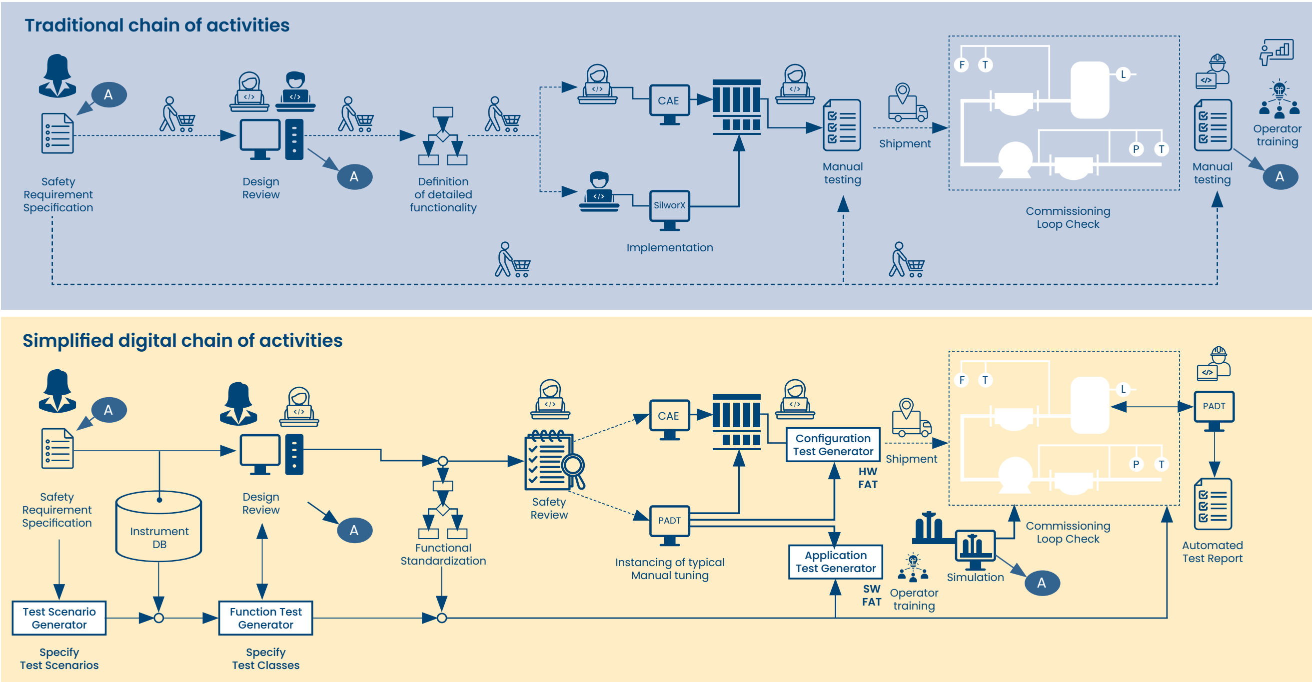

Figure 8: Digitalized Engineering

controller (including application software) to be ready.

This allows to split up Hard- and Software implementation and testing, so that after the completion of the hardware tests the target hardware can be shipped at site and commissioning can be started.

For commissioning support, the correctness of the wiring can be tested step by step without the complete controller functionalities. In parallel, the application software is tested against the pass/fail conditions specified as part of the SRS , e.g., run the application in a simulation environment, enabling more intense testing covering also errors states of field devices and the impact of other mal functions. Once the test is completed, the application is loaded into a simulation environment where operator training and software optimization takes place. Here, during the operator training typically changes required will be identified. After the completion of the training and the implementation of all modifications required, the software is shipped at site and after implementing it into the target hardware a final test of Hard and Software can be done against the SRS.

All in all digitalization of safety engineering drives compliance (completeness of test procedures) driving efficiency due to more flexible implementation.

5.3 Digitalized Device Failure Data Handling

Reliability is the foundation of functional safety in the process industry, but there are still challenges when it comes to reliability data, which are reflected in the reliability data collection, including the untimely data collection and the loss of key parts of the data, which leads to the low availability of the reliability data.

However, if the data collection is carried out by digital means, the collection and processing of reliability data can be made convenient and fast, and the specific reliability data types can refer to the standard IEC TS 63164-1 to calculate and analyze the data according to the standard.

Due to the digitization of collected data, the failure generated in the production process may be misjudged, and the nature of the failure further classified whether random or systematic (aging, etc.) may also be mixed. Therefore, it is essential to ensure the accuracy of data analysis results during data collection and analysis. Reliability

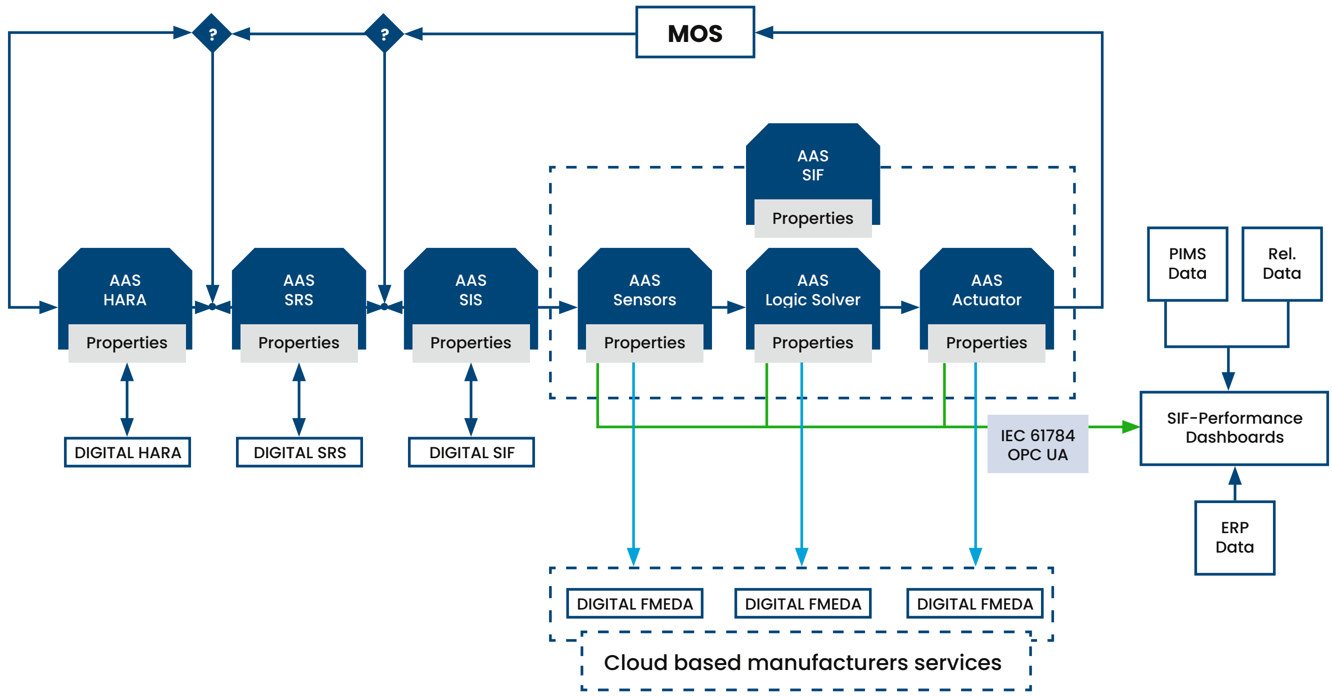

Figure 9: Digitalized FMEDA

reviews should be implemented, incorporating manual verification, algorithm-based verification, and knowledge-based verification for classifying collected failure data.

Finally, according to the life cycle of the process, digital data collection provides the possibility to establish a reliability data management platform for the whole life cycle under the current functional safety standards, which will be conducive to recording on-site use data and normalizing data recording and reliability review. The data management platform also provides strong support for the SIF-Performance dashboards and dynamic risk assessment.

5.3.1 New Safety Data Handling Philosophy

Today we are using device manuals to capture device reliability data. However, this is just a snapshot reflecting only random hardware failures. 'The use of an application-specific FMEDA will also allow reflecting additional effects such as environmental conditions and abrasion.

In case we anticipate the creation of an adequate Asset Administration Shell, including the FMEDA relevant data, supporting a standardized interface for such data it would be possible to interlink the FMEDA functionality of different devices making up a safety function and by doing so creating a machine-readable digital safety analysis.

This strategy may pose an IP-related challenge, because if FMEDA models are published, the complete internal setup of a product may get public domain know. This, however, can be prevented by providing a trustworthy cloud environment in which such functionality may be implemented.

The process indicated in Figure 8 is, compared to what is done today, a major change. Indeed, today users are getting data sheets either digitally (e.g., NAMUR Container) or paper based. 'The disadvantage of this approach is that every data sheet is merely a spotlight on a device's behavior, reflecting a standardized environment. The question if these assumed surroundings are of relevance for a dedicated application is verified by practical tests (e.g., 10 devices to be operated for 1 year like defined in IEC 61511). 'This applies to' simple 'devices with limited complexity (parameters to be changed), but not to complex devices. An example for a complex device might be a flow meter (Coriolis type) where typically more than 1.000 parameters can be modified.

In today's industrial practice complex electronical circuitries are getting tested by AI based Failure Mode Effect Diagnostics Analysis (FMEDA) tools. Such tools having the ability to take into consideration all reliability aspects of all single components of a circuitry, the PCB's as well as cross influences between components and environmental circumstances.

For such solutions, it is also feasible to adjust them so that the behavior of devices under certain conditions becomes predictable, or at least predictable in a way that upcoming malfunctions can be detected early (e.g., abrasion at a valve or blockage of a transmitter hookup are typically not sudden events but develop over time and are detectable if using the right analytical tools).

When talking about digitalization, it will be feasible, that device manufacturers will make these FMEDA tools available to users, so that static data sheets can be replaced by dynamical model based solutions where individual surroundings can be taken into consideration.

In fact, such an FMEDA model will provide highly detailed insights into the internal design of devices—information that may constitute intellectual property the manufacturer wishes to protect. These models could be made available as trusted cloud applications, allowing users to input application-related data and obtain relevant safety parameters. This then will open up 3 possibilities:

1. Getting a more decent idea on how a device will behave under certain conditions

2. Create application specific products tailored for a dedicated application

Where proven reliability data are available (e.g., NAMUR Smart) the existing models might be tuned reflecting reality as good as possible. Of course, this will give rise to new information security issues, which will be addressed in the subsequent research of the working group.

5.4 Digitalized Functional Safety Life Cycle Management

Figure 10 introduces a fully digitalized safety life cycle solution, where all relevant data from all safety related engineering processes are collected and processed.

Such solution also need to be interconnected with the testing and inspections as well as repair data.

Note:
It need to be clearly stated, that all automated functions described in this document need to be seen as support for human based activities. This in particular is valid for all equipment testing activities, as the automated self-test on device level only in seldom cases (e.g., Coriolis flow meters) is achieving a higher diagnostic coverage as 20 to 30%.

5.4.1 Digitalized Operate and Maintain

The operational phase is a critical stage in the functional safety lifecycle, requiring safety instruments to perform protective functions as expected to ensure the operation of industrial processes. 'However, most safety instrumented functions are executed on demand, and self-diagnostics typically cannot detect all dangerous failures during operation. To ensure their functionality, it is necessary to conduct proof testing and verification to reveal undetected failures, which is one of the most important tasks during the operational phase of the functional safety lifecycle.

'Traditional proof testing involves manipulating electrical circuits and separating electrical tests from manual inspections. Automated proof test functions support electrical testing without manipulating the circuits and can be combined with mechanical inspections and plausibility checks. This reduces risks and save costs.

After SIS is equipped with digital functions, its failure information can be monitored and maintenance activities can be executed online during operation. Functional safety technicians can monitor or conduct on-site testing and verification, and data collection and upload will also be

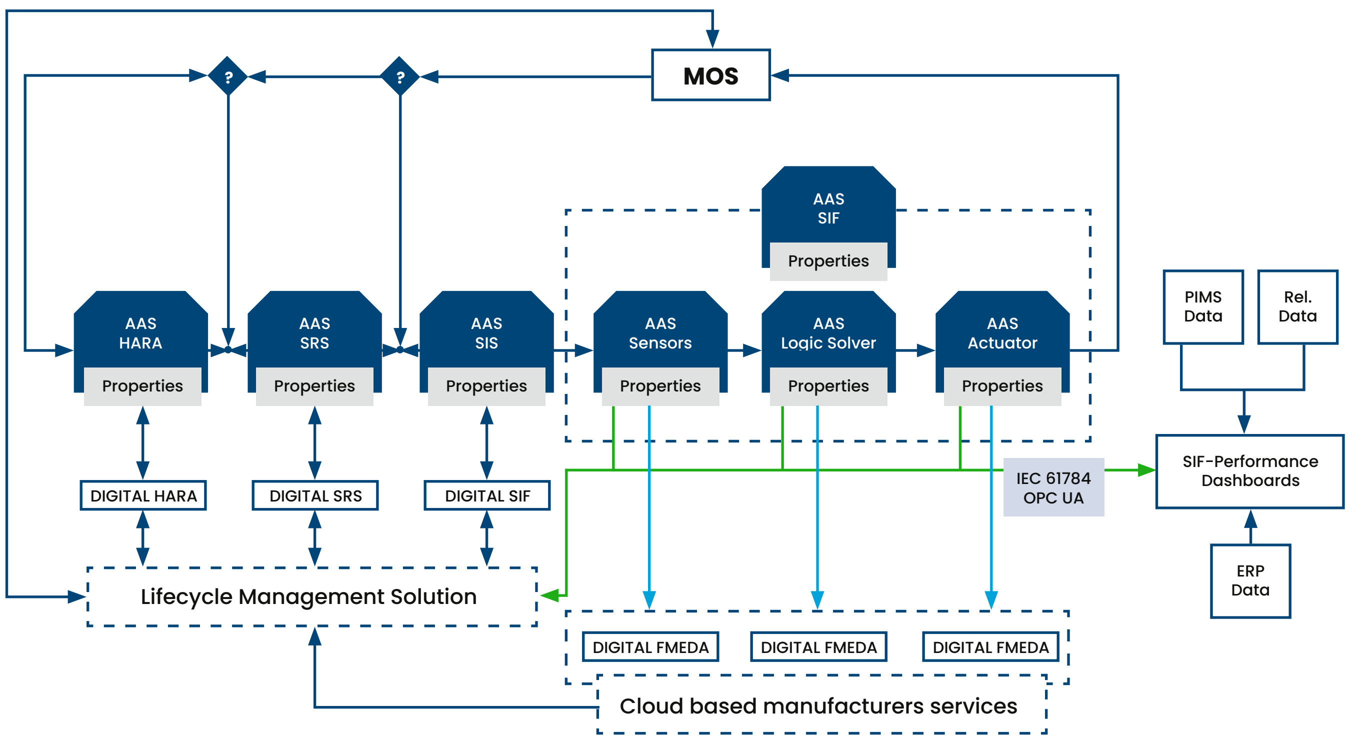

Figure 10: Introduction of a lifecycle Solution

more real-time and reliable. Maintenance engineers can also dynamically adjust the regular maintenance schedule based on on-site data, and predictive maintenance can be adopted for equipment that meets certain monitoring data requirements to save maintenance costs and time.

5.4.2 Distribution of Test Results

During the operation process, the test results have to be made available to the stakeholders of the functional safety management systems.

These are in particular:

1. **Maintenance managers**
   responsible for implementing the related maintenance programs.

2. **Operations managers**
   responsible for safe, effective operations of the individual plants.

3. **Business leaders**
   responsible for effective operations of business units.

4. **Safety experts**
   working on the basics for design and implementation of safety instrumented systems.

The individual stakeholders need to get target group oriented representations of the test results.

This means that for an operations manager, it is important to understand whether the achieved risk reduction aligns with the design values (derived from PHA) and what the cost of nuisance trips is.

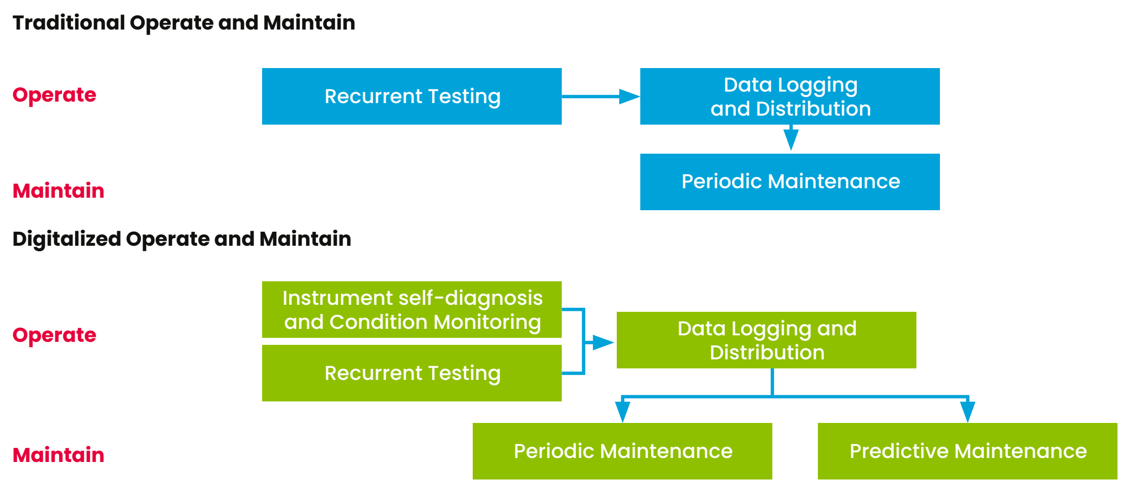

Figure 11: Digitalized Operate and Maintain

For safety experts working on basic design concepts for functional safety, it is crucial to verify whether a dedicated device, when applied in a specific configuration, meets the expected reliability standards. If not, corrective actions can be initiated.

A digitalized safety lifecycle management solution needs to be able to provide this type of information timely and efficiently. ‘By building a specific application, each role can obtain corresponding on-site information based on their respective focus areas, thus avoiding information overload and misjudgment.

5.5 Usage of Digital Twins

Figure 12 shows the introduction of functional digital twins. This reflects the need for intensive testing of SIF during all phases of implementation. A digital twin concept includes all relevant data (such as device failure modes) and allows for intensive testing without impacting other implementation tasks. ‘Such a digital twin concept is not limited to technical functionalities but can also be applied in safety design, where process simulations can be used to better understand the process to be protected and streamline related engineering processes. As shown in Figure 8, the digital engineering and testing approach not only enhances the quality of achievable testing but also supports the parallel execution of various engineering and optimization tasks.

Today, early solutions are available that allow direct transfer of process simulation results into the application program of a safety PLC. ‘By doing so, it is becoming feasible to define a completely new safety lifecycle where dedicated steps—not only the layering of protection levels but also the entire safety requirements specification—may be eliminated. This, however, is still in the future, because the larger the individual steps along the design path become, the harder it will be to verify the correctness of such steps.

5.6 Safety Related Digital Twin

Testing capabilities like described in 5.5 are important as driving quality as well as efficiency.

Especially when considering change management, it is crucial to question the reliability of test results based on digital twins.

If pre-tested solutions are intended to be implemented without requiring re-testing on the safety-related runtime system, the digital twins must also be safety-related.

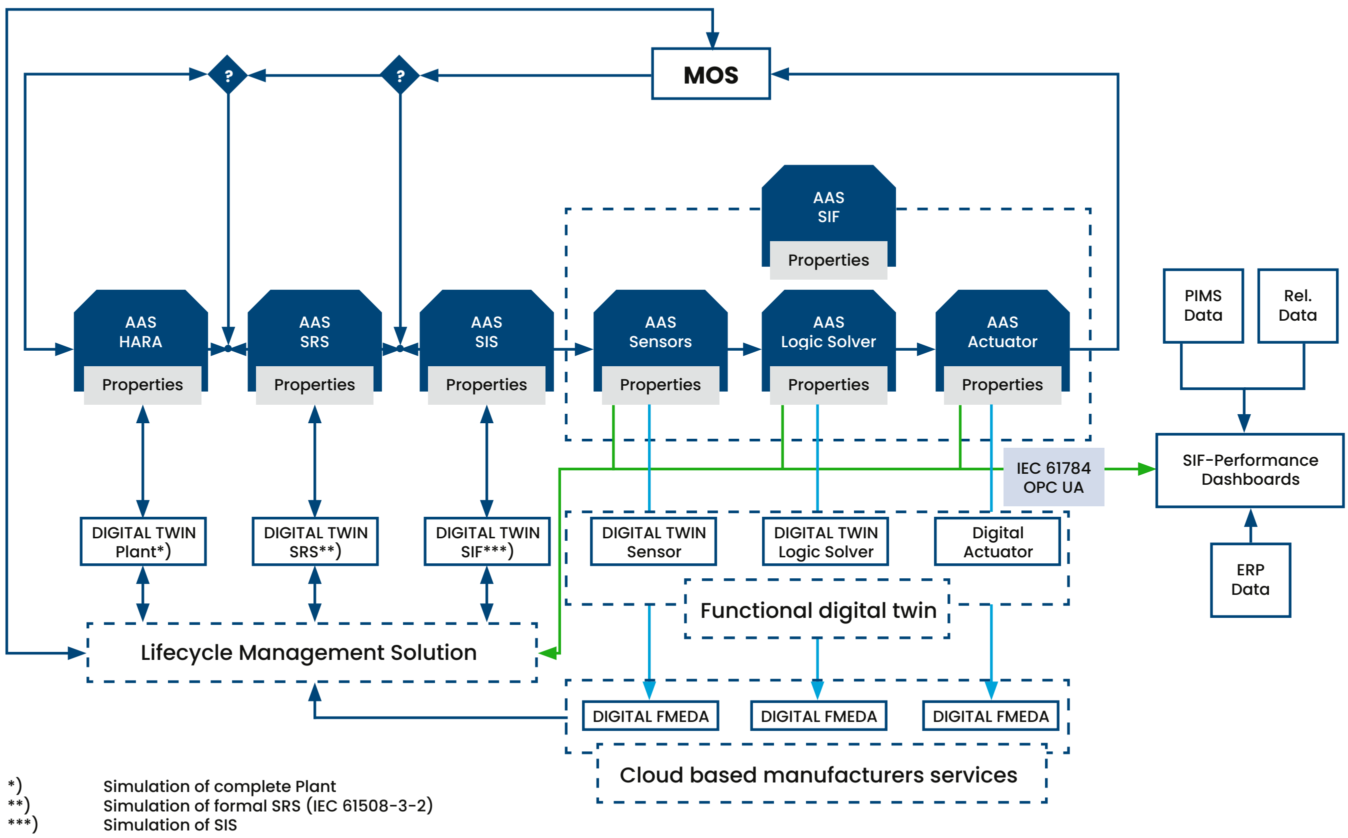

Figure 12: Introducing a functional digital Twin

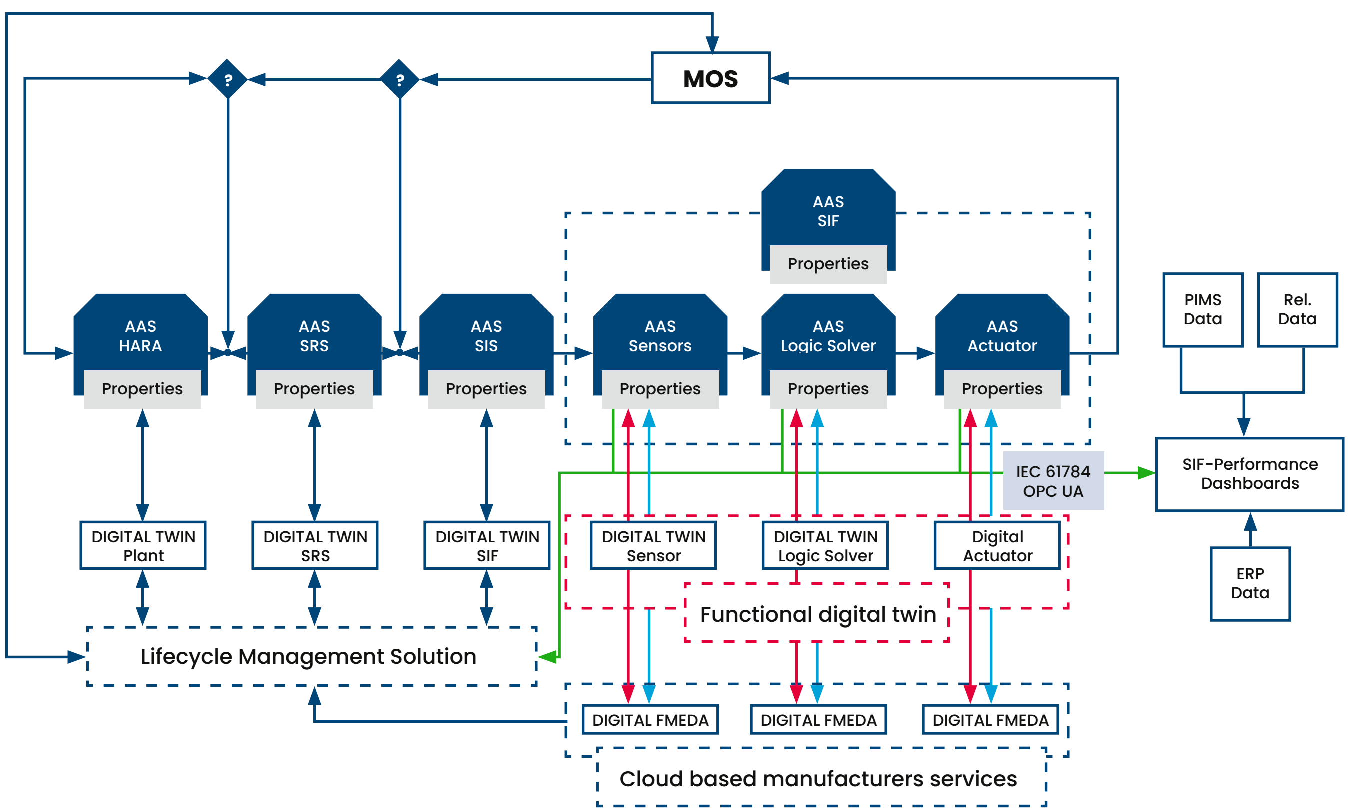

Figure 13: Introduction of safe digital twin

The level of such "safety testbed" should be subject to further evaluations, while these days the first safety related cloud applications are piloted.

Note:
The handling of safety relevant data at the AAS doesn't automatically imply that the AAS need to be the same safety integrity level with related safety functions (e.g., for SIL3 SIF need SIL1 OR SIL2 AAS), as it just is handling but not processing data.

5.7 Concluding the Usage of Asset Administration Shells (AAS)

Figure 14 illustrates the correlation between different Asset Administration Shells, related to activities of the management of functional safety, the digitalized representation of the activities as well as the physical assets such as Input devices (Sensors), logic solvers and actuators (final Elements) as well as the activities required by standards such as IEC 61511.

The aim of the digital elements in this concept is to more effectively interconnect the physical assets and the management processes, required to maintain a specific safety integrity level.

Developing an information model capable of creating a digital twin for functional safety is the first step in creating industry-specific use cases that generate added value through digitalization while maintaining the highest level of interoperability.

'The existing AAS concept is tailored in such a way that it applies to various assets in a very flexible manner, thus covering tangible as well as intangible assets that are independent of brownfield or greenfield scenarios.

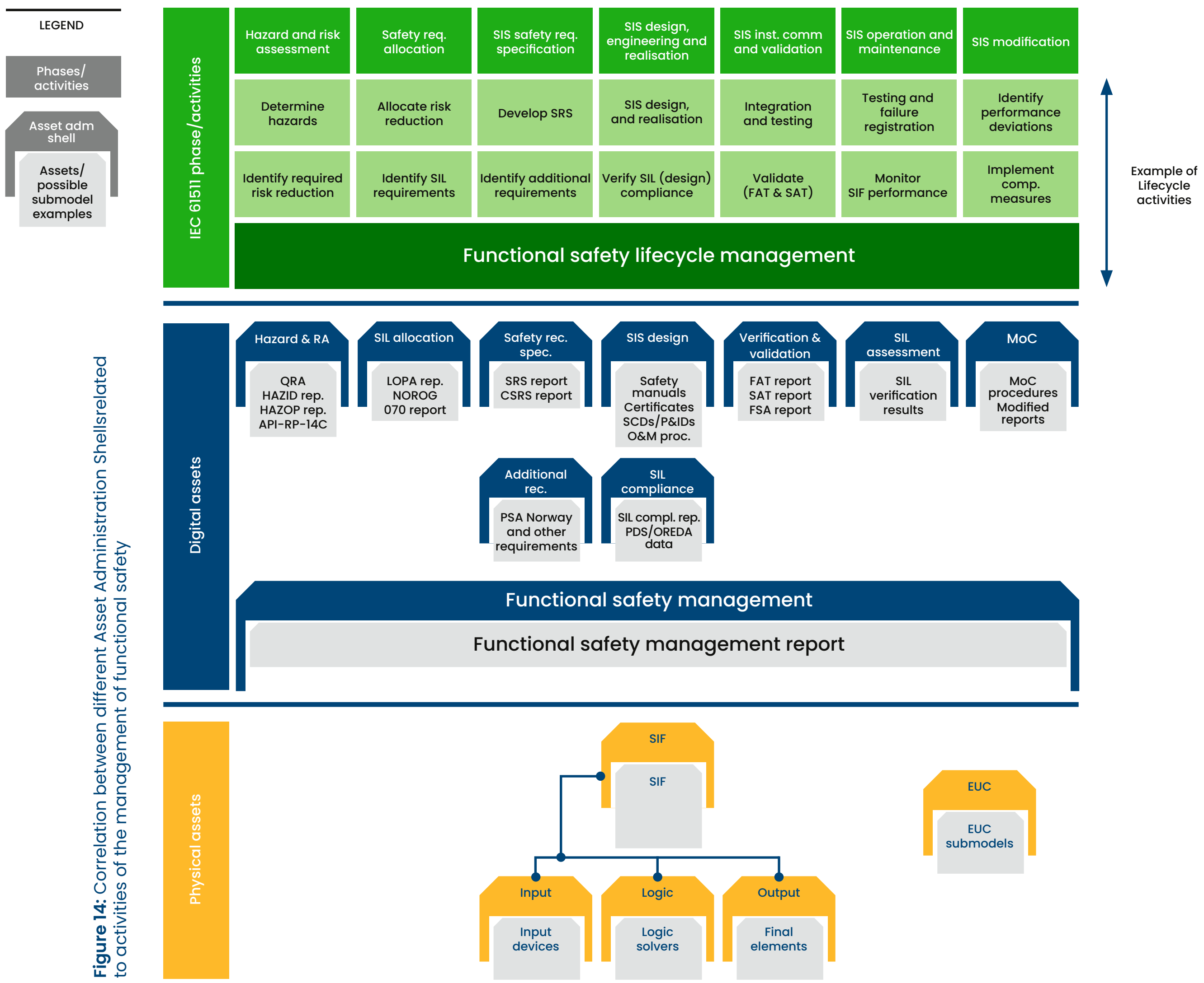

Figure 14: Correlation between different Asset Administration Shellsrelated to activities of the management of functional safety

6 SAFETY AND SECURITY

6.1 General Consideration

“There is no functional safety without security” is a statement, which today is even more important than ever. The extensive use of digitized tools and processes is opening up a completely new set of attack vectors.Following the traditional approach, safety systems themselves and their interconnected devices need to be protected; this was at least the prevailing view for many years. In a digitalized world, the scope of what needs to be protected has expanded dramatically, as attacks are feasible at all phases of the security lifecycle, and even lateral attacks require attention due to system interconnections.

Note:
When carrying out a lateral attack, an attacker is seeking for the weakest element at a network and then is developing through the entire network until getting control on the key functions.

‘The development of standards such as IEC 62443 and IEC TR 63069 demonstrates how this can be addressed.

Figure 15 shows an example of a zoning concept developed in line with the stipulations laid down in IEC 62443 and IEC TR 63069. ‘The idea behind this concept is to establish different security zones that maintain different levels of protection at zone transitions. This, combined with adequate device-level protection (defense in depth), enables the creation of a security environment where safety functions operate to achieve the desired overall risk reduction.

Note:
It needs to be emphasized that such security concepts must cover all phases of the lifecycle, including not only normal operations but also revamping and modifications.

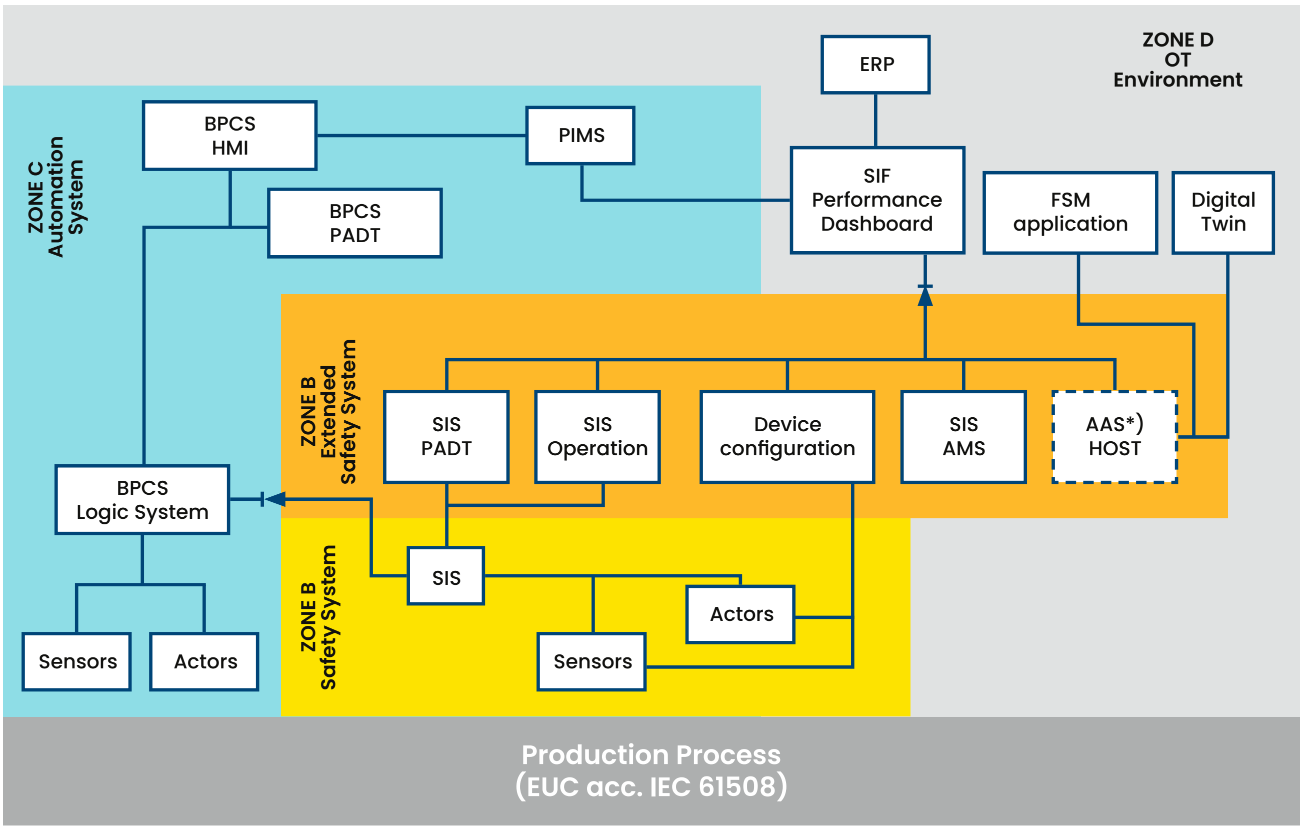

Figure 15: Example of a security Zoning concept

'One might say that based on this, all security challenges seem to be solved.

Nevertheless, in reality, we face critical challenges regarding security. This is mainly because the development pace of international standards like IEC 62443—developed through consensus—lags behind China's and Europe's security legislation (e.g., MLPS in China, and NIS2 and CRA in Europe). Furthermore, there remains insufficient understanding of the differences between industrial security and traditional IT information security (for example in the industrial field, availability is more important than confidentiality), which results in poor adaptability of some regulations or laws to industrial control security. Here, it is important that on the one hand, the standardization process is accelerated, and on the other hand, local legislation is not formulated in a way that creates new trade barriers.

6.2 Baseline for Communications

'The decision regarding which communication protocol to use and where depends on the host of the AAS, which can be the device itself or an external unit.

From today's perspective, OPC UA appears to be the preferred communication protocol for physical interconnection of different systems.

It offers sufficient performance and enables the implementation of adequate security measures to ensure that the requirements outlined in Chapter 6 are met.

Even safety-related communication, as required to interconnect safety-relevant functional units, will soon be available.

In fact, a key gap to address is communication with/between low-performance devices (e.g., field devices) or for applications requiring fast response times (e.g., LDPE plants or turbomachinery applications). For this type of application, OPC UA has limited value. Here, communication protocols according to IEC 61158 and IEC 61784 are more suitable. Examples include: PROFIsafe (via PROFIBUS/PROFINET), SafetyBUS p (CAN-based), Safety over EtherCAT, openSafety (POWERLINK), FSoE (Fail-Safe over EtherCAT), and EPA safety.
For example:

- PROFIsafe (via PROFIBUS/PROFINET)
- SafetyBUS p (CAN-based)
- Safety over EtherCAT
- openSafety (POWERLINK)
- FSoE (Fail Safe over EtherCAT)
- EPA safety

For these protocols, security aspects—at least in part—are not yet sufficiently addressed and need to be handled in an application-specific manner. From a system-wide perspective, implementing additional measures such as isolation and monitoring to ensure information security in this region is one optional approach.

From the communication perspective, the coordination between safety and security also needs to be a key consideration, for example. To maintain completeness: for time-critical or highly safety-critical communication internal strong security measures (e.g., encryption) may not be applicable, lightweight measures should be considered.

7 CONCLUSION

Implementing digitalized workflows for functional safety can deliver significant benefits in improving the reliability of safety solutions. This is achieved by making the supporting processes for functional safety more resilient to human errors during design, implementation, and maintenance, while also reducing costs. A major challenge in leveraging these benefits is the fragmented landscape of tools, which are typically not designed to enable effective data exchange with related activities. More importantly there currently is no overall data representation covering the different areas making up a functional safety lifecycle. There are certain islands of data standardization like the Administration Shell for safety devices. 'IDTA's current efforts to develop a comprehensive set of standardized data structures are moving in the right direction. However, the current focus of these activities needs to be critically reviewed, as the overall need for standardized data extends far beyond what is currently being addressed.

As an example, consider the concept of publicly accessible FMEDA models, which would enable application-specific technical analyses at a level far beyond what is feasible today. This sounds promising, but it will require device manufacturers to agree to standardize processes and tools that are currently proprietary. No manufacturer currently publishes this information or even considers standardizing these elements. 'The introduction of IEC 61360 (IEC Common Data Dictionary, IEC CDD) demonstrates one approach to standardizing data repositories. However, implementing such a concept across all areas relevant to functional safety will take considerable time.

'From today's perspective, the most appropriate approach is to follow a structured methodology where the various elements described in Chapters 4.1 to 4.5.2 can be utilized as needed, but independently of one another.

As outlined in Chapter 4.6 the usage of digital twins created new possibilities to streamline the management of functional safety and the related lifecycle activities, but such changes need to be seen critical due to the required verification activities , which typically are done as a kind of Black Box testing in case models like digital twins are used. From today's perspective, we can identify two potential approaches:

1. Developing new, reliable test methodologies for more complex elements.

2. Developing digital twins with the same reliability level as the target systems.

Both will require fundamental changes to safety standards such as IEC 61508 or the development of new standards, since the entire safety concept currently relies on the principle of conducting sufficient manual reviews.

The future will determine which solution will be most widely accepted.

Regarding functional safety and industrial security, as outlined in Chapter 6, both safety and security must go hand in hand. We are currently witnessing a strong politically driven movement in China as well as in Europe. We should also not overlook the specific characteristics of industrial information security compared with traditional IT security—particularly when considering coordination with safety—since safety and industrial security will inevitably become more closely interconnected. The necessity to enhance security, especially in critical applications, is undisputed; however, it must be ensured that global standardization is not undermined by political initiatives such as NIS2 and CRA in Europe or MLPS in China.

Another important area are digital simulations. In this area we see a very steamy development where AI based simulators are enabling complete new dimensions of predicting the behavior of systems of functional safety. Even so today none of them are complying with safety recommendations, the usage is beneficial because the more we know about the equipment we use, the better we can predict what to worry about and what not, so design and maintenance activities can be steered better to the point.

In general, despite facing numerous challenges, we believe the process of digitalization in functional safety is unstoppable. Processes such as functional safety AAS, SIF performance implementation monitoring, and dynamic risk assessment will transform the traditional safety assurance system and are bound to bring substantial benefits to the entire industrial sector.