



A Common Development Process for IEC 61508 and IEC 62443

White Paper

exida

80 N. Main St.

Sellersville, PA

www.exida.com

March 2019

exida White Paper Library

<http://www.exida.com/Resources/Whitepapers>

Copyright exida.com L.L.C. 2018-2020

Abstract

A good product development process should ensure a good understanding of what is to be developed, how it is to be developed and that it was developed correctly. IEC 61508 and IEC 62443-4-1 both have development process requirements. These requirements overlap and separate efforts when assessing compliance to both standards would mean duplicating efforts to assess the common requirements. By identifying what process requirements are in common between IEC 61508 and IEC 62443-4-1 and showing that the IEC 61508 process requirements meet the IEC 62443-4-1 process requirements, the cost of developing procedures, and assessing procedures for compliance, can be reduced.

Conclusion

The IEC 61508 and IEC 62443-4-1 standards have process requirements that can be met with a single set of procedures. This presents an opportunity to achieve significant cost savings by avoiding unnecessary redundant assessment efforts. While the simultaneous assessment of both standards is more effort than for a single standard, the additional effort to assess both standard simultaneously is significantly smaller than assessing both sets of requirements separately.

Introduction

With the appearance of malware and nation state attacks on Industrial Control Systems (ICS), such as the Stuxnet (2010), Industroyer (2016) and TRITON (2017) attacks, the IEC 62433 standards are now being aggressively used to strengthen cybersecurity. While the potential attack targets in an ICS system are many-fold, one plant asset that could be targeted is the system. Many safety equipment OEMs are seeking to certify their products to both IEC 61508 Functional Safety requirements as well as IEC 62443 Cybersecurity requirements.

Both standards include requirements to document the development process and to verify that the process has been followed correctly and completely. One way to minimize the time and effort to document and use a development process that is compliant with both standards, is to identify overlapping requirements in the two standards and provide common solutions.

Development Process Requirements

Development process requirements specify a process to ensure product developers have a good understanding of what is to be built, how it is to be built and that it was built correctly. “Process”, in this context, is the sequence of steps necessary to carry out a task that transforms specific inputs into one or more specific outputs. For example, a procedure to create a product’s architecture design might be defined as first reading the product requirements, then documenting the design, technology and process choices needed to transform the requirements into design.

Common Requirements

The requirements of the IEC 61508 and IEC 62443-4-1 standards overlap a great deal, so separate documentation and assessment efforts would be required if not undertaken in a coordinated manner. By identifying what process requirements are in common between IEC 61508 and IEC 62443-4-1, and showing that the IEC 61508 process requirements cover them, the cost of creating, maintaining and assessing process for compliance with both standards can be reduced. IEC 62443-4-1 process requirements are identified and shown to be covered by an IEC 61508-compliant process. IEC 62443-4-1

requirements will be called out by the requirement identifiers, given by the standard (e.g., SM-1, DM-xx, SR-xx, SD-xx, SI-xx, SVV-xx, SG-xx, etc.).

The authors of IEC 62443-4-1 understood that the use of a properly defined and executed lifecycle is an effective way to avoid the introduction of vulnerabilities into a product's design/implementation. They also understood that there are existing standards which specify lifecycle process requirements that can be effectively used in this context. Instead of "re-inventing" lifecycle requirements, IEC 62443-4-1 allows for the use of "commonly accepted" processes, specified in several other existing standards, so that IEC 62443-4-1 can focus on the other requirements specific to cybersecurity. IEC 61508 is such a standard and specifies an excellent set of process requirements.

Because of this choice, SM-1 requires that "A general product development / maintenance / support process shall be documented and enforced that is consistent and integrated with commonly accepted product development processes." It goes on to require the following general characteristics in a selected/defined process but leaves it up to the specification of that process to spell out the details. SM-1 requires the specification to include the following activities:

- Configuration management
- Requirements specification with requirements traceability (also SR-1, SR-3)
- Documented SW and HW design and implementation practices (also SD-4, SI-2)
- Repeatable verification and validation (also SR-5, SD-3, SI-1, SVV-1)
- Review and approval of development records (also SM-12)
- Lifecycle support

Since IEC 61508 process requirements cover all the process constraints in SM-1, any process compliant with IEC 61508 process requirements will meet the general process constraints in SM-1.

Competency Requirements

SM-2 and SM-4 require identification of project roles and responsibilities, personnel assignments to those roles and documented confirmation that assigned personnel are competent to perform their assignments, and if not, identification of required training. IEC 61508 has these same competency requirements. Both standards' requirements can be met with a common procedure and documentation such as a RACI chart, though the specific skills and knowledge required for safety and security roles will not completely overlap.

SM-9 requires management of COTS components and their 3rd party suppliers in terms of managing product security risks, including:

- Ensuring acceptable rigor in development of the component
- Ensuring adequate degree of component security verification and validation
- Determining how to receive/monitor security-related issues from component supplier
- Determining the degree to which supplier supports component software (e.g., updates)

Supplier Qualification Requirements

IEC 61508 requires that suppliers are assessed/audited to ensure adequate quality in the supplier's development/manufacturing process and in the component's reliability. Therefore, procedures must be created to assess/audit a supplier. The information to be captured must be specified. The qualification

criteria depend on the function, technology and complexity of the supplied component. The same overall supplier assessment/audit procedure can be used for both safety and security. However, the non-overlapping safety-specific and security-specific data will need to be captured separately (e.g., separate forms or separate fields). For example, depending on the product supplied, a supplier may need to show that they actively review known vulnerability databases (security requirements) or that they record the phase of the product lifecycle in which a safety issue was discovered with respect to safe operation (such as receipt, commissioning, operation, etc. – to more accurately determine safety-related failure rates).

Design Requirements

SD-1 requires that certain design principles are included in design guidelines documentation. IEC 61508 requires that design “best practices” are included in guidelines documentation to provide guidance in specific design techniques. Functional safety best practices and security best practices are largely overlapping, because anything that leads to unpredictable operation is important to both safety and security. For instance, a common principle is to specify external interfaces in design documentation, to indicate whether each one is accessible by users or other products and to specify valid protocols and data ranges. External interface design documentation is used to support both hazard analysis for safety, and to support threat analysis for both safety and security, for example, using *exida*’s ARCHx™ tool (see Figure 1).

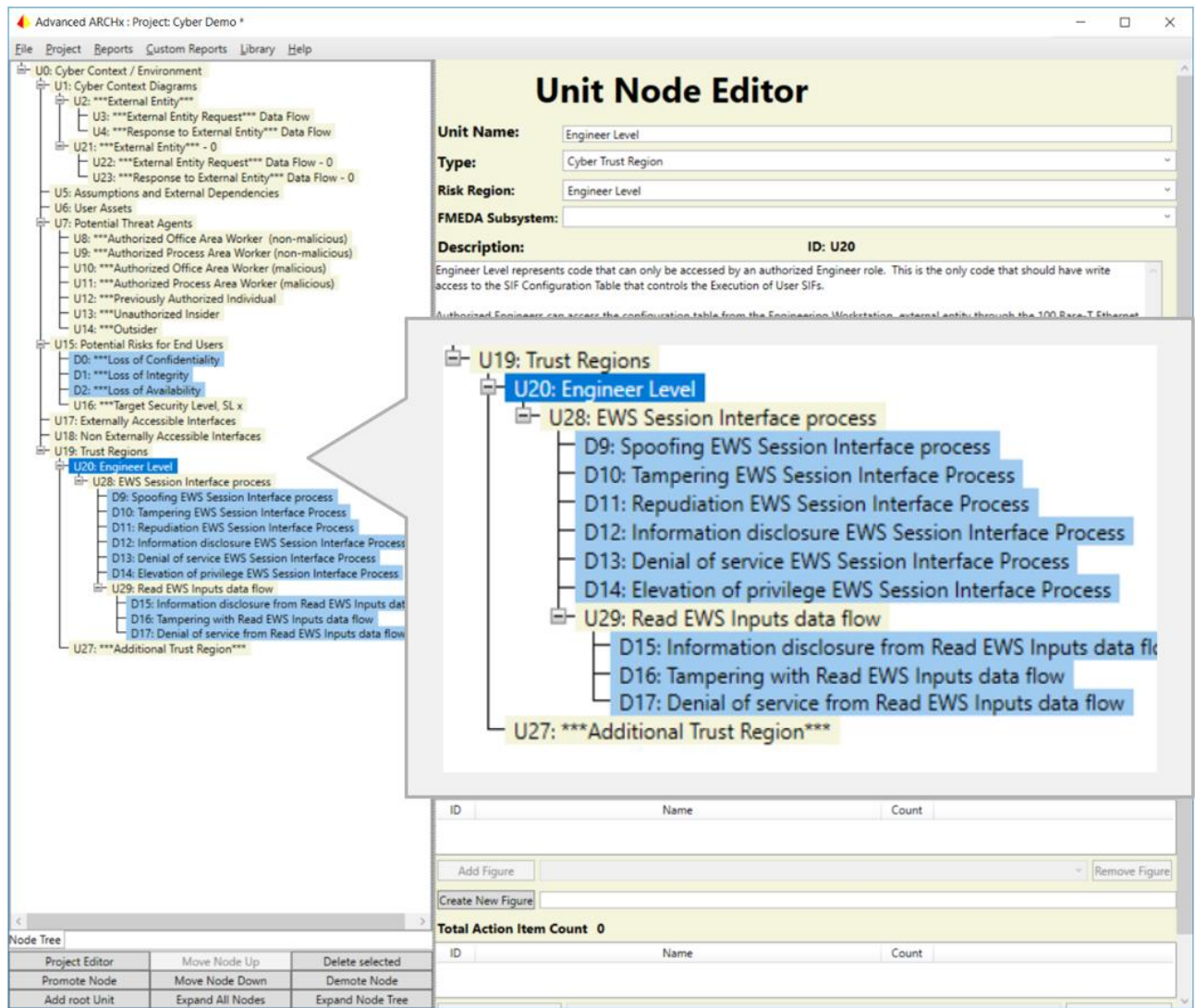


Figure 1 - Threat Analysis, using *exida's* ARCHx Tool

SM-10 in IEC 62443-4-1 requires custom components (as opposed to COTS components), developed by 3rd parties, to be developed to the same rigor as the rest of the product if the custom component can have an impact on security in the context of its use in the product. IEC 61508 also requires partner/contractor companies to comply with development process requirements. Simultaneously assessing safety and security process requirements should provide the same reductions in effort as outlined herein for the assessment of the product manufacturer's process.

Validation/Verification Requirements

IEC 61508, while not prescriptive, does provide a "default" lifecycle model to give a context to some of the requirements in that standard. The model can be viewed as a "V", with construction activities (requirements, design, implementation, etc.) descending the left side of the V and verification activities (testing, inspection, analysis) ascending the right side of the V. As shown in Figure 2, the activities are

partitioned into phases. Each phase has defined phase inputs, phase activities, verification activities, verification outputs and phase outputs.

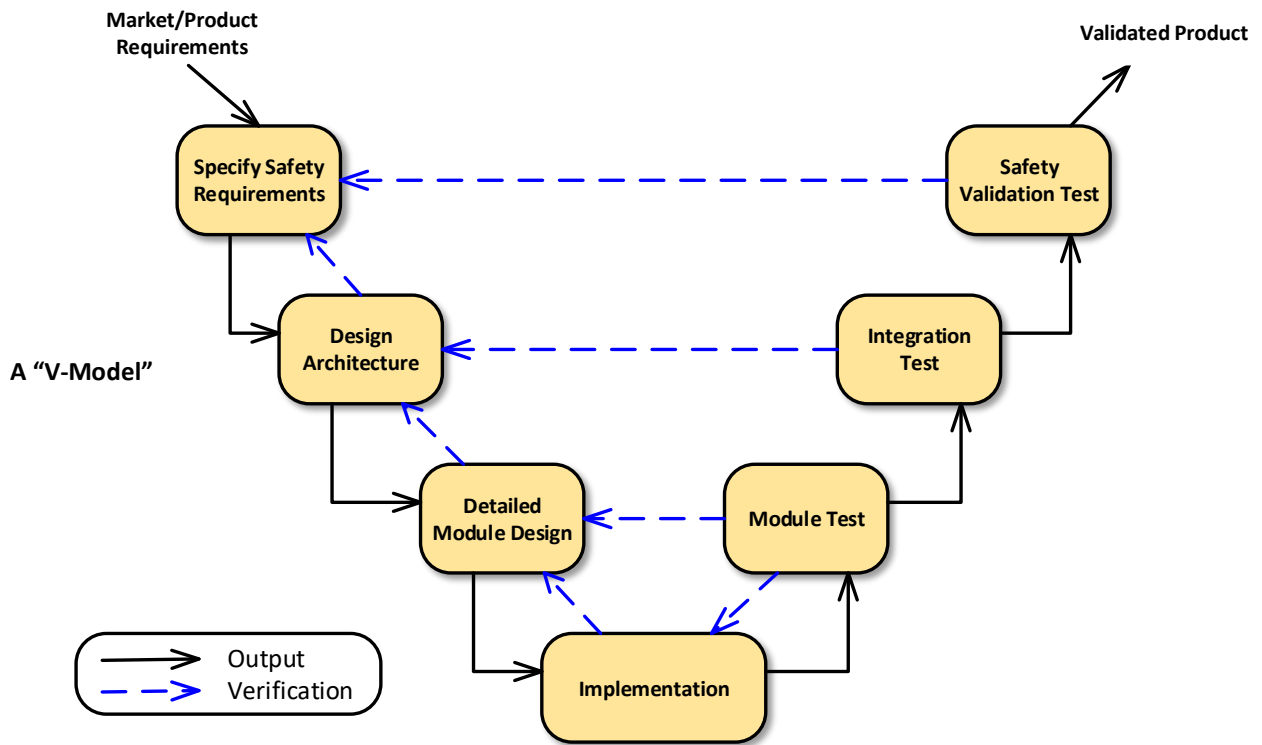


Figure 2 - IEC 61508 "V-model"

Several IEC 62443-4-1 requirements can be grouped as “verification/validation-related requirements” (see Table 1). These requirements are identical to requirements in IEC 61508. For example, SR-5 requires that security requirements must be reviewed. This requirement is covered by the IEC 61508 process requirement for review of requirements.

SR-5	Requirements Review
SD-3	Design Review
SI-1.a, SI-1.b, SI-1.d, SI-1.e	Implementation Review
SI-1.c	Static Code Analysis
SM-1.d	Module Testing & Integration Testing
SVV-1	Validation Testing
SG-7	User Documentation review

Table 1 - IEC 62443-4-1 Verification/Validation-Related Requirements covered by IEC 61508

SM-11 requires a process for verifying all security related issues have been addressed and tracked to closure prior to release or update of a product. IEC 61508 requires any action items discovered during the development process to be captured, described and tracked to resolution. Additionally, IEC 61508’s phase verification requirements are intended to ensure that all phase activities are completed. Tracking action items is usually done through one or more of the following: an issue tracker feature built into an integrated development tool (e.g., exida’s ARCHx™ tool, see Figure 3), formatted meeting minutes,

spreadsheets, issue tracker software products, etc. Issues are captured, dispositioned with opened/closed statuses (at a minimum), document resolutions and are checked for closure at appropriate life-cycle milestones.

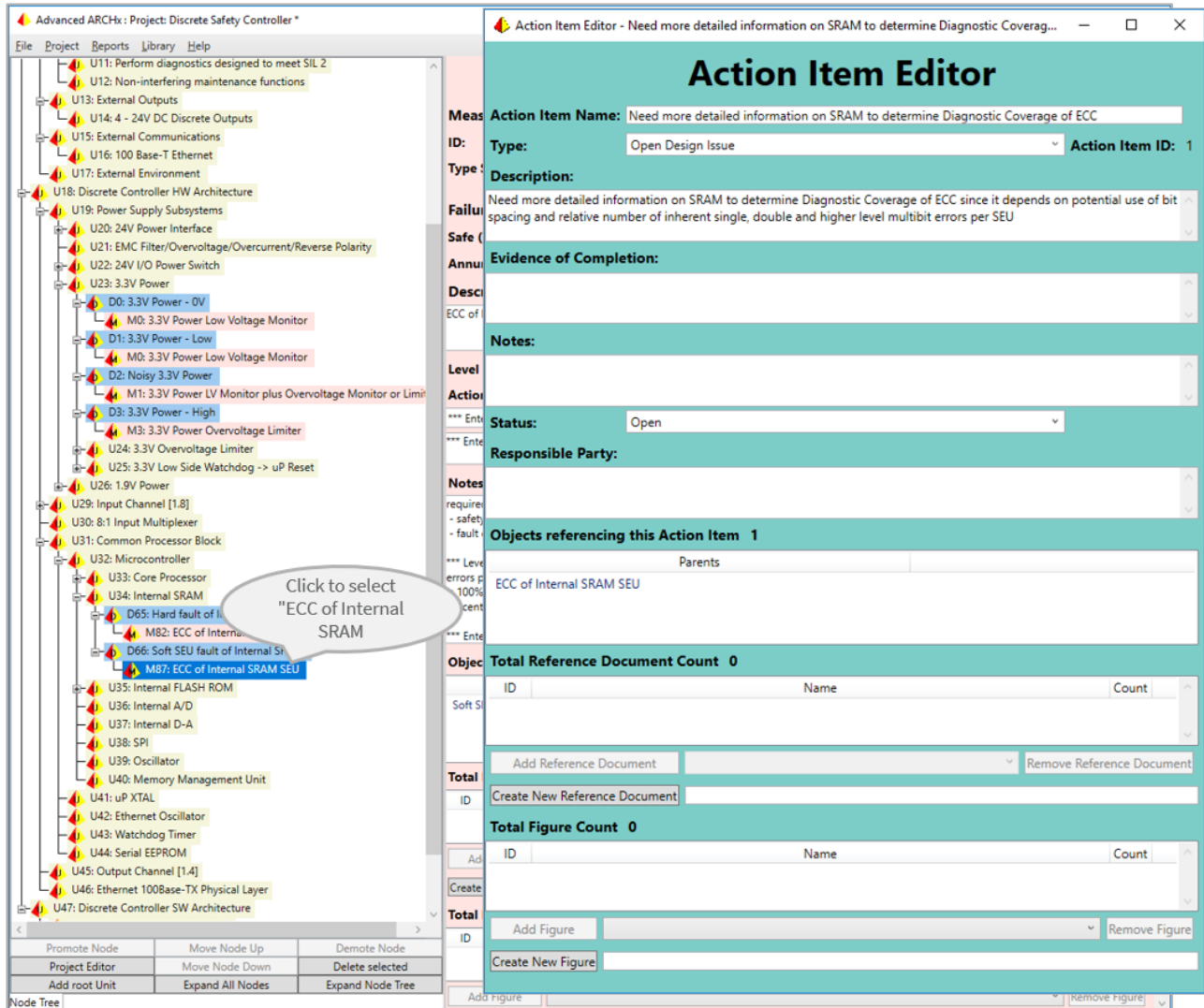


Figure 3 - Action Item feature in *exida's* ARCHx Tool

Requirements for Handling Field Issues

DM-1, DM-2, DM-3 and DM-4 specify requirements for receiving, reviewing, assessing and addressing security-related issues when they are reported by internal or external sources. These are issues reported either by internal (to the product manufacturer) or external personnel. These issues must be treated seriously as they may identify previously unknown product vulnerabilities. IEC 61508 requires field failure reports to be captured and investigated. The same failure reporting procedures can be used for both safety and security, though different types of data may need to be captured for a given incident.

Change Management Requirements

Both IEC 61508 and IEC 62443-4-1 require procedures for change request, change authorization, impact analysis, root cause analysis, documentation of required re-verification and re-validation required and tracking of all modification documentation, including both engineering and user documentation (see Figure 4). While there is a significant overlap of safety and security requirements, there will be some safety-specific and security-specific needs as well. For example, the procedure should require that a vulnerability score (e.g., CVSS) is documented for a security-related issue. Similarly, it may be necessary to capture information about the use of the product in which a safety product failure is detected (shipping, inspection, commissioning, operation, etc.) may be necessary for safety-related issues to more accurately determine failure rates.

Customer Notification Requirements

DM-5 requires the appropriate disclosure of reportable security-related issues to end users of the product in a timely manner. This requirement is like IEC 61508’s requirement for product manufacturers to notify end users of any systematic safety issues reported to them that might affect the product’s ability to perform the safety function reliably. While there may be some differences in content of the notifications, a single customer notification procedure can surely serve to communicate both security-related and safety-related product issues (see Figure 4).

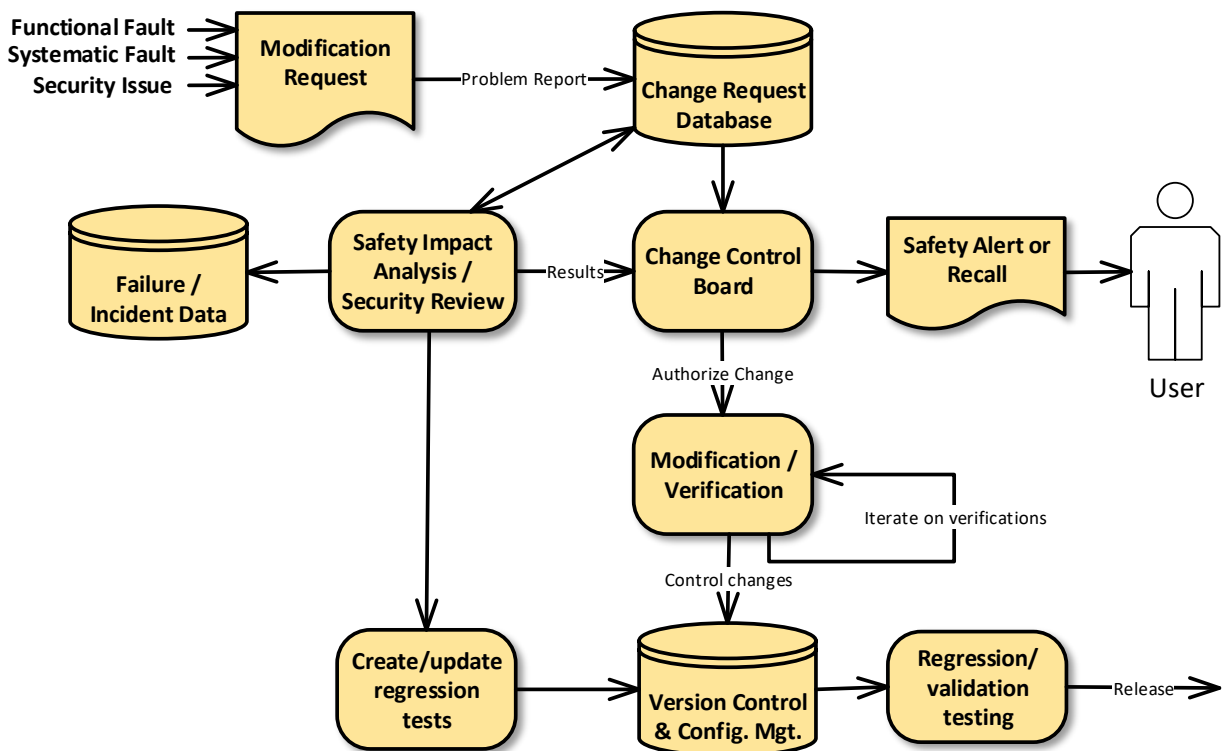


Figure 4 – A typical IEC 61508 Modification Process

SUM-1 requires that validation and verification of security updates ensure that the updates perform as specified and don't cause any regression of function or performance. The security update management requirements in IEC 62443 correspond with the IEC 61508 modification process requirements (see Figure 4). The IEC 61508 modification process requires impact analysis to include specification of regression testing, re-validation and re-verification of all modifications to the product. A 61508-compliant impact analysis, performed as part of the modification process, will ensure that a security update is to be tested as is required by SUM-1.

User / Manufacturer Responsibility Requirements

SG-5 requires user documentation to specify user responsibilities and communicate assumptions concerning secure operation of the product. There is a similarity between these requirements and those for a functional safety manual specified by IEC 61508, which calls for required information such as interface descriptions, product behavior, product versions, changes from previous versions, etc. A single procedure to create/maintain a user document that describes the user requirements to use the product correctly, whether for safety or security operation is adequate to cover requirements in both standards, though there may be additional safety-specific or security-specific document content requirements.

Reference Documents

Industry Standards

Item	Identification	Description
N1	IEC 61508: ed2, 2010	Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems, International Electrotechnical Commission, Geneva, Switzerland
N2	IEC 62443-4-1, 2018	Security for Industrial Automation and Control Systems, Part 4-1: Secure Product Development Lifecycle Requirements

Terms and Definitions

AB: Accreditation Body

ANSI: American National Standards Institute

CB: Certification Body

COTS: Commercial Off-the-Shelf

IAF: International Accreditation Forum

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

RACI: Responsible, Accountable, Consulted and Informed. A RACI matrix describes the “participation by various roles in completing tasks or deliverables for a project” (from https://en.wikipedia.org/wiki/Responsibility_assignment-matrix)

Revision History

Author: Dave Butler

Version V1, Revision R0

March 4, 2019

Dave Butler

Author Biography

Dave Butler is a Senior Safety Engineer for exida, a global, leading, accredited Certification Body, specializing in automation system safety and cybersecurity. As a software and system engineer, he developed products and systems for process control, telecommunications and medical instruments for 30+ years. A graduate of Lehigh University, Dave holds a BS in Electrical Engineering and earned a MS in Computer Engineering from Villanova University.

exida – Who we are.

exida is one of the world's leading accredited certification and knowledge companies specializing in automation system cybersecurity, safety, and availability. Founded in 2000 by several of the world's top reliability and safety experts, exida is a global company with offices around the world. exida offers training, coaching, project-oriented consulting services, standalone and internet-based safety and cybersecurity engineering tools, detailed product assurance and certification analysis, and a collection of online safety, reliability, and cybersecurity resources. exida maintains a comprehensive failure rate and failure mode database on electrical and mechanical components, as well as automation equipment based on hundreds of field failure data sets representing over 350 billion unit operating hours.

exida Certification is an ANSI (American National Standards Institute) accredited independent certification organization that performs functional safety (IEC 61508 family of standards) and cybersecurity (IEC 62443 family of standards) certification assessments.

exida Engineering provides the users of automation systems with the knowledge to cost-effectively implement automation system cybersecurity, safety, and high availability solutions. The exida team will solve complex issues in the fields of functional safety, cybersecurity, and alarm management, like unique voting arrangement analysis, quantitative consequence analysis, or rare event likelihood analysis, and stands ready to assist when needed.

Training

exida believes that safety, high availability, and cybersecurity are achieved when more people understand the topics. Therefore, exida has developed a successful training suite of online, on-demand, and web-based instructor-led courses and on-site training provided either as part of a project or by standard courses. The course content and subjects range from introductory to advanced. The exida website lists the continuous range of courses offered around the world.

Knowledge Products

exida Innovation has made the process of designing, installing, and maintaining a safety and high availability automation system easier, as well as providing a practical methodology for managing cybersecurity across the entire lifecycle. Years of experience in the industry have allowed a crystallization of the combined knowledge that is converted into useful tools and documents, called knowledge products. Knowledge products include procedures for implementing cybersecurity, the Safety Lifecycle tasks, software tools, and templates for all phases of design.

Tools and Products for End User Support

- exSILentia® – Integrated Safety Lifecycle Tool
 - PHAx™ (Process Hazard Analysis)
 - LOPAx™ (Layer of Protection Analysis)
 - SILAlarm™ (Alarm Management and Rationalization)



excellence in dependable automation

- SILect™ (SIL Selection and Layer of Protection Analysis)
- Process SRS (PHA based Safety Requirements Specification definition)
- SILver™ (SIL verification)
- Design SRS (Conceptual Design based Safety Requirements Specification definition)
- Cost (Lifecycle Cost Estimator and Cost Benefit Analysis)
- PTG (Proof Test Generator)
- SILstat™ (Life Event Recording and Monitoring)
- exSILentia® Cyber- Integrated Cybersecurity Lifecycle Tool
 - CyberPHAx™ (Cybersecurity Vulnerability and Risk Assessment)
 - CyberSL™ (Cyber Security Level Verification)

Tools and Products for Manufacturer Support

- FMEDAx (FMEDA tool including the exida EMCRH database)
- ARCHx (System Analysis tool; Hardware and Software Failure, Dependent Failure, and Cyber Threat Analysis)

For any questions and/or remarks regarding this White Paper or any of the services mentioned, please contact exida:

exida.com LLC
80 N. Main Street
Sellersville, PA, 18960
USA
+1 215 453 1720
+1 215 257 1657 FAX
info@exida.com