



Standards
Certification
Education & Training
Publishing
Conferences & Exhibits

Setting the Standard for Automation™

TECHNICAL REPORT

ISA-TR84.00.09-2017

Cybersecurity Related to the Functional Safety Lifecycle

Approved 10 April 2017

NOTICE OF COPYRIGHT

This is a copyright document and may not be copied or distributed in any form or manner without the permission of ISA. This copy of the document was made for the sole use of the person to whom ISA provided it and is subject to the restrictions stated in ISA's license to that person. It may not be provided to any other person in print, electronic, or any other form. Violations of ISA's copyright will be prosecuted to the fullest extent of the law and may result in substantial civil and criminal penalties.

ISA-TR84.00.09-2017, Cybersecurity Related to the Functional Safety Lifecycle

ISBN: 978-1-945541-49-0

Copyright © 2017 by ISA. All rights reserved. Not for resale. Printed in the United States of America.

ISA
67 Alexander Drive
P. O. Box 12277
Research Triangle Park, NC 27709 USA

PREFACE

This preface, as well as all footnotes and annexes, is included for information purposes and is not part of ISA-TR84.00.09-2017.

This document has been prepared as part of the service of ISA, the International Society of Automation, toward a goal of uniformity in the field of instrumentation. To be of real value, this document should not be static but should be subject to periodic review. Toward this end, the Society welcomes all comments and criticisms and asks that they be addressed to the Secretary, Standards and Practices Board; ISA; 67 Alexander Drive; P. O. Box 12277; Research Triangle Park, NC 27709; Telephone (919) 549-8411; Fax (919) 549-8288; E-mail: standards@isa.org.

It is the policy of ISA to encourage and welcome the participation of all concerned individuals and interests in the development of ISA standards, recommended practices and technical reports. Participation in the ISA standards-making process by an individual in no way constitutes endorsement by the employer of that individual, of ISA or of any of the standards, recommended practices and technical reports that ISA develops.

CAUTION — ISA DOES NOT TAKE ANY POSITION WITH RESPECT TO THE EXISTENCE OR VALIDITY OF ANY PATENT RIGHTS ASSERTED IN CONNECTION WITH THIS DOCUMENT, AND ISA DISCLAIMS LIABILITY FOR THE INFRINGEMENT OF ANY PATENT RESULTING FROM THE USE OF THIS DOCUMENT. USERS ARE ADVISED THAT DETERMINATION OF THE VALIDITY OF ANY PATENT RIGHTS, AND THE RISK OF INFRINGEMENT OF SUCH RIGHTS, IS ENTIRELY THEIR OWN RESPONSIBILITY.

PURSUANT TO ISA'S PATENT POLICY, ONE OR MORE PATENT HOLDERS OR PATENT APPLICANTS MAY HAVE DISCLOSED PATENTS THAT COULD BE INFRINGED BY USE OF THIS DOCUMENT AND EXECUTED A LETTER OF ASSURANCE COMMITTING TO THE GRANTING OF A LICENSE ON A WORLDWIDE, NONDISCRIMINATORY BASIS, WITH A FAIR AND REASONABLE ROYALTY RATE AND FAIR AND REASONABLE TERMS AND CONDITIONS. FOR MORE INFORMATION ON SUCH DISCLOSURES AND LETTERS OF ASSURANCE, CONTACT ISA OR VISIT WWW.ISA.ORG/STANDARDSPATENTS.

OTHER PATENTS OR PATENT CLAIMS MAY EXIST FOR WHICH A DISCLOSURE OR LETTER OF ASSURANCE HAS NOT BEEN RECEIVED. ISA IS NOT RESPONSIBLE FOR IDENTIFYING PATENTS OR PATENT APPLICATIONS FOR WHICH A LICENSE MAY BE REQUIRED, FOR CONDUCTING INQUIRIES INTO THE LEGAL VALIDITY OR SCOPE OF PATENTS, OR DETERMINING WHETHER ANY LICENSING TERMS OR CONDITIONS PROVIDED IN CONNECTION WITH SUBMISSION OF A LETTER OF ASSURANCE, IF ANY, OR IN ANY LICENSING AGREEMENTS ARE REASONABLE OR NON-DISCRIMINATORY.

ISA REQUESTS THAT ANYONE REVIEWING THIS DOCUMENT WHO IS AWARE OF ANY PATENTS THAT MAY IMPACT IMPLEMENTATION OF THE DOCUMENT NOTIFY THE ISA STANDARDS AND PRACTICES DEPARTMENT OF THE PATENT AND ITS OWNER.

ADDITIONALLY, THE USE OF THIS DOCUMENT MAY INVOLVE HAZARDOUS MATERIALS, OPERATIONS OR PROCESS EQUIPMENT. THE DOCUMENT CANNOT ANTICIPATE ALL POSSIBLE APPLICATIONS OR ADDRESS ALL POSSIBLE SAFETY ISSUES ASSOCIATED WITH USE IN HAZARDOUS CONDITIONS. THE USER OF THIS TECHNICAL REPORT SHOULD EXERCISE SOUND PROFESSIONAL JUDGMENT CONCERNING ITS USE AND APPLICABILITY UNDER THE USER'S PARTICULAR CIRCUMSTANCES. THE USER SHOULD ALSO CONSIDER THE APPLICABILITY OF ANY GOVERNMENTAL REGULATORY LIMITATIONS AND ESTABLISHED SAFETY AND HEALTH PRACTICES BEFORE IMPLEMENTING THIS TECHNICAL REPORT.

ISA (www.isa.org) is a nonprofit professional association that sets the standard for those who apply engineering and technology to improve the management, safety, and cybersecurity of modern

automation and control systems used across industry and critical infrastructure. Founded in 1945, ISA develops widely used global standards; certifies industry professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its 40,000 members and 400,000 customers around the world.

ISA owns Automation.com, a leading online publisher of automation-related content, and is the founding sponsor of The Automation Federation (www.automationfederation.org), an association of non-profit organizations serving as "The Voice of Automation." Through a wholly owned subsidiary, ISA bridges the gap between standards and their implementation with the ISA Security Compliance Institute (www.isasecure.org) and the ISA Wireless Compliance Institute (www.isa100wci.org).

The following members of ISA84 Working Group 9 served as active contributors in the development of this technical report revision:

NAME	AFFILIATION
Harold W Thomas (Hal), Chair	exida
Kevin Arnold	Phillips 66
David Bennett	Phillips 66
Rahul Bhojani	BP
John D. Day	Air Products and Chemicals
David Deibert	Air Products and Chemicals
Andrew Feben	Eigen Ltd
David Gunter	Air Products and Chemicals
Eric Hopp	Rockwell Automation
Kevin Klein	Chevron ETC
Vic Maggioli	Feltronics Corp
Marcelo Mollicone	SYM PCS
Nagappan Muthiah	Wood Group
Eric Persson	exida
Jeff Potter	Emerson
Richard Roberts	Suncor Energy
Eloise Roche	SIS-TECH Solutions
Byron Schneidau	BP Pipelines & Logistics
Herman Storey	Herman Storey Consulting
Paulo Vergara	Zavior Consulting

The following members of ISA84 and ISA99 are acknowledged for their peer review of this technical report revision:

NAME	AFFILIATION
John Ayuk	Wood Group
Marcio Baeta	SIS-TECH Solutions
Marc Baque	Total
Brad Bonnette	Wood Group
Bob Brown	Consultate LLC
Libero Corvaglia	SIS-TECH Solutions
Eric Cosman	OIT Concepts
John Cusimano	aeSolutions
David Dalke	Wood Group
Koji Demachi	Yokogawa
Harvinder Gambhir	Reliance JIO
James Gilsinn	Kenexis Consulting
Paul Gruhn	aeSolutions

Rahul Gupta
James Harris
Jean-Pierre Hauet
William Hearn
Dennis Holstein
Eric Jandik
Kevin Klein
Scott Nielsen
Khar Peng Ong
Nicholas Sands
Angela Summers
Joseph Weiss
Dennis Zetterberg

Wood Group
UOP
KB Intelligence
SIS-TECH Solutions
OPUS Consulting Group
Chevron ETC
Chevron ETC
Wood Group
Chevron ETC
DuPont
SIS-TECH Solutions, LP
Applied Control Solutions
Chevron

The following served as members of the Standards and Practices Board and approved the document on 10 April 2017:

NAME

M. Wilkins, Vice President
D. Bartusiak
D. Brandl
P. Brett
E. Cosman
D. Dunn
J. Federlein
B. Fitzpatrick
J. Gilsinn
J.-P. Hauet
D. Lee
G. Lehmann
K.-P. Lindner
T. McAviney
V. Mezzano
C. Monchinski
G. Nasby
M. Nixon
D. Reed
N. Sands
H. Sasajima
H. Storey
K. Unger
I. Verhappen
D. Visnich
W. Weidman
J. Weiss
D. Zetterberg

AFFILIATION

Yokogawa
ExxonMobil Research & Engineering
BR&L Consulting
Honeywell Inc.
OIT Concepts, LLC
Phillips 66
Federlein & Assoc. LLC
Wood Group Mustang
Kenexis Consulting
KB Intelligence
UCDS
AECOM
Endress+Hauser Process Solutions AG
Consultant
Fluor Corp.
Automated Control Concepts Inc.
City of Guelph Water Services
Emerson Process Management
Rockwell Automation
DuPont
Fieldcomm Group Inc. Asia-Pacific
Herman Storey Consulting
Consultant
Industrial Automation Networks
Burns & McDonnell
Consultant
Applied Control Solutions LLC
Chevron Energy

This page intentionally left blank.

CONTENTS

FOREWORD	9
0 Introduction	11
0.1 Executive summary	11
0.2 Integrated lifecycle	11
0.3 Safety versus cybersecurity considerations	13
1 Scope	17
2 References	17
3 Terms, definitions, abbreviated terms, acronyms, and conventions	18
3.1 Terms and definitions	18
3.2 Abbreviated terms and acronyms	20
4 Management of SCAI cybersecurity in the process sector	23
4.1 Objective	23
4.2 Guidelines	23
5 Cyber risk assessment phase	27
5.1 Overview	27
6 Hazard and risk analysis	29
7 Allocation of Security Levels (SL)	32
8 Cybersecurity Requirements Specification (CSRS) for the IACS	33
9 Cybersecurity design and implement phase	35
9.1 Overview	35
10 Design and engineering	37
10.1 Cybersecurity concept	37
10.2 Other means of cyber risk reduction	40
10.3 Security level verification	40
10.4 Detailed design	41
10.5 Detailed design verification	42
10.6 System Integration	43
10.7 Cybersecurity FAT (CFAT)	43
11 Installation, commissioning and validation	44
11.1 Overview	44
11.2 Cybersecurity Site Acceptance Test (CSAT)	44
11.3 Initial validation of countermeasures	44
11.4 Pre-Startup Safety Review (PSSR)	44
12 Operate and maintain phase	45
12.1 Overview	45
12.2 Operation	47
12.3 Cybersecurity metrics	47
12.4 Physical security of a SCAI system	47
12.5 Unauthorized access of a SCAI system	48
12.6 Authorized change management of a SCAI system	48
12.7 Unauthorized communication with a SCAI system	48

12.8 Cybersecurity threat events.....	49
12.9 Normal maintenance	49
12.10 Mechanical integrity	49
12.11 Inspection/Audit	49
12.12 Remote access	49
12.13 Bypasses	51
12.14 Tools.....	51
12.15 Periodic assessments	51
13 Modification	51
14 Decommissioning.....	53
Annex A – Example SCAI interfaces	55
A.1 Overview.....	55
A.2 Air-gapped (2 zones)	59
A.3 Interfaced (2 zones)	61
A.4 Integrated systems with isolated networks (2 zones)	63
A.5 Integrated systems with shared network (partial 2 zone)	65
A.6 Combined systems with strong dependency (1 zone)	67
A.7 Shared logic solver (1 zone)	68
A.8 Supervisory control and data acquisition systems (SCADA)	70
Annex B – Cyber risk assessment example procedures	73
B.1 High level cyber risk assessment procedure.....	73
B.2 Detailed cyber risk assessment procedure	75
Annex C – Cyber vulnerability assessment	81
C.1 Ongoing lifecycle vulnerability assessment	81
C.2 First time existing plant vulnerability assessment ¹⁶	81
Annex D – Cybersecurity level verification example	83
D.1 Example cyber risk criteria	84
D.2 Example results of high level cyber risk assessment	85
D.3 Example countermeasure strength assessment.....	88
D.3.1 External denial of service (DoS) example SL verification	90
D.3.2 Unintentional internal DoS example SL verification	93
D.3.3 External general virus example SL verification	94
D.3.4 External sophisticated intentional malware attack example SL verification	95
D.4 SL verification planning	97
Annex E – Cybersecurity metrics for IACS.....	99
E.1 Preface	99
E.2 Introduction.....	99
Annex F – Manufacturer cybersecurity manual	105
Annex G – Typical countermeasures	107
Annex H – ISA-TR84.00.09 / IEC 61511 cross references	113
Bibliography	114

FOREWORD

This technical report is part of a series of standards and technical reports that address the issue of safety instrumented system security. It has been developed by Working Group 9 of the ISA84 committee in cooperation with the ISA99 committee.

This technical report provides guidance on how to implement cybersecurity within the IEC-61511 and ISA-84.00.01-2004 lifecycle. This is the second issue of this technical report. Members of the ISA84 and ISA99 committees contributed to this effort.

Readers of this technical report are asked to send comments on the content and suggestions for coverage in future revisions to the following email address:

standards@isa.org

This page intentionally left blank.

0 Introduction

0.1 Executive summary

Safety Instrumented Systems (SIS) represent one layer of protection that may be implemented in order to reduce risk within the process industry. Other layers of protection may consist of instrumented systems performing alarms, interlocks, permissive functions or controls using devices within the basic process control system (BPCS), as well as non-instrumented systems such as relief devices, check valves, etc. Traditional process hazard analysis (PHA), in the past, has generally excluded the potential for cyber related attacks to cause process safety incidents. Given that targeted attacks on industrial automation and control systems (IACS), including the systems executing safety controls, alarms, and interlocks (SCAI), have occurred and these systems are increasingly being connected to other business systems, cyber vulnerabilities represent a significant potential for common mode failure. As a result, it is necessary in today's world to include cyber risk in the overall PHA.

Without addressing cybersecurity throughout the entire safety lifecycle, it is not possible to adequately understand the relative independence and integrity of the various layers of protection that involve instrumented systems, including the SIS.

The underlying premise of this document is to help the reader understand how to integrate cybersecurity into the safety lifecycle. Guidance is provided on how to implement, operate and maintain safety controls, alarms, and interlocks (SCAI) in a secure manner. As part of this integration, it should also be understood that achieving higher security levels may result in less convenience to the end user. Addressing cybersecurity and functional safety of the SCAI systems within the IACS requires that this document serve both the ISA84 series of standards as well as the ANSI/ISA-62443 series of standards.

0.2 Integrated lifecycle

The work process to ensure security of the IACS should account for the entire functional safety lifecycle, including risk assessment, design, manufacture, factory acceptance testing (FAT), site acceptance testing (SAT), commissioning, operation, maintenance, the ongoing mechanical integrity program, modification and decommissioning. As part of the safety lifecycle (SLC), as documented in ISA-84.00.01-2004 (see Figure 1), security should be addressed at all phases.

Figure 2 seeks to show, at a high level, how functional safety and cybersecurity could integrate within the overall safety lifecycle, starting with a new process plant at the initial scope stage and continuing throughout all phases of the lifecycle. Although the NIST (National Institute of Standards and Technology) framework is not the only one that can be selected, it was used as a quality assurance tool when developing this technical report to help ensure any potential gaps were minimized. The overall result is an example of a single process safety management process, incorporating IEC-61511, ISA-84.00.01, ANSI/ISA-84.91.01, Draft ISA-84.91.03, and the applicable ANSI/ISA-62443 series of standards. Additional lifecycle details are provided throughout this technical report. It is recognized that the lifecycle figures in this technical report are an interpretation and that there may be other appropriate means to address the IEC 61511 lifecycle with respect to functional safety and cybersecurity. It should also be recognized that different functional disciplines will of necessity be responsible for different aspects of the lifecycle. This technical report is mainly targeted at process control, process safety, and operations personnel so that the impact of cybersecurity regards process safety can be better understood as well as to help understand the necessary relationship with information technology (IT) personnel. While not directly targeted at IT personnel, they may find this document useful regards the relationship between safety and cybersecurity in the process industry.

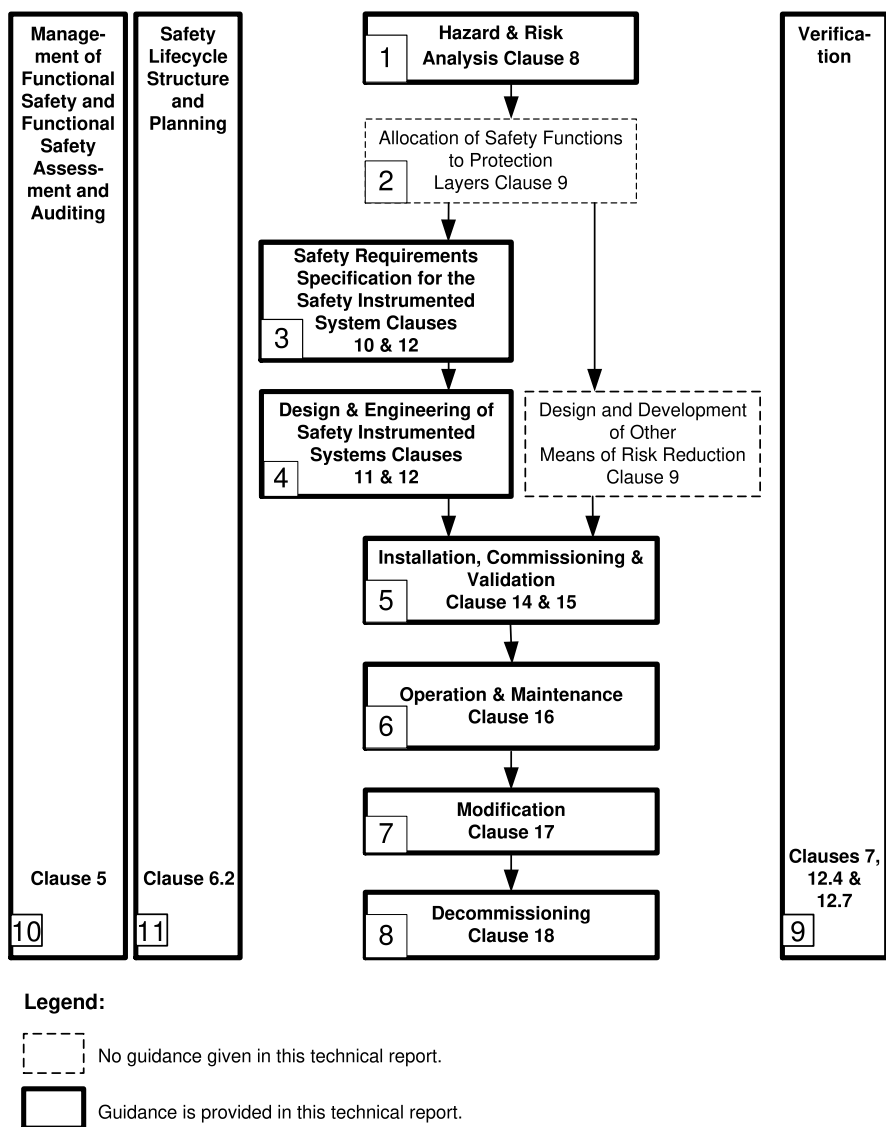


Figure 1 – Graphical representation of the safety lifecycle

NOTE The clause numbers within the elements of Figure 1 above refer to clauses in ISA-84.00.01-2004 Part 1 (IEC 61511-1 Mod).

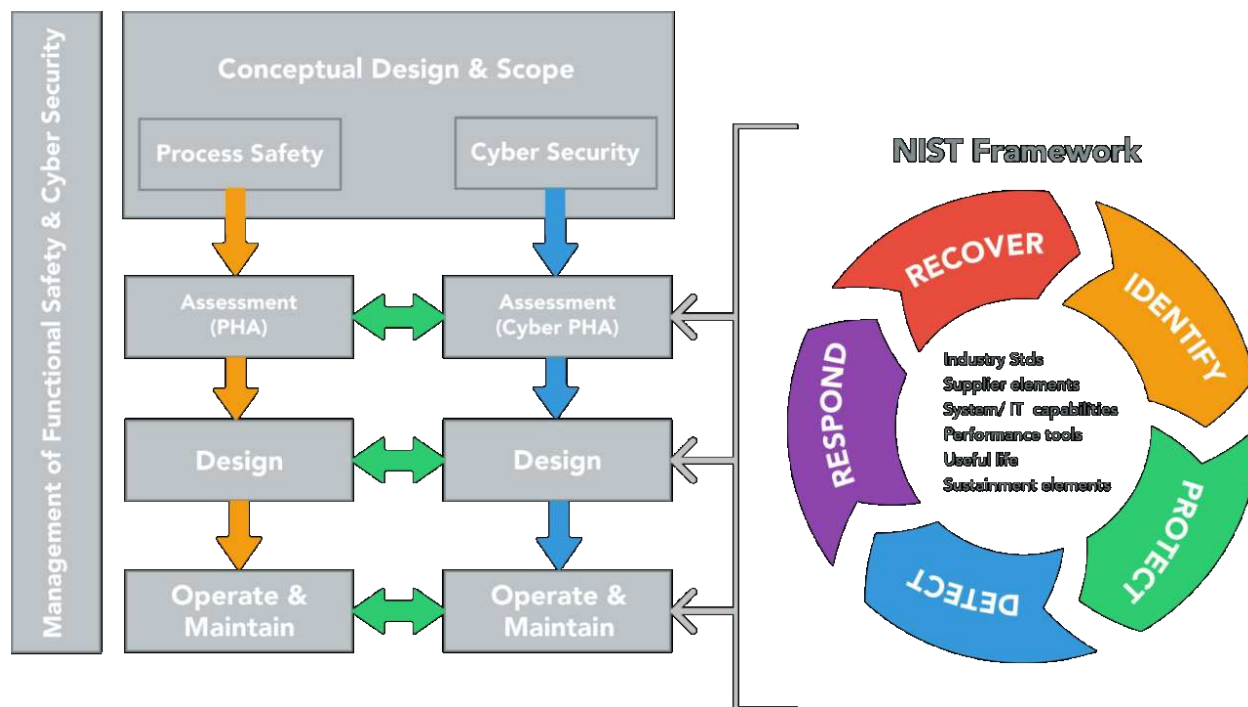


Figure 2 – Cybersecurity lifecycle integrated with process safety management

0.3 Safety versus cybersecurity considerations

Traditionally, different disciplines have dealt with safety and cybersecurity with not much overlap. In today's world, neither functional safety nor information technology are independent of one another. It is important for both functional areas to understand the differences as well as the overlaps so that jointly, appropriate best practices can be employed and any culture of "Us versus Them" can evolve into "We." As such, it is important to understand the typical differences in how the IT professional views their requirements versus how a process control engineer views theirs.

Common differences between IT and IACS that typically exist today are included in Table 1:

Table 1 – Current snapshot comparison of IT versus IACS disciplines

	IT	IACS
Response time performance	Limited knowledge of process response time requirements	Should be real time relative to the process dynamics, e.g., milli-seconds, seconds.
Availability	Occasional outages tolerated	Outages not tolerable
Data confidentiality	Data privacy is critical	Data privacy generally less critical
Data integrity / Configuration and/or software integrity	Critical	Critical
Technology lifecycle	3 – 5 years	20+ years
Outsourcing	Common	Less common
Patching	Timely	Less frequent / As required
Anti-virus	Common	Old legacy systems may not be supported. Potential undesirable side-effects with real-time process control software.
Cybersecurity awareness	Good	Poor / Improving
Process safety risk awareness	Poor	Good
Risk assessment granularity	Coarse (e.g., all control loops)	Fine (e.g., individual loop)
Changes	Easy to implement	Difficult to implement
Safety integrity awareness	Poor	Good
PHA revalidation	No explicit requirement	No greater than 5 years

Successful cybersecurity programs consider the differences between traditional IT roles and IACS to develop a cohesive program that delivers on the needs of both organizations.

Table 2 below contrasts cybersecurity versus functional safety as a function of the safety lifecycle.

Table 2 – Comparison of functional safety and IT cybersecurity in IACS using a lifecycle approach ^[21]

Lifecycle phase		Functional safety	IACS cybersecurity
Risk analysis	Target of evaluation	- Equipment under control (EUC)	- System under Consideration (SuC)
	Failure likelihood	- Random failures due to operational and environmental stresses - Systematic failures due to errors during safety lifecycle	- Threats: internal, external or combination - Vulnerabilities due to • component or system design flaws • making non-validated changes • not following cybersecurity practices and procedures • Threats exploiting vulnerabilities leads to failure
	Consequence severity	- Impact on environment, health and safety of personnel and the general public	- Loss of availability and/or data integrity has direct impact, and loss of confidentiality has indirect impact on functional safety
	Risk categorization	- Based on likelihood and severity; risk may be quantified	- Based on likelihood and severity; risk is currently qualitative - Risk categorization for every cybersecurity requirement - Multi-dimensional problem - Assigned to zone with target SL for each zone/conduit
	Risk mitigation measures	- Relies on independent protection layers concept - Safeguards reduce likelihood of consequence evaluated - Identifies integrity requirements for safeguards; for SIF assigns target SIL	- Relies on cybersecurity countermeasures within zones, conduits interconnecting zones, and defense in depth concept - Countermeasures reduce likelihood - Identifies requirements for countermeasures to meet the zone target SL for each threat vector
Implementation of measures		- Safety manual for components - Quantitative SIL verification for SIF	- Cybersecurity manual for components - Verification through different levels of testing for target SL
Operation and maintenance		- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Demand rate and component failures to be monitored - Awareness and training	- Restrict access to IACS components to competent personnel with necessary access privileges - Periodic testing of measures - Frequent reviews to identify new vulnerabilities and take appropriate action, if necessary - Awareness and training - Cyber risk reassessment after each software or hardware change
Management system		- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation	- Defines requirements for competency, training, verification, testing, audit, MOC, and documentation

This page intentionally left blank.

1 Scope

This document is intended to address and provide guidance on integrating the cybersecurity lifecycle with the safety lifecycle as they relate to Safety Controls, Alarms, and Interlocks (SCAI), inclusive of Safety Instrumented Systems (SIS). This scope includes the work processes and countermeasures used to reduce the risk involved due to cybersecurity threats to the Industrial Automation and Control System (IACS) network.

This scope provides recommendations to ensure SCAI are adequately secured due to the potential for cyber attacks that can act like common mode failures that initiate a hazardous demand and also prevent instrumented protection functions, including the SIS, from performing their intended purpose. The scope is intended to address cybersecurity from both external and internal threats. Although not directly within the scope, enterprise networks, business networks and process information networks (demilitarized zones) that represent a threat vector to the SCAI systems, or contain countermeasures that reduce the risk to the SCAI systems from external cyber threats, are included.

The scope does not address physical plant protection (for example, fences, bollards, and grounding) that has the intent of preventing unauthorized entry into the plant so as to prevent theft, vandalism, or physical damage, but does address physical access issues related to cybersecurity of the IACS (12.4 of this technical report). SCAI systems that are constructed exclusively of electrical/electronic components without digital signal technology are not vulnerable to cybersecurity attacks, and these technologies are not discussed in this technical report.

2 References

The following documents are important for understanding this technical report. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies. For information on obtaining ISA standards and technical reports, visit: www.isa.org/findstandards

In addition, readers should be aware of the ongoing development of additional standards in the ANSI/ISA-62443 series, *Security for Industrial Automation and Control Systems*, listed in the Bibliography. For an update on the status of these standards, visit <https://www.isa.org/isa99/>.

- IEC-61508-2010, *Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems*
- IEC-61511-1, *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*.
- ISA-84.00.01-Part 1 (IEC 61511-1), *Functional Safety: Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, Definitions, System, Hardware and Software Requirements*.
- ANSI/ISA-84.91.01-2012, *Identification and Mechanical Integrity of Safety Controls, Alarms, and Interlocks in the Process Industry*, 2012.

3 Terms, definitions, abbreviated terms, acronyms, and conventions

3.1 Terms and definitions

Conduit [ANSI/ISA-62443-1-1 & ISA -62443-1-2 revised]	1) Logical grouping of communication assets that protects the security of the channels it contains. 2) Logical grouping of communication channels, between connecting two or more zones that share common security requirements. Note to entry: Conduits are analogous to the way that a physical conduit protects cables from physical damage.
Countermeasure [ANSI/ISA-62443-1-1]	Action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken. Note to entry: The term "control" is also used to describe this concept in some contexts. The term countermeasure has been chosen to avoid confusion with the word control in the context of "process control".
Cyber asset	Device contained within the system under consideration (SuC), e.g., controller, server, engineering work station, etc.
Cyber incident	Communication with an E/E/PE device within a control system that negatively impacts process safety, the environment, operations, confidentiality, SCAI integrity, or IACS availability
Cybersecurity [ISA -62443-1-2]	Measures taken to protect a computer or computer system against unauthorized access or attack
Industrial Automation and Control System (IACS) [ISA -62443-3-3]	Collection of personnel, hardware, software and policies involved in the operation of the industrial process and that can affect or influence its safe, secure and reliable operation.
Risk	A measure of human injury, environmental damage, economic loss, loss of intellectual property or loss of privacy in terms of both the incident likelihood and the magnitude of the loss or injury. A simplified version of this relationship expresses risk as the product of the likelihood and the consequences (i.e., risk = consequence x likelihood) of an incident.
Risk Reduction Factor (RRF) - Target	The measure of the degree of risk reduction required to achieve tolerable risk. RRF can be expressed as the ratio of unmitigated risk divided by tolerable risk.
Risk Reduction Factor (RRF) - Achieved	The measure of the degree of risk reduction achieved by a safeguard, countermeasure, or protection strategy. Achieved RRF can be expressed as the ratio of unmitigated risk divided by mitigated risk resulting from that safeguard, countermeasure, or protection strategy. For an independent low demand safety function, this can be expressed as the reciprocal of the average probability of failure on demand.
Risk tolerance	Willingness by authority having jurisdiction to live with a risk so as to secure certain benefits in the confidence that the risk is one that is worth taking and that it is being properly controlled. However, it does not imply

	that everyone would agree without reservation to take this risk or have it imposed on them.
Risk tolerance criteria [CCPS Criteria]	A predetermined measure of risk used to aid decisions about whether further efforts to reduce risk are warranted.
Safety [ISO/IEC Guide 51:1999, definition 3.1]	Freedom from unacceptable risk.
Safety controls, alarms and interlocks [ANSI/ISA-84.91.01]	Process safety safeguards implemented with instrumentation and controls, used to achieve or maintain a safe state for a process, and required to provide risk reduction with respect to a specific hazardous event. Note 1 to entry: There are many types of safety controls, alarms, and interlocks, for example: safety alarm, safety interlock, safety permissive, detection or suppression, emergency shutdown, safety critical control, and safety instrumented system. The terms listed in the illustration are not intended to be construed as the only terms applied to safety controls, alarms, and interlocks; neither should it be assumed that each type is necessarily separate and independent. Note 2 to entry: Refer to ISA-84.00.01-2004 (IEC 61511 Mod) for additional requirements related to safety instrumented systems. Note 3 to entry: Examples of non-instrumented safeguards include rupture disks, relief valves, dikes, etc.
Security level [ANSI/ISA-62443-1-1]	Level corresponding to the required effectiveness of countermeasures and inherent security properties of devices and systems for a zone or conduit based on assessment of risk for the zone or conduit.
Security level 0 [ISA -62443-3-2]	Security level with the following attributes: • No specific requirements or security protection.
Security level 1	Security level 1 has the following attributes: • Intended to protect against casual or coincidental violation • Countermeasure and detection effectiveness capable of delaying or denying an attack for a period of 4 to 8 hour
Security level 2	Security level with the following attributes: • Intended to protect against intentional violation using simple means with low resources, generic skills and low motivation • Countermeasure and detection effectiveness capable of delaying or denying an attack for a period of days • Order of magnitude improvement in risk reduction factor (RRF) over a security level 1
Security level 3	Security level with the following attributes: • Intended to protect against intentional violation using sophisticated means with moderate resources, IACS specific skills and moderate motivation • Countermeasure and detection effectiveness capable of delaying or denying an attack for a period of days to weeks

	Order of magnitude improvement in risk reduction factor (RRF) over a security level 2
Security level 4	Security level with the following attributes: - Intended to protect against intentional violation using sophisticated means with extended resources, IACS specific skills and high motivation - Countermeasure and detection effectiveness capable of delaying or denying an attack for a period of weeks to months - Order of magnitude improvement in risk reduction factor (RRF) over a security level 3.
Threat	- Potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause harm. - Circumstance or event with the potential to adversely affect organizational operations (e.g., mission, functions, reputation), organizational assets, IACS, or personnel via means contrary to security policy, intentionally or unintentionally cause the destruction, disclosure, modification of data, control logic, SCAI logic, and/or denial of service.
Threat agent	Method(s), individual(s) or organization(s) that could breach the security of a facility, operation or system by exploiting a vulnerability
Threat vector [ISA -62443-1-2]	Path or means by which a threat agent can gain access to an asset resulting in a negative outcome
Unmitigated cyber risk	Level of risk that is present in a system before any cybersecurity countermeasures are considered
Vulnerability [ISA -62443-1-2 slight revision to no. 2]	- Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's integrity or security policy. - Weakness in an IACS function, procedure, internal control or implementation that could be exploited or triggered by a threat source, either intentionally designed into computer components (e.g., remote port access) or accidentally inserted at any time during the lifecycle.
Zone [ISA -62443-3-3]	Grouping of logical or physical assets that share common security requirements. Note to entry: A zone has a clear border. The security policy of a zone is typically enforced by a combination of mechanisms both at the zone edge and within the zone.

For additional definitions, see IEC-61511 ^[2], ISA-84.00.01-2004 ^[3], and ISA-62443-1-2 ^[5]

3.2 Abbreviated terms and acronyms

The abbreviated terms and acronyms used in this document are defined as follows:

ACL	Access Control List
APT	Advanced Persistent Threat
ALARP	As Low as Reasonably Practical

ANSI	American National Standards Institute
BPCS	Basic Process Control System
CCPS	Center for Chemical Process Safety
CFAT	Cybersecurity Factory Acceptance Test
CMMI-SVC	Capability Maturity Model Integration - Services
COM	Communication Module
COTS	Commercial off the Shelf
CSA	Cybersecurity Assessment
CSAT	Cybersecurity Site Acceptance Test
CSRS	Cybersecurity Requirements Specification
DC	Data Confidentiality
DEP	Data Execution Prevention
DoS	Denial of Service
DNP	Distributed Network Protocol
EMC	Electromagnetic Compatibility
FAT	Factory Acceptance Testing
FR	Foundational Requirement
FSA	Functional Safety Assessment
H&RA	Hazard and Risk Assessment
HAZID	Hazard Identification Assessment
HAZOP	Hazard and Operability Method
HIDS	Host Intrusion Detection System
HMI	Human Machine Interface
HSE	Health and Safety Executive
HTTPS	Hypertext Transfer Protocol Secure
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control Systems
IAMS *	Instrument Asset Management System
IEC	International Electrotechnical Commission
IP	Internet Protocol
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
LOPA	Layer of Protection Analysis
MOC	Management of Change
MI	Mechanical Integrity

NIDS	Network Intrusion Detection System
NIPS	Network Intrusion Prevention System
NIST	National Institute of Standards and Technology
NIC	Networked Interface Card
OPC	Open Platform Communications
OS	Operating System
PCN	Process Control Network
PE	Programmable Equipment
PES	Programmable Electronic System
PHA	Process Hazard Analysis
PIN	Process Information Network
PKI *	Public Key Infrastructure
PSSR	Pre-startup Safety Review
RA	Resource Availability
RAGAGEP	Recognized and Generally Accepted Good Engineering Practices
RFI	Radio Frequency Interference
RDF	Restricted Data Flow
SAT	Site Acceptance Testing
SCAI	Safety Controls, Alarms, and Interlocks
SI	System Integrity
SIF	Safety Instrumented Function
SIL	Safety Integrity Level
SIS	Safety Instrumented System
SL *	Security Level
SL-A	Security Level Achieved
SL-C	Security Level Capability
SL-T	Security Level Target
SLC	Safety Lifecycle
SRS	Safety Requirements Specification
SSH	Secure Shell Protocol
SuC	System under Consideration
TRE	Timely Response to Events
UC	Use Control
USB	Universal Serial Bus

NOTE Acronyms and associated terms marked with an asterisk do not appear in IEC 61511.

4 Management of SCAI cybersecurity in the process sector

4.1 Objective

Successful management of safety includes a series of functional safety and cybersecurity related management activities, all of which are necessary in order to ensure that functional safety objectives are met. The functional safety management system is intended to ensure the assumed performance is achieved by the SCAI. As such, for the remainder of this document, higher level terms such as IACS and SCAI will be used when referring to the organizations associated with those policies and strategies, including management of physical access relating to functional safety and cybersecurity of SCAI.

4.2 Guidelines

4.2.1 General

An organization's functional safety policy and strategy should be underpinned by an organizational cybersecurity strategy, both of which will be supported by robust performance measurement procedures. Cybersecurity countermeasures employed by an organization should consist of both cybersecurity policies and procedure-level countermeasures as well as technical countermeasures. Cybersecurity policies and procedure-level countermeasures may include staff training and awareness programs, testing programs, change management programs, identification and authorization procedures, and the like. The policies should be understood and supported by senior management.

Any cybersecurity management system implemented within an organization should have included in it conditions which dictate re-evaluating the risk assessment. These may include, but are not limited to

- developing a new, or designing a modification to, an existing process control system or SCAI system;
- implementing a new or modified process control system or SCAI system; and
- retiring/decommissioning a process control system or SCAI system.

4.2.2 Organization and resources

Those responsible for the execution and/or measurement of the performance for each of the safety lifecycle phases should be clearly identified and then communicated to applicable personnel so that they understand their accountabilities and responsibilities therein. These roles and responsibilities extend beyond the organization itself and includes product suppliers as well. There are a range of potential requirements that may apply, requiring a breadth of applicable engineering competencies, including process engineering, instrumentation and controls, cybersecurity, physical security, legal and regulatory knowledge, functional safety engineering, etc.

The roles and responsibilities associated with cybersecurity should be aligned with both internal roles as well as with external partners.

The complexities and potential shortfalls in individual, organizational, and product supplier competency while maintaining cybersecurity and functional safety within the IACS are such that a sustainable, auditable program of training, familiarization and assessment is recommended.

4.2.3 Competency

The achievement of functional safety and cybersecurity requires the implementation of the safety lifecycle while ensuring that persons who are responsible for any safety lifecycle activities also have the appropriate competency in cybersecurity. The following competence factors should be addressed when assessing as well as justifying the competency level of persons to carry out their duties:

- Experience appropriate to the application area
- Experience appropriate to the information technology and have the ability to demonstrate knowledge
- Experience appropriate to the IACS technology and have the ability to demonstrate knowledge
- Functional safety engineering experience appropriate to the technology
- Knowledge of the legal and safety regulatory framework
- The consequences of failure of the safety-related system(s) due to a cyber incident
- The safety requirements of the safety-related system(s) process control network
- The novelty of the network design, design procedures or application
- Previous experience and its relevance to the specific duties to be performed and the technology being employed
- The ability to recognize when specialist advice or assistance is needed

Personnel capable of performing the work should be identified through a documented competency assessment process. Aspects of this may include:

- Attended appropriate level of training for duties to be performed
- Requirements for requalification
- Auditable records of training and qualification assessments
- External cybersecurity accreditation by a recognized professional body
- Witness of suitable performance by competent person

4.2.4 Risk management

Throughout the safety lifecycle, risk assessment and management should be accomplished with respect to all identified process safety and cyber hazards or vulnerabilities. Clear documentation of risk tolerance should be developed and made available as it relates to potential cyber attacks. When considering process safety risk, the Center for Chemical Process Safety has released several guidelines books on how to establish the risk criteria. In addition, IEC 61511 Part 3 provides examples of different criteria used to support the selection of SIL. Similar criteria and methodologies can be used for cybersecurity risk assessments. Financial considerations should specifically consider the cost as it relates to duration of downtime and degraded operability as well as to damaged equipment, in addition to personal safety and environmental impact.

4.2.5 Safety / Cybersecurity planning

A safety lifecycle plan should document all activities and resources necessary to sustain and secure the IACS, including the SCAI systems, through the entire safety lifecycle. This plan should include an appropriate level of detail regarding cybersecurity and be maintained throughout the lifecycle.

Having access to the sensitive information contained in zone and conduit drawings and the documents related to countermeasure design, verification, and validation would provide significant assistance to a malicious attacker. For this reason, this information should be documented separately from the remainder of the safety plan and consideration should be given in the safety plan to identifying access restrictions that should be applied to this information during all stages of the lifecycle. Documents that are intended to be more widely available (e.g., safety plan and safety requirement specification) should avoid providing countermeasure related details.

Within each organization, a chain of command should be established so that appropriate levels of authority can have access to the information necessary to maintain a safe and cyber secure plant

environment. The plant manager should not be the only person with access to the implementation plan, however; it should also not be publicly available to those without a clear need to know.

4.2.6 Organization procedures

In order to respond effectively to events and changing requirements throughout the lifecycle, procedures should be in place to affect a timely resolution, particularly if these are instigated from audits, investigations, risk / threat assessment or assurance activities.

Network and design information and attributes should be properly classified as to their sensitivity. Distribution and access to the information should be controlled appropriately to prevent distribution of confidential information that is vital to the cybersecurity of the system.

4.2.7 Organizational performance measurement

Procedures should be developed to measure the performance of the cybersecurity countermeasures against the cybersecurity requirements specification (CSRS). The procedures should consider key performance indicators (KPI), incident investigation, audits, testing, and inspection in order to measure reliability, identify and prevent systematic failures or vulnerabilities, and redress failure and/or demand rates where they exceed acceptable limits.

4.2.8 Human resources

When hiring personnel who will have potential logical or physical access to the IT or IACS networks, it is important to screen prospective applicants to ensure a low likelihood of malicious motive or intent to execute cyber attacks as well as to evaluate that they have sufficient technical skills. Screening should not be a single exercise, as a person may change over time. As such, consideration should be given to periodic background checks.

Whenever a person is no longer associated with the SuC, all means of access should be eliminated immediately.

4.2.9 Supply chain cybersecurity

Any product supplier stating compliance with 61511 should have a functional safety management system that suitably addresses cybersecurity. A product supplier with responsibilities for one or more phases of the safety lifecycle should have a quality management system supported by policies, procedures and countermeasures sufficient to provide the required security level capability specified by the purchaser and ultimately the end user.

4.2.10 Cybersecurity assessments (CSA)

A procedure should be defined and executed for a cybersecurity assessment in such a way that a judgement can be made as to the cybersecurity SL achieved with respect to the IACS, including the SCAI systems. Procedures should include an assessment team with the technical, application and operations expertise appropriate for the particular installation. The CSA should be conducted in conjunction or as a subset of the functional safety assessment (FSA).

The stages in the safety lifecycle at which the CSA activities are to be carried should be identified during the safety planning. Consideration should be given to carrying out CSA activities at the following stages:

- Stage 1 – After the detailed cyber risk assessment has been carried out, the required countermeasures have been identified and the CSRS has been developed. Intent of this assessment is to ensure that the conceptual design is complete and consistent with the intent of the risk assessment prior to detailed design engineering commencing.
- Stage 2 – After the IACS cybersecurity countermeasures have been designed. Intent of this assessment is to ensure that the detailed design engineering is complete and consistent with the intent of the conceptual design prior to issuing contracts for construction.

- Stage 3 – After the installation, pre-commissioning and final validation of the IACS cybersecurity countermeasures have been completed and operation, maintenance, and emergency response procedures have been developed. This should be conducted as part of the pre-startup safety review (PSSR). Intent of this assessment is to ensure the plant is secure and safe to begin operations.
- Stage 4 – After gaining experience in operating and maintenance. Intent is to validate assumptions made and to correct risk assessment as applicable.
- Stage 5 – After modifications and prior to decommissioning. Intent is to ensure robust management of change (MOC).

During the CSA, the team may also need to evaluate any development, production or tools used to develop, support or maintain the systems in order to safeguard against negative impact on the SCAI through the use, or misuse, of these tools.

Periodic or reactive CSA's may be performed throughout the lifecycle. These are used to review existing procedures and performance or to evaluate the impact of a change. These are additional, not replacement, activities which complement the scheduled FSA's embedded in the safety lifecycle plan.

4.2.11 Cybersecurity audits

In order to validate the performance of the cybersecurity management system, an independent, scheduled audit process should be implemented to evaluate compliance and ensure that any identified gaps are reviewed and, where appropriate, rectified.

4.2.12 Cybersecurity configuration and change management

A rigorously controlled configuration management procedure addressing every lifecycle phase should exist for the IACS software, hardware and procedures (and its directly affecting components) that have potential to impact the cyber risk analysis or the cybersecurity countermeasure design. Modifications (not like for like) should be controlled through a management of change procedure that is capable of identifying and managing changes to the IACS (including the SIS and other SCAI systems) and cybersecurity countermeasures.

4.2.13 Physical security

Cybersecurity is a subset of overall security, with its concerns for potential material theft, vandalism and physical attacks. Part of this physical security overlaps with cybersecurity to the extent that it prevents or mitigates the potential for unauthorized access to cyber assets and subsequent malicious manipulation or theft of its data.

The roles and responsibilities of those responsible for physical security and those responsible for cybersecurity should be identified and communicated so that the required security level is not compromised.

4.2.14 Cybersecurity management maturity

ANSI/ISA-62443-1-1 introduced the concept of maturity models relative to the lifecycle and its respective activities as well as to service providers, using information from Capability Maturity Model Integration - Services (CMMI-SVC). Companies should strive to achieve and maintain the maturity level that is most appropriate for the specific situation. The actual maturity level for a company today will depend upon how well they have addressed cybersecurity within their organization (see Table 3). Companies who have just recently identified cybersecurity as a concern can expect to initially be at a lower level.

Table 3 – Maturity levels

Level	Level description	Level attributes
1	Initial	Activities typically performed in an ad-hoc and often undocumented (or not fully documented) manner. Requirements for the activity are typically specified in a statement of work under contract with the asset owner. As a result, consistency throughout the lifecycle and within projects may not be able to be shown.
2	Managed	At this level, the organization has the capability to manage the delivery and performance of applicable lifecycle activities according to written policies (including objectives). The organization also has evidence to show that personnel have the expertise, are trained, and/or are capable of following written procedures to perform the activity. The organization's discipline reflected by Maturity Level 2 helps to ensure that practices are repeatable, even during times of stress. When these practices are in place, their execution will be performed and managed according to their documented plans.
3	Defined (Practiced)	The performance of a Level 3 organization can be shown to be repeatable across the organization as well as being inclusive of its service providers. Level 3 activities may be tailored for individual projects based upon the contract and statement of work.
4	Improving	Using suitable process metrics, organization controls the effectiveness and performance of the lifecycle activities.
5	Optimizing	Demonstrate continuous improvement in the effectiveness and performance of lifecycle activities as well as security level effectiveness.

5 Cyber risk assessment phase

5.1 Overview

Figure 3 shows a typical work process flow that integrates the assessment phases of the safety and cybersecurity lifecycles. As part of any new project involving process industry hazards, a scope, detailing what is to be included within the project should be formulated. This should also address cybersecurity and its relation to the IACS, such as what regulations and standards are to apply.

A requirement in ISA-62443-3-2 ^[13] is to perform a high level cyber risk assessment. Its purpose is to help finalize the scope for the project.

In preparation for a high level cyber risk assessment, it is necessary to identify the system under consideration (SuC). As part of this, initial system architecture drawings should be prepared based upon corporate policies and standards. A complete inventory of cyber assets that is intended to comprise the scope of the project also should be developed and documented.

Results from the high level cyber risk assessment should be used to modify initial architectural drawings / zone and conduit drawings if necessary, once a better understanding of high level risk is available. It is also important at this stage to consider and provide an initial definition of the countermeasures to be implemented based upon known potential vulnerabilities. The zone and conduit drawings and planned countermeasures provide needed information in order to conduct the detailed cyber risk assessment required by ISA-62443-3-2 ^[13] that follows the traditional process hazard analysis (PHA).

The traditional process hazard review, utilizing HAZID, HAZOP, LOPA or other applicable methodologies, should be performed prior to the detailed level cyber risk review. This sequence allows the traditional review to identify and analyze the major process hazards that should be considered when conducting the detailed level cyber risk assessment.

Any major cyber risks identified may need a more rigorous evaluation. This can involve traditional quantitative consequence analysis techniques and possibly quantitative cyber threat analysis as part of the likelihood analysis when determining risk in order to determine if the tolerable risk criteria can be achieved. If the risk criterion is not met, then additional measures should be considered until the risk criterion is met.

Once the risk criterion is determined to be achievable, a CSRS is documented in a similar manner to the safety requirements specification (SRS) for SIS so detailed design can begin. Following development of the CSRS, a stage 1 CSA can be performed as part of the FSA that is recommended in IEC-61511.

Clause 6 addresses the high level and detailed level cyber risk assessments. Clause 7 addresses the determination of security level targets (SL-T) for the zones and cyber assets. Clause 8 addresses the CSRS.

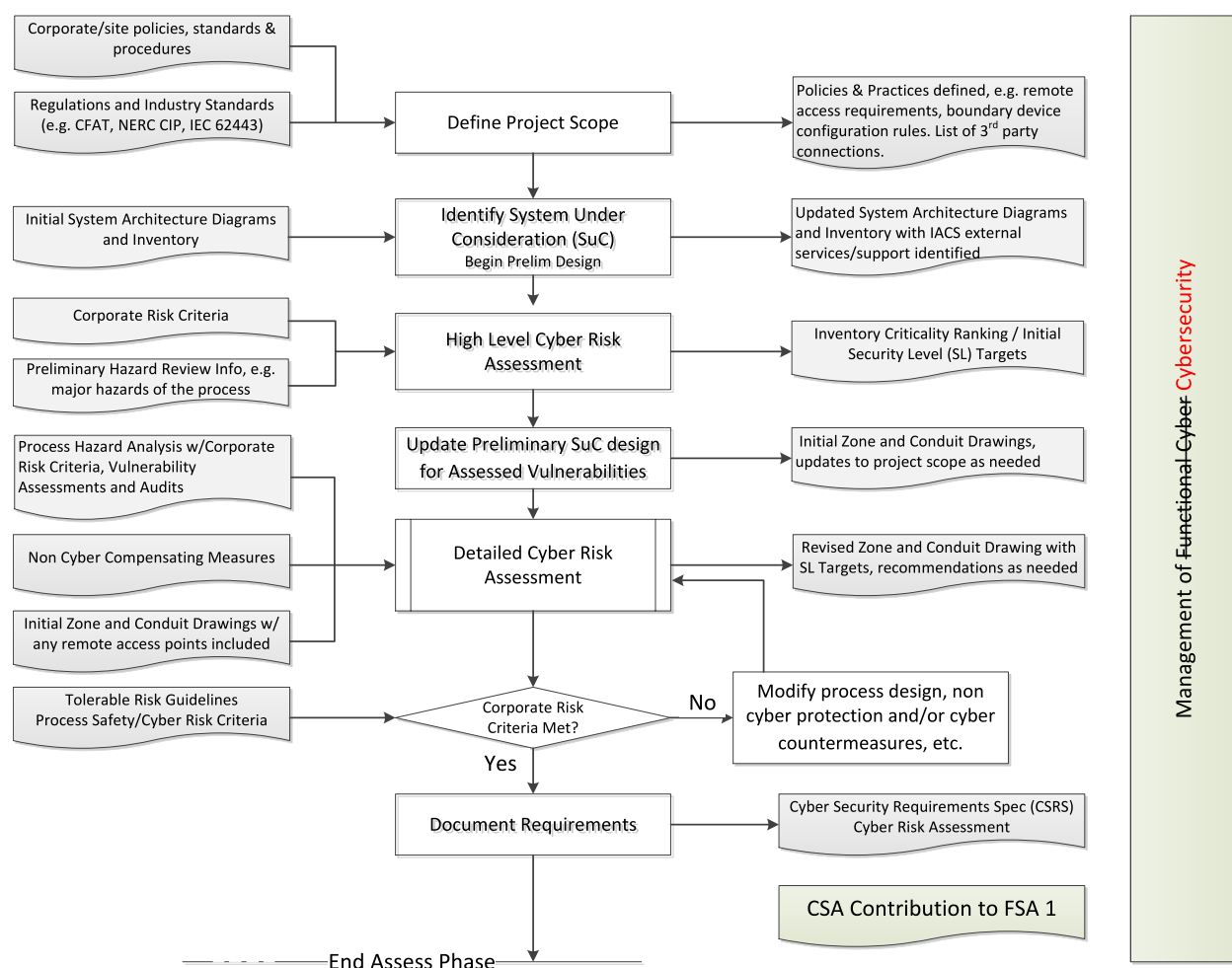


Figure 3–Cybersecurity lifecycle assessment phase ^[16]

6 Hazard and risk analysis

From a process safety perspective in the process industry, there are added concerns beyond data confidentiality and degraded performance that much of the overall industries focus on. When SCAI is involved, there are two overriding concerns that set these systems and functions apart when considering security measures:

- Safety function failure to perform when needed. This concern is exacerbated as a cyber attack poses as a potential common mode that may produce the demand and cause the safety function failing to respond. This can directly relate to the functional safety requirement specification (SRS) requirement to identify dangerous combinations of output states the SIS needs to avoid and to the requirement to assess all protection layers for the impact of common cause failures with other protection layers and with the initiating source of the hazard. As a result, when considering cybersecurity, the cyber risk analysis should be extended to the overall IACS.
- Spurious operation. In this case, the potential goes beyond simply causing a safety function to spuriously operate. As a cyber attack is more likely to affect multiple safety functions, the potential business interruption and equipment damage may be much more significant.

When performing the hazard and risk analysis, the methodology should facilitate not only the identification of potential hazards and vulnerabilities, but also should provide the ability to make practical recommendations for implementation as well as decisions.

The cybersecurity threat landscape is continually changing, but there are some general classifications of potential threat agents or sources that an organization should consider, as each of these could be a cause of cyber incidents.

- Malicious attacker— an individual or group whose objective is to penetrate without authorization the cybersecurity defenses of a third party computer system or network. [ISO/IEC-27002] (attacker may be funded by a large organization or a government).
- Malicious insider—an individual (employee or contractor) who has authorized access to systems and may be inclined to do harm resulting from their state of mind with regards to the organization.
- Well-meaning insider – an individual (employee or contractor) who has authorized access to systems and who, during the course of their work, circumvents cybersecurity countermeasures in order to “get the job done” and / or inadvertently initiates a cyber event.
- Third-party contractor – an individual or organization that may have privileged access to the process control system, SCAI system, and/or other control-related systems through an agreement in order to operate or maintain those systems.

These potential threat agents may exploit vulnerabilities that result in consequences. As with the list of potential threat agents or sources, the potential vulnerabilities can be quite extensive. A few examples of vulnerabilities are included below:

- Software bugs – errors introduced, either intentionally or unintentionally, while programming the software and/or firmware on devices that allow a threat source to circumvent cybersecurity countermeasures.
- Hardware failures – failure of devices, for any reason, that results in the potential compromise of a system and/or circumvention of cybersecurity countermeasures.
- Cybersecurity countermeasure degradation – cybersecurity countermeasures whose effectiveness degrades over time and are able to be circumvented due to new cybersecurity techniques, additional computing performance, and the like, such as encryption techniques that are broken or using short passwords (re: ANSI/ISA-62443-1-1 definition of password strength).

- Credential reuse – using the same set of credentials at multiple locations allows a threat source to potentially compromise multiple systems.
- Confidential information release – releasing confidential information to a potential threat source, whether intentionally or unintentionally, that allows the threat source to circumvent cybersecurity countermeasures. These vulnerabilities could be in both technical and countermeasures specified by cybersecurity policies, such as by not securing credential databases, sending passwords in clear text across a network, or targeted social engineering of employees.
- Systematic errors leading to misconfiguration (for example, failure to change default passwords).
- “General Viruses” that are not created to target a particular host, but they may cause hazards after penetrating into the plant network.
- “Unintentional Deactivation of a Cybersecurity Countermeasure” where a cybersecurity countermeasure is bypassed as an indirect result of an action that is taken for a different purpose.

EXAMPLE Systematic errors in the design of the system, causing failure of a cybersecurity measure while working on another cybersecurity mechanism.

- “Designed Security Bombs” that might be implanted in the system during the design phase to cause damages at later stages during plant operation.

The other aspect when conducting a cyber risk assessment that should be considered are threat vectors that represent the pathways that various threat agents may use to exploit vulnerabilities that exist for the system under consideration (SuC). Additionally, common inadvertent actions that result in degradation of the cybersecurity of the network, although non-malicious, should also be considered. Some examples include:

- A well-meaning insider unwittingly introduces malware via a USB port using a flash drive that had been compromised when using it on their personal computer connected to the internet.
- A vendor or employee adding an unauthorized wireless access point because wireless was not available.
- Attaching an unauthorized laptop to the process control network (PCN) to do work.
- Plugging in a cable that (bypasses the firewall) connects the PCN to the internet.
- Plugging both ends of a cable into the same switch or two switches which already are connected to the network thereby causing broadcast data (storm) to be fed directly back into the network.
- Defective network interface card (NIC) card causing chatter.
- Equipment plugged in with duplicate IP Address creating IP Address conflict.
- Lab or test environment connected creating duplicate IPs, loops, duplicate HMI connections etc.
- Modbus, Ethernet/IP, DNP3, and most other protocols having false master send commands or data to slaves.
- Malware collects system data to be utilized later during an active attack.
- Unauthorized/Inadvertent switch/router/firewall change allows unauthorized, or blocks necessary, traffic.
- Multi-homed computer gets compromised propagating malware or inadvertent routing across NICs.

- Cross-connection of separate segments or zones or redundant network limbs.
- Cross-connection of IACS networks with business (IT), telecomm or other service networks.

To address the additional contributions to risk posed by potential cybersecurity incidents, the ANSI/ISA-62443 series of standards requires cyber risk assessments to be conducted. They include a high level cyber risk assessment and a detailed level cyber risk assessment.

The high level risk assessment can usually be performed at a corporate level to determine in general what high level risks exist for their various processes. A high level risk review can be completed using brain storming sessions or a more methodical criticality assessment. These type of risk assessments are particularly important for new process technology or when no past cyber risk assessments have been performed. For plants using processes that have been previously reviewed using a high level risk assessment methodology, a quick checklist approach to determine if any significant changes exist in the new project scope is a more appropriate means to conduct this review. If significant changes are found to exist in the new project scope, then a more rigorous review of those changes and their potential impact would be appropriate.

The more detailed cyber risk assessment should contain aspects of both safety and cybersecurity and reflect the possible consequences of a failure to provide adequate cybersecurity countermeasures as well as non-cyber layers of protection where appropriate for a given facility with a specific design. The major hazards identified during a traditional process hazard analysis should be considered during the cyber risk assessment. As part of this consideration, some scenarios may have safeguards that are not prone to cyber attack, e.g., hard wired safety instrumented functions, check valves, relief devices, etc. This level of understanding can assist criticality ranking and prioritization of potential recommendations when conducting a detailed level cyber risk assessment.

Safety risk assessments are, in general, much more quantitative in nature than those currently performed for cybersecurity due to the different potential threat sources and relative maturity of the current analysis techniques. Based upon industry cyber incidents, it should be possible to create histograms that allow a relative estimate of probabilities for different types of cyber attack. For instance, it would be expected to see external attacks involving non-targeted malware or viruses on essentially a continuous basis that would be considered high demand while a targeted malware attack would be more likely to be seen as a low demand mode attack. This type of information is necessary in order to estimate risk during a cyber risk assessment, even if it is only semi-quantitative for the present.

Just as a process hazard analysis requires process safety information, equivalent base line information is necessary to conduct a detailed level cyber risk assessment. This information includes but is not necessarily limited to:

- Zone and conduit drawings
- Cybersecurity policies currently in place
- Cyber related standards and procedures currently in place
- Corporate risk criteria that can be related to cyber induced consequences
- Inventory of cyber assets
- Manufacturer cybersecurity manuals
- Service provider cybersecurity capabilities
- List of third party connections
- Vulnerability assessment information that may exist and defined countermeasures to be implemented

Just as there are multiple PHA methodologies, there is no single means to conduct a cyber risk assessment. Example(s) are provided in Annex B.

7 Allocation of Security Levels (SL)

During the high level cyber risk assessment, a first pass may be taken to define security level targets (SL-T) for cyber assets or cyber asset categories. See Annex B for an example(s) methodology.

The specified SL for the cyber assets to support the zone security level should be confirmed and/or modified as needed during the detailed level cyber risk assessment. The sophistication of the attack and its associated likelihood are greatly impacted by the specific threat agent and their motivation at any given point in time. The potential worst case consequences are fixed once the process (e.g., chemical, means of electrical generation, etc.) is fixed heading into design. The SL target should be determined as a function of risk, which in turn is a function of the potential consequences and their likelihood.

Risk criteria for cyber incidents in the process industry should be aligned with risk criteria for process safety, business interruption/financial loss, and environmental harm. When allocating security levels, they should be such that reduction against worst case risk is afforded. This generally includes consideration of worst case consequences. Once worst case risk reduction requirements are established, as long as it is shown that recognized and generally accepted good engineering practices (RAGAGEP) have been employed, it is generally not necessary to further consider lesser risk events with respect to security level allocation and verification, unlike more traditional safety hazard analysis.

It should be recognized that cybersecurity is necessary for the reliable function of the process control and SCAI systems, however the reverse may not be true. ^[17] SL-T are assigned to zones and conduits that potentially encompass multiple logic solvers and other associated equipment such as fire walls, engineering work stations, HMI, etc. This situation allows a targeted malware attack to potentially cause a demand from instrumented controller(s), while preventing the function of the alarm layer of protection as well as the SIS as part of a single attack. A lesser effort could simply attack one of the three aforementioned layers, however, countermeasures that protect against all three should provide risk reduction against this case as well. In contrast, safety integrity levels (SIL) are assigned to specific safety instrumented functions. This is a significant contrast in granularity between functional safety and cybersecurity. Security levels in effect are intended to protect against the cumulative risks associated with the zone being compromised, while a SIF is intended to protect against a specific hazard.

When demarcating zone security levels, it is important to take into consideration interdependency between the zones to implement functional safety. Very often zones are demarcated on the basis of hardware and software components within the zone without consideration of the safety functionality. For example, consider a hydraulic valve that is closed on high pressure as part of a SIF. The close signal for the hydraulic valve is connected to the SIS logic solver, while the hydraulic system is controlled by a process control logic solver. This is an example of an energize-to-trip SIF, where utilities should be available in order to take the valve to closed position, i.e., safe state in response to a SIF demand. When zone security levels are being demarcated, a typical approach would be to place the SIS in a zone with a higher target security level than the process control logic solver controlling the hydraulic system as shown on the left side in Figure 4. However from a safety risk perspective, it would be sensible to include both the SIS and the process control logic solver for the hydraulic system in the same zone and thereby the same target security level as shown on the right side in Figure 4. An alternative would be to keep them in separate zones, but implement the same security level.

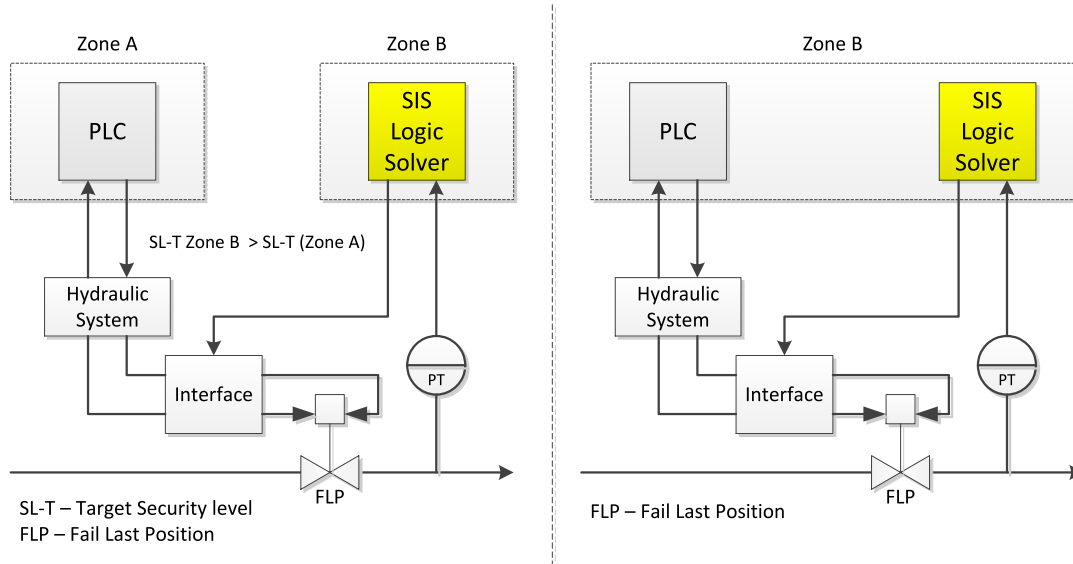


Figure 4—Examples of zone security level demarcation

The likelihood part of risk is dependent on the threats and vulnerabilities. In the event different threat vectors and associated vulnerabilities are evaluated separately from a risk perspective, it is possible to define different security levels for each threat vector. The security level for each class of threat vector should be selected based upon the worst case risk identified among the threat vectors within that class. In such a case, it is possible to have more finely defined security level requirements within a zone or conduit that results in greater or lesser need for each of the seven foundational requirements described and defined in ANSI/ISA-62443-3-3 as they relate to the different security levels.

8 Cybersecurity Requirements Specification (CSRS) for the IACS

A cybersecurity requirements specification (CSRS) should be developed as a separate document or as part of the SRS with a section dedicated to cybersecurity countermeasure requirements. The intention is to document what is required to achieve and maintain the necessary security level(s) while not adversely impacting necessary IACS functions. Selection of the cybersecurity countermeasures should take into account the ability to support interoperability of different manufacturers' devices without degrading the achieved risk reduction, the reliability (spurious trip rate), or the communication speed of the SCAL. In some cases, the CSRS is necessary to support a competitive bid.

The CSRS should address the following as a minimum:

- A high-level description and depiction of the SuC should include as a minimum:
 - name;
 - high-level description of the function and the intended usage of the SuC;
 - description of the equipment or process under control;
 - illustration of the SuC and associated data and process flows.
- Plant/Facility zone and conduit drawings.
- Description of all general cybersecurity countermeasures required for all zones and conduits.
- Description of target cybersecurity level for each zone and conduit having a potential impact on the IACS.

- List of third parties with external interfaces and type of connection for each:
 - Modbus;
 - Profibus;
 - OPC;
 - IEC-61850;
 - DNP3;
 - Wireless (ISA-100, WiHART, 802.11);
 - Other vendor system-specific protocols.
- Description of all cybersecurity countermeasures required for each documented third party interface.
- Requirement that the cybersecurity countermeasures should not impact the performance of the SCAI system.
- If the cybersecurity countermeasure(s) has the potential to impact the overall response time of the safety functions, then the response time impact of the cybersecurity countermeasure should be incorporated in the evaluation of the overall response time of the safety functions (for example, the time from process deviation detection through the process response to final element action).
- Definition of the safe state of the process for each identified countermeasure.
- Target security level to be achieved for each zone.
- Security level (SL) risk reduction expected to be achieved by each countermeasure as a function of threat vector.
- Requirement for cybersecurity testing, e.g.:
 - penetration testing;
 - vulnerability assessments;
 - white hat.
- Cybersecurity countermeasure inspection and test frequencies.
- Response time requirement for each countermeasure to bring the process to a safe state.
- Requirements for manual action as part of countermeasure, for example, physical isolation of the control network from enterprise network/DMZs, etc.
- Disaster recovery requirements for restoring full functionality following actuation of a countermeasure.
- Remote access requirements, e.g., safeguards for remote access.
- Description of system hardening measures to be implemented.
- Management support requirements for countermeasures.
- User access control strategy to be implemented for IACS, including SCAI systems.
- Physical access restriction requirements.
- Required virus prevention and detection measures to be employed on the control network, as well as frequency of scans.
- Patching strategy and requirements to be implemented where relevant to the IACS, including SCAI systems.
- Upgrade strategy to address emerging and future potential threats as they become known.
- Frequency of detailed cyber risk assessment revalidation.

- Required network communications uptime (at all levels) with required need for high reliability of network devices. Network specification should consider frequency of network upgrades.

9 Cybersecurity design and implement phase

9.1 Overview

Figure 5 shows the various activities during the design and implement phase. Once the CSRS is provided, an iterative design process between network, IACS, and process safety personnel should take place to ensure that the planned layers of cybersecurity countermeasures, including policies, procedures equipment, software capabilities, and level of rigor are appropriate for the cybersecurity performance expectations.

The zone and conduit drawings coupled with the specification of cyber assets and the CSRS comprise the conceptual design. The security levels recommended during the detailed cyber risk assessment should be verified. Should the risk criteria not be met, alternate means of risk reduction may need to be considered. Once security level verification has been completed and it is determined that a tolerable risk level can be achieved with the proposed design, detailed design can begin. In parallel with the detailed design, the procedures to test and validate the cybersecurity countermeasures should be developed. Following completion of design, a stage 2 CSA can be performed as part of the FSA that is recommended in IEC 61511.

The test procedures should support the cyber portions of the factory acceptance test (CFAT) and the site acceptance test (CSAT), as well as the initial validation of the cybersecurity countermeasures. This work parallels and should be conducted as part of the SCAI verification and validation.

Following the CFAT, the IACS is delivered, installed and the commissioning begins. Once all devices in the SuC have been installed, connected, and configured, a CSAT may be performed. An initial validation of the cyber countermeasures should be conducted, just as an initial validation of the SCAI is conducted.

Concluding this phase of the lifecycle is the pre-startup safety review (PSSR) that checks to make sure the system is ready and capable of performing as it was defined and that all of the recommendations made during the detailed level risk assessment have been appropriately addressed. Ensuring that the cybersecurity countermeasures are in place and have been tested and ready to go is part of the overall PSSR. The cybersecurity contribution to the PSSR would be considered the stage 3 CSA and should be performed as part of the FSA that is required in process safety management industry standards as well as IEC 61511.

Clause 10 covers the countermeasure design and engineering, security level verification, and activities up to and including the CFAT. In the event cybersecurity countermeasures alone cannot achieve the necessary risk reduction, other means of risk reduction are also addressed in Clause 10. Clause 11 covers installation and commissioning, the CSAT and the initial validation. The PSSR is addressed in Clause 12.

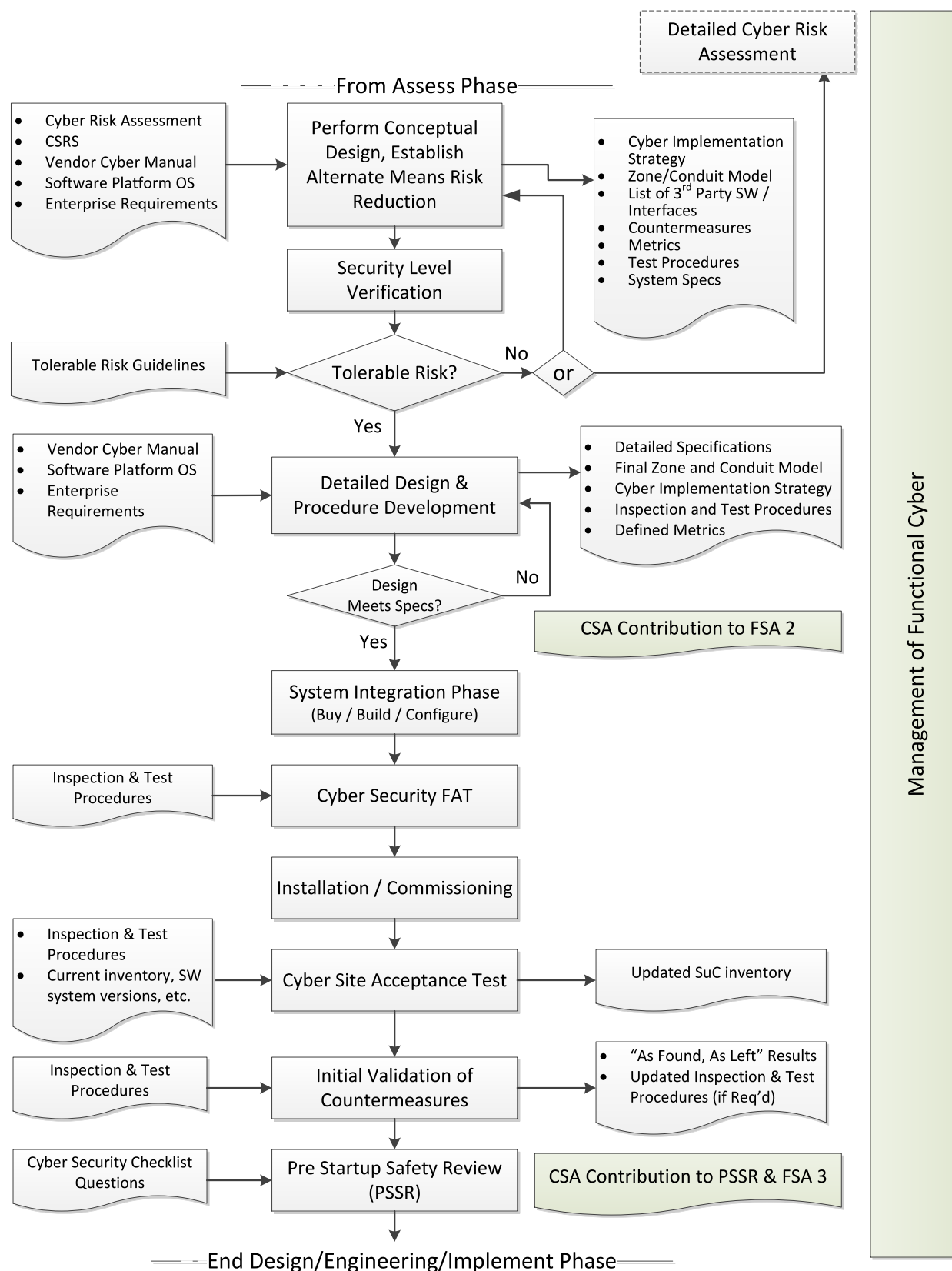


Figure 5–Cybersecurity lifecycle design and implement phase ^[16]