

TABLE OF CONTENTS

1.	SCOPE.....	3
1.1	Purpose.....	3
1.2	Application.....	3
2.	REFERENCES.....	3
2.1	Applicable Documents	3
2.1.1	SAE Publications.....	3
2.1.2	ISO/IEC/IEEE Publications	3
2.1.3	NIST Publications.....	3
2.1.4	U.S. Government Publications.....	4
2.2	Related Publications	4
2.3	Acronyms	5
2.4	Terms and Definitions	6
3.	REQUIREMENTS	13
3.1	Domains of Consideration.....	13
3.2	CPSS Life Cycle Management Processes.....	17
3.2.1	Planning Process	17
3.2.2	Enabling-Processes	18
3.2.3	Supporting Processes	19
3.3	CPSS System and Software Engineering Technical Processes Overlay.....	20
3.3.1	Business or Mission Analysis Process.....	21
3.3.2	Stakeholder Needs and Requirements Definition Process.....	23
3.3.3	System Requirements Definition Process.....	24
3.3.4	Architecture Definition Process.....	26
3.3.5	Design Definition Process	28
3.3.6	System Analysis Process.....	30
3.3.7	Implementation Process.....	30
3.3.8	Integration Process	33
3.3.9	Verification Process	34
3.3.10	Transition Process	34
3.3.11	Validation Process	35
3.3.12	Operations Process.....	36
3.3.13	Maintenance Process.....	37
3.3.14	Disposal Process	38
3.4	Triggering Events	38
3.4.1	Document CPSS Risk Assessment	39
3.5	Reporting Requirements	39
3.5.1	Incident and Exploitation Disclosures	39
3.5.2	Vulnerability Disclosure.....	39
3.5.3	Supplier and Integrator Disclosures.....	40
4.	NOTES	40
4.1	Revision Indicator.....	40
APPENDIX A	STANDARDS THAT ADDRESS DOMAINS OF CONSIDERATION.....	41
APPENDIX B	TRIGGERING EVENTS DESCRIPTION	49
APPENDIX C	RISK MANAGEMENT GUIDANCE.....	52
Figure 1	Example security environment context	7
Figure 2	Non-repudiation and associated terms	13
Figure 3	Overlay loop processes.....	21

1. SCOPE

1.1 Purpose

This SAE Standard establishes practices to:

- a. Manage risk and ensure security of a cyber-physical system (CPS) throughout its life cycle by utilizing systems engineering principles;
- b. Assess the impact of cyber-physical systems security (CPSS) objectives and requirements;
- c. Assess the security risks to CPS technical effectiveness and functions, and address weaknesses and vulnerabilities;
- d. Address various domains of consideration (see [3.1](#)) that take into account operating conditions of the system, command and control, configuration management (refer to SAE EIA649), etc., that could negatively impact CPSS or CPS-designed purpose;
- e. Perform design validation and verification to assess security and risk of the CPS.

1.2 Application

This standard is recommended for use by all contracting officers and system security engineers, and designated subject matter experts for organizations that design or procure CPS. This standard also applies to third parties who support or provide a logical (digital-electronic) interface, system, or service to CPS. The requirements of this standard are to be applied/coordinated by all organizations that design or procure CPS, regardless of type, size, or product provided. This standard is intended to complement other existing standards used in various sectors of industry. The requirements are applicable to any sector needing CPSS to address the pervasive threat.

2. REFERENCES

2.1 Applicable Documents

The following publications form a part of this document to the extent specified herein. The latest issue of SAE publications shall apply. The applicable issue of other publications shall be the issue in effect on the date of the purchase order. In the event of conflict between the text of this document and references cited herein, the text of this document takes precedence. Nothing in this document, however, supersedes applicable laws and regulations unless a specific exemption has been obtained.

2.1.1 SAE Publications

Available from SAE International, 400 Commonwealth Drive, Warrendale, PA 15096-0001, Tel: 877-606-7323 (inside USA and Canada) or +1 724-776-4970 (outside USA), www.sae.org.

SAE EIA649 Configuration Management Standard

ISO/SAE 21434 Road Vehicles - Cybersecurity Engineering

2.1.2 ISO/IEC/IEEE Publications

Copies of these documents are available online at <http://webstore.ansi.org/>, www.iec.ch, or www.ieee.org.

ISO/IEC/IEEE 15288 Systems and Software Engineering - System Life Cycle Processes

2.1.3 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

NIST SP-800-160 Vol. 1 Systems Security Engineering: Considerations for a Multidisciplinary Approach to the Engineering of Trustworthy Secure System

2.1.4 U.S. Government Publications

Copies of these documents are available online at <https://quicksearch.dla.mil>.

MIL-STD-882 Department of Defense Standard Practice: System Safety

2.2 Related Publications

The following publications are provided for information purposes only and are not a required part of this SAE Technical Report.

2.2.1 ANSI Accredited/NEMA Publications

Copies of these documents are available online at <http://webstore.ansi.org/>. Also available from National Electrical Manufacturers Association, 1300 North 17th Street, Suite 900, Arlington, VA 22209, Tel: 703-841-3200, www.nema.org.

ANSI/NEMA HN 1-2019 Manufacturer Disclosure Statement for Medical Device Security

2.2.2 IPC - Association Connecting Electronics Industries Publications

Available from IPC, 3000 Lakeside Drive, 309 S, Bannockburn, IL 60015, Tel: 847-615-7100, www.ipc.org.

IPC-2551 International Standard for Digital Twins

2.2.3 ISO/IEC Publications

Copies of these documents are also available online at <http://webstore.ansi.org/>. Also available from IEC Central Office, 3, rue de Varembe, P.O. Box 131, CH-1211 Geneva 20, Switzerland, Tel: +41 22 919 02 11, www.iec.ch.

ISO/IEC 62443 Suite of Standards - Cybersecurity Certificate Programs

ISO/IEC 27036 Suite of Standards - Information Technology - Security Techniques - Information Security for Supplier Relationships

ISO/IEC 15408-1 Information Technology - Security Techniques - Evaluation Criteria for IT Security - Part 1: Introductions and General Model

2.2.4 ISO Publications

Copies of these documents are available online at <http://webstore.ansi.org/>.

ISO 23247 Digital Twin Manufacturing Framework

ISO 27035 Information Technology - Security Techniques - Information Security Incident Management

ISO 29147 Information Technology - Security Techniques - Vulnerability Disclosure

2.2.5 NIST Publications

Available from NIST, 100 Bureau Drive, Stop 1070, Gaithersburg, MD 20899-1070, Tel: 301-975-6478, www.nist.gov.

Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1

NIST 800-61 Guidance Rev 2 Computer Security Incident Handling Guide

NIST SP-800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST SP-800-37 Rev. 2 Risk Management Framework for Information Systems and Organizations
Approach for Security and Privacy

NIST SP-800-53 Rev. 4	Security and Privacy Controls for Federal Information Systems and Organizations
NIST SP-800-82 Rev. 2	Guide to Industrial Control Systems (ICS) Security
NIST SP-800-160 Vol. 2	Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
NIST SP-800-171 Rev. 2	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
NIST SP-1500-201	Framework for Cyber-Physical Systems: Volume 1, Overview
NIST SP-1900-202	Cyber-Physical Systems and Internet of Things

2.2.6 Other Publications

Auto-ISAC Best Practice Guides on Incident Response

FIRST's Product Security Incident Response Team (PSIRT) Services Framework

2.3 Acronyms

ANSI	American National Standards Institute
BOM	Bill of materials
CISA	Cybersecurity and Infrastructure Security Agency
C-SCRM	Cyber-supply chain risk management
CPS	Cyber-physical system
CPSS	Cyber-physical system security
CPSSEP	Cyber-physical system security engineering plan
CVSS	Common vulnerability scoring system
CWSS	Common weakness scoring system
DMSMS	Diminishing manufacturing sources and material shortages
FIRST	Forum of Incident Response and Security Teams
HwA	Hardware assurance
IC	Integrated circuit
ICS	Industrial control system
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronic Engineers
IPC	Institute for Printed Circuits
ISA	International Society of Automation
ISAC	Information Sharing and Analysis Center
ISO	International Organization for Standardization

IT	Information technology
MIL-STD	Military standard
NEMA	National Electrical Manufacturers Association
NIST	National Institute Standards and Technology
OEM	Original equipment manufacturer
OT	Operational technology
SoS	System of systems
SwA	Software assurance

2.4 Terms and Definitions

ACCEPTABLE MEANS OF COMPLIANCE: Non-binding standards adopted by the certification authority to illustrate means to establish compliance with the basic regulation and its implementing rules.

ACCESS CONTROL: A domain of consideration encompassing the restrictions of resource access to only authorized entities.

ANTI-MALICIOUS: A domain of consideration encompassing protections against the intentional creation or insertion of an exploit that could have a negative impact on a CPS.

ANTI-TAMPER: A domain of consideration encompassing systems engineering activities intended to deter, detect, and/or delay exploitation of critical technologies in a system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

ARTIFACT: A piece of evidence, such as text or a reference to a resource, that is submitted to support a response to a question.

ASSET MANAGEMENT: A domain of consideration encompassing a systematic and measurable approach and associated tools to managing the CPSS risks associated with CPS physical, functional, or logical [assets](#) and their associated intellectual property.

ASSURANCE: Grounds for justified confidence that a claim has been or will be achieved.

NOTE 1: Assurance is typically obtained relative to a set of specific claims. The scope and focus of such claims may vary (e.g., security claims, safety claims) and the claims themselves may be interrelated.

NOTE 2: Assurance is obtained through techniques and methods that generate credible evidence to substantiate claims. For further guidance on assurance, refer to the ISO/IEC 15026 document series.

ASSURANCE CASE: A reasoned, auditable artifact created that supports the contention that its top-level claim (or set of claims) is satisfied, including systematic argumentation and its underlying evidence and explicit assumptions that support the claim(s).

AUTHORITY HAVING JURISDICTION: The governmental organization having statutory authority to respond to, enforce, or prosecute laws.

CERTIFICATION: The recognition that a product, service, organization, or person complies with the applicable requirements. Such certification comprises the activity of technically checking the product, service, organization, or person, and the formal recognition of compliance with the applicable requirements by issue of a certificate, license, approval, or laws, regulations, and procedures.

CERTIFICATION AUTHORITY: Organization or person responsible for granting approval in accordance with applicable regulations and/or requirements.

CERTIFICATION BASIS: The applicable criteria and any additional certification authority specific requirements.

COMMAND AND CONTROL (C2): A tactic often used by attackers to retain communications with compromised systems within a target network. (OPTIV, 2021)

NOTE: Attackers then issue commands and controls to compromised systems (as simple as a timed beacon, or as involved as remote control or data mining). It is usually the compromised system/host that initiates communication from inside a network to a command and control server on the public Internet. Establishing a command and control link is often the primary objective of malware (<https://www.optiv.com/cybersecurity-dictionary/c2-command-and-control>)

CONSEQUENCES: The effects of the activity with respect to the values defined (such as human life and health, environment, and economic assets), covering the totality of states, events, barriers, and outcomes. The consequences are often seen in relation to some reference values (planned values, objectives, etc.), and the focus is often on negative, undesirable consequences.

NOTE 1: The consequences should have a value (e.g., red-yellow-green, a numerical value, and so forth) associated with it.

NOTE 2: Consequences are normally associated with a threat.

NOTE 3: Similar terminology includes impact or severity.

COUNTERFEIT ITEM: 1. An unauthorized (a) copy, (b) imitation, (c) substitute, or (d) modified item which is knowingly, recklessly, or negligently misrepresented as a specified genuine item from an authorized manufacturer; or 2. A previously used item which has been knowingly, recklessly, or negligently misrepresented as new without disclosure to the customer.

NOTE: The counterfeit item definition may differ from civil or criminal laws that address the acts of counterfeiting or fraud and is not intended to make a legal determination. Used items sold as new that have not been modified are not counterfeit, according to some civil and criminal statutes.

CPS ASSURANCE LEVEL: The degree of confidence that a CPS meets its associated security claims.

CPS LIFE CYCLE: The period of time from CPS conception through retirement, decommissioning, or disposal.

CPS SECURITY ENVIRONMENT: The security context (e.g., physical, environmental, cyber-environment) in which an asset performs its function. For a CPS, or sub-system of a CPS, the system security environment is characterized by the set of security assumptions and considerations that are used in the assessment of the systems technical effectiveness and functions. These assumptions and considerations will change over the life cycle of the CPS and as triggering events occur within the security environment.

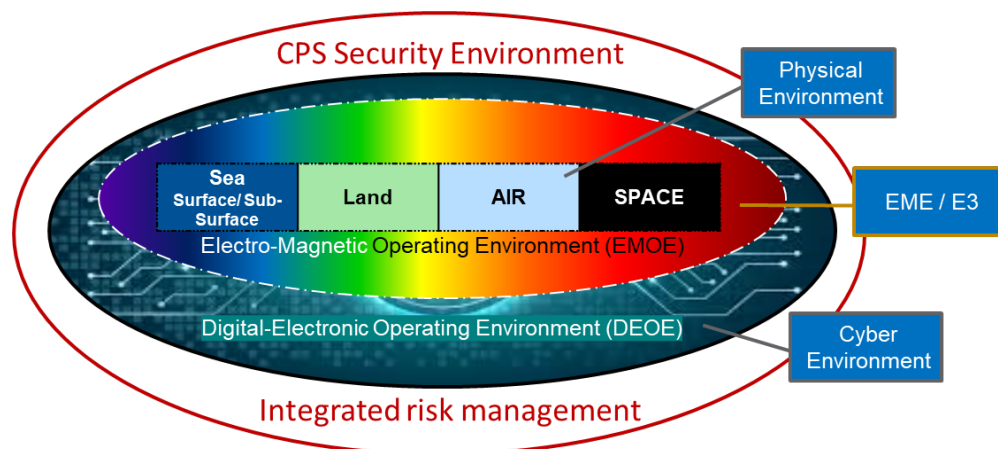


Figure 1 - Example security environment context



Documents

Document Sharing Hub

CPS VULNERABILITY: The characteristics of a CPS and its elements, procedure, control, or implementation that can cause the CPS to be degraded (incapability to perform the designated function or mission) and, if compromised, could cause an undesirable consequence.

NOTE: Considerations in measuring and assessing system vulnerability may include susceptibility (exploitability), accessibility (exposure), and feasibility (practicality).

CPS WEAKNESS: A system limitation, defect or flaw in CPS architecture, design, code, hardware, or process.

NOTE 1: Not all weaknesses are vulnerabilities. A weakness becomes a vulnerability when it can be exploited to cause a negative technical impact..

NOTE 2: Weaknesses represent potential source vectors for zero-day exploits.

CPSS APPLICATION SECURITY: A domain of consideration encompassing the discipline and process of developing, adding, testing, and remediating features within applications to prevent weaknesses and vulnerabilities from being exploited throughout the CPS life cycle.

CPSS ASSURANCE REQUIREMENTS: Specification of the techniques and methods employed in the engineering effort to generate evidence used to verify that the CPS meets its security functional and nonfunctional requirements; to substantiate the trustworthiness of the CPS; and to identify the residual risk of the delivered CPS based on its intended use to support the mission or business.

CPSS COUNTERMEASURES: Protective measures prescribed to meet the security requirements (i.e., availability, integrity, and confidentiality) specified for a CPS. Controls and safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

CPSS ENGINEERING PLAN (CPSSEP): Documentation of a risk-based or risk-informed approach for CPSS that is based on the requirements of this standard.

CPSS NEEDS: Conditions that ensure the CPS's ability to perform its intended functionality in support of the business or mission objective within the expected operating environment.

CPSS OWNERSHIP: Effective establishment of responsible owner's CPSS trustworthiness and pedigree with cryptographic credentialing of software/firmware assets that enable the CPSS overall secure functionality throughout the CPSS life cycle.

NOTE 1: CPSS ownership is assigned to an individual or organization responsible or accountable for CPSS at varying stages of the CPS life cycle.

NOTE 2: Key questions answered to establish ownership throughout the CPSS life cycle are: (1) Who is the initial CPSS responsible party for initial CPSS software/firmware credentialing? (2) How is a CPSS to be initialized with its very first credentials? (3) Once initialized, how is ownership of the CPSS to be transferred to another responsible party?

CPSS PERFORMANCE METRICS: A set of measurable properties that track and assess how well CPSS needs or requirements are met.

CPSS STAKEHOLDERS: Individual(s) or organization(s) having a right, share, claim, or interest in a CPS or in its possession of security characteristics that meet their needs and expectations.

CYBER-PHYSICAL SYSTEM (CPS): A system in which a mechanism is controlled or monitored by computer-based algorithms.

NOTE 1: CPS are defined as technologies that combine the cyber and physical worlds that can respond in real time to their environments. CPS include electronic parts, assemblies, systems, and system elements that operate as a single, self-contained device or within an interconnected network providing shared operations. An added distinction of this CPS definition is a requirement affecting a tangible physical output through command and control embedded in the device or distributed across network nodes. The command and control system could be manipulated through a physical process and/or physical input of the data flow (e.g., manipulating sensor input to spoof or disrupt the expected data).

NOTE 2: Examples of CPS include operational technology (OT) such as wearable medical devices, smart grids, autonomous vehicles (land, sea, air, space), supervisory control and data acquisition (SCADA) systems, industrial control systems (ICS), internet of things (IoT) systems, and satellite communication systems (SATCOM) that include software, firmware, and electronics hardware.

CYBER-PHYSICAL SYSTEM SECURITY (CPSS): Proactive and coordinated efforts needed to provide security and manage risk for CPS.

CYBER-RESILIENCY: The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber-resources. (NIST, 2021)

CYBER-SUPPLY CHAIN RISK MANAGEMENT (C-SCRM): A domain of consideration encompassing the process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of information technology (IT) or OT product and service supply chains. C-SCRM covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction) as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.

DATA AND INFORMATION SECURITY: A domain of consideration encompassing the protection of data and information from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

NOTE: Data Integrity and availability may be critical to ensure CPS safety or mission critical functions. Data security becomes an exploitable vector that requires protection under this standard.

DATA ITEM: Recorded information, regardless of form or method of recording.

DESIGN TRADEOFF ANALYSIS: Analysis that is focused on determining the design approach that is best suited for implementing the elements, physical safeguards, and procedural measures of the system.

NOTE: A design tradeoff analysis includes the following considerations: whether technical elements, physical safeguards, or procedural measures are appropriate to implement the system security requirements; and whether acquiring an off-the-shelf product, accessing, or developing a service or custom development is appropriate to implement the system security requirements.

DOMAIN OF CONSIDERATION: An area to consider, when determining whether and how to manage CPSS risks related to weaknesses and vulnerabilities that could impact the CPS. For each applicable domain of consideration, functional and non-functional requirements should be established to address those CPSS risks that are identified through a risk assessment process.

ELECTRONIC SECURITY: A domain of consideration encompassing CPSS of the physics, engineering, technology, and applications that address the emission, flow, and control that result in an outcome from electronics, including physical and virtual elements. This includes the sum of mechanisms that electronics support and provide to protect one or multiple security properties.

NOTE: Emissions security is an important part of this domain that involves protecting unintentional electromagnetic emissions from interception, exploitation, or attack.

ENABLING ELEMENTS: Aspects of processes and systems (e.g., manufacturing, fabrication, production, simulators, modeling, and digital engineering systems) that are necessary to support the operation of the CPS of interest; examples include supply chain elements, external security, and so forth.

ENABLING PROCESSES: Processes that are key to the achievement of critical goals (security, business, assurance, acceptable risk level, CPS functions, etc.), but do not necessarily translate directly to the production of goods or services.

FIRMWARE: A specific class of software held in non-volatile memory devices or programmable logic on hardware or logical components.

FUNCTIONAL CPSS REQUIREMENT(S): Specification of the protection capability provided by the CPS; the capability for the CPS to protect itself, and the capability for secure management of the CPS.

HARDWARE: The material physical components of a CPS.

NOTE: See also software and firmware for other CPS components.

HARDWARE ASSURANCE (HwA): The processes, practices or methodologies employed to achieve a level of confidence that microelectronics function as intended and are free to an acceptable level of assurance from weaknesses and vulnerabilities, either intentionally or unintentionally designed or inserted, throughout the life cycle.

INDEPENDENCE: Separation of responsibilities that assures the accomplishment of objective evaluation, e.g., validation activities not performed solely by the developer of the requirement of a system or item.

INFORMATION: The contextual (subjective) interpretation of data.

INFORMATION PROTECTION: A domain of consideration encompassing the measures that protect and defend data, information, and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

INFORMATION SHARING AND REPORTING: A domain of consideration encompassing the bi-directional communication and dissemination of information associated with any CPSS concern.

NOTE: Concerns include, but are not limited to, risks, issues, threats, breaches, and triggering events.

ISSUES AND EVENTS MANAGEMENT: A domain of consideration encompassing the identification, assessment, and addressing of CPSS risks associated with weaknesses, vulnerabilities, and threats including forensics, prognostics, and recovery and incident responses.

NOTE: Risk management for addressing issues and events may include building in resilience, graceful degradation of functionality, removing functionality, or deception strategy.

LIFE CYCLE SUPPORT: A domain of consideration encompassing the evolution of a CPS from conception through retirement, decommissioning, or disposal, including processes for addressing relevant weaknesses and vulnerabilities with a CPS.

NON-FUNCTIONAL CPSS REQUIREMENT(S): Specification of the security behavior, performance, strength-of-function, and quality characteristics and attributes of the CPS.

NON-REPUDIATION: The assurance that someone cannot deny the validity of something or refute responsibility.

OBSOLESCENCE: A domain of consideration encompassing the lack of availability of an item or raw material resulting from process, design, or statutory/regulatory changes. It deals with the process or condition by which a piece of equipment becomes no longer useful, or a form and function become no longer current or available for production or repair (adapted from DAU glossary citation).

NOTE: Implementation of new technology causes older technology to become less supportable because of the diminished availability of parts and suppliers. For purposes of this standard, synonymous with DMSS.

ORGANIZATION: Group of people and facilities with an arrangement of responsibilities, authorities, and relationships associated with adoption of this standard.

PEDIGREE: The validation of the composition and provenance of technologies, products, and services. (NIST SP-800-161, 2021)

NOTE: For microelectronics, this includes material composition of components. For software this includes the composition of open source and proprietary code, including the version of the component at a given point in time. Pedigrees increase the assurance that the claims suppliers assert are correct.

PHYSICAL SECURITY: A domain of consideration encompassing the part of security concerned with active and passive measures designed to prevent unauthorized access to physical assets.

PROBABILITY: A measure for representing or expressing uncertainty, variation, or beliefs, following the rules of probability calculus.

NOTE 1: Related terms which can be substituted for probability include likelihood and frequency.

NOTE 2: There may be situations where it is not possible to assign a mathematical value to probability. That does not imply it cannot happen.

NOTE 3: If a quantitative value cannot be computed, a qualitative value should be determined.

PRODUCT: Anything used in or resulting from the execution of a process including the process itself. (SAE EIA649C, 2019).

PRODUCTION: Fabrication, assembly and/or calibration of an item or component.

PROVENANCE: The chronology of the origin, development, ownership, location, and changes to a system or system component and associated data. It may also include personnel and processes used to interact with or make modifications to the system, component, or associated data. (NIST SP-800-161, 2021)

NOTE: In this standard:

- a. Provenance is applied to all life cycle activities from concept through disposal (e.g., development, supply chain).
- b. Provenance information establishes evidence of non-compromise and may include chronology, source, responsibility, licensing, personnel, processes (i.e., development, integration, configuration changes, etc.). A compromise may result in unauthorized alteration, forgery/ reproduction, reverse engineering, theft, etc.
- c. Provenance documents the assurance of origin, authenticity, custody, security and integrity of selected/identified products this includes initial delivery or subsequent configuration changes, and modification through patching and updating.

RESIDUAL RISK: The level of risk after risk mitigation action (e.g., countermeasures, safeguards, controls, preventions, or overrides) are in place.

RISK: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs; and (2) the likelihood of occurrence.

NOTE: There are many ways of measuring risk. Each organization should determine its own risk model.

RISK ASSESSMENT: Product or process that collects information, measures risk to inform priorities, develops or compares courses of action, and informs decision making.

NOTE: "Measures risk" implies documentation of the level of risk, e.g., red-yellow-green, a numerical value, and/or some other method.

RISK MANAGEMENT: Activities to identify, assess, and address risk.

NOTE: Risk management often includes trade-offs between costs and benefits of risk reduction and choice of a level of tolerable risk.

RISK SCENARIOS: Events, situations, narratives, or use cases connecting a potential threat exploiting a weakness or vulnerability to impact a critical function or asset leading to a business/mission loss. Scenarios provide a frame of reference for performing the risk assessment.

NOTE 1: Industry segments may have other terms representing the intent of this definition.

NOTE 2: A risk scenario is the combination of a threat scenario and a damage scenario as defined by ISO/SAE 21434.

NOTE 3: For aviation, “threat scenario” is defined by DO-326A/ED-202A and DO-356A/ED-203—precisely the same as “risk scenario” here.

SECURITY PERIMETER: The notional boundary between an internal security context and the external security environment of the CPS or element under consideration. It marks the change of security control. The internal security context is comprised of the assets contained in the security perimeter and the relevant security measures.

SOFTWARE: The virtual elements of logical sub-systems (e.g., computers) that perform instructions, resulting in outcomes.

SOFTWARE ASSURANCE (SwA): Refers to the justified confidence that software functions as intended and is free of weaknesses and vulnerabilities throughout the product life cycle.

NOTE: Software assurance applies to all virtual elements, including embedded code and programmable logic.

SYSTEM ELEMENT: All hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, and materials or any combination that constitutes everything within a CPS.

SYSTEMS ENGINEERING: Interdisciplinary approach governing the technical and managerial effort required to transform a set of stakeholder needs, expectations, and constraints into a CPS throughout its life cycle.

THREAT: Potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

TRACEABILITY: A domain of consideration encompassing the process for determining the provenance of an item (also referred to as tracking).

TRIGGERING EVENT: An occurrence such as changes in the existing design or interfaces; changes in the risk profile of the system and its external supporting processes or procedures; or planned assessments.

NOTE: The triggering event should result in a risk assessment to identify any changes to the risk profile and the associated impacts of those changes on a CPS.

TRUST: The confidence one element has in another, that the second element will behave as expected. (NIST, 2021)

TRUSTWORTHINESS: Worthy of being trusted to fulfill whatever critical requirements may be needed for a particular component, subsystem, system, network, application, mission, business function, enterprise, or other entity. (NIST, 2021)

NOTE: From a security perspective, a trustworthy system is a system that meets specific security requirements in addition to meeting other critical requirements.

VALIDATION: A systems and software engineering technical process whose CPSS purpose is to produce evidence that the CPS and its associated enablers satisfy CPSS requirements and characteristics at the appropriate level of assurance in the accomplishment of the mission and/or business needs within the intended operational environment.

VERIFICATION: A systems and software engineering technical process whose CPSS purpose is to produce evidence that hardware or software system elements, as well as their enablers, meet CPSS functional, non-functional, and assurance requirements.

3. REQUIREMENTS

The organization shall develop and implement a risk-based cyber-physical systems security engineering plan (CPSSEP) in accordance with the requirements specified in Section 3.

NOTE 1: The CPSSEP may be a documented plan or process required by an industry accepted standard that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE 2: CPSSEP could impact interrelated systems engineering disciplines. The requirements specified in Section 3 may complement other disciplines.

3.1 Domains of Consideration

The domains of consideration represent a set of areas to consider, when determining whether and how to manage CPSS risks related to weaknesses and vulnerabilities that could impact the CPS. For each applicable domain of consideration, functional and non-functional requirements should be established to address CPSS risks, as identified through a risk assessment process as established in risk management framework guidance ([Appendix C](#)).

Related to each priority weakness and vulnerability for the CPS (see [Appendix C](#) for how priorities are applied), there will also be an associated assurance requirement which establishes a level of confidence that the associated functional or non-functional requirements will address the weakness or vulnerability, as desired.

NOTE: A risk assessment provides a means to prioritize mitigations based on CPSS risks that are unacceptable to the stakeholders. An assurance case could be developed that includes top-level claims, and the evidence and explicit assumptions that underlie the argument that the CPSS risks have been mitigated. Provenance, traceability, and pedigree of information and data tied to the physical system(s) and component(s) that substantiate the claims are important to establish non-repudiation to the claims (see [Figure 2](#)). In this manner, non-repudiation can be linked to the domains of consideration and provide a bridge to measurable, evidence-based risk management processes.

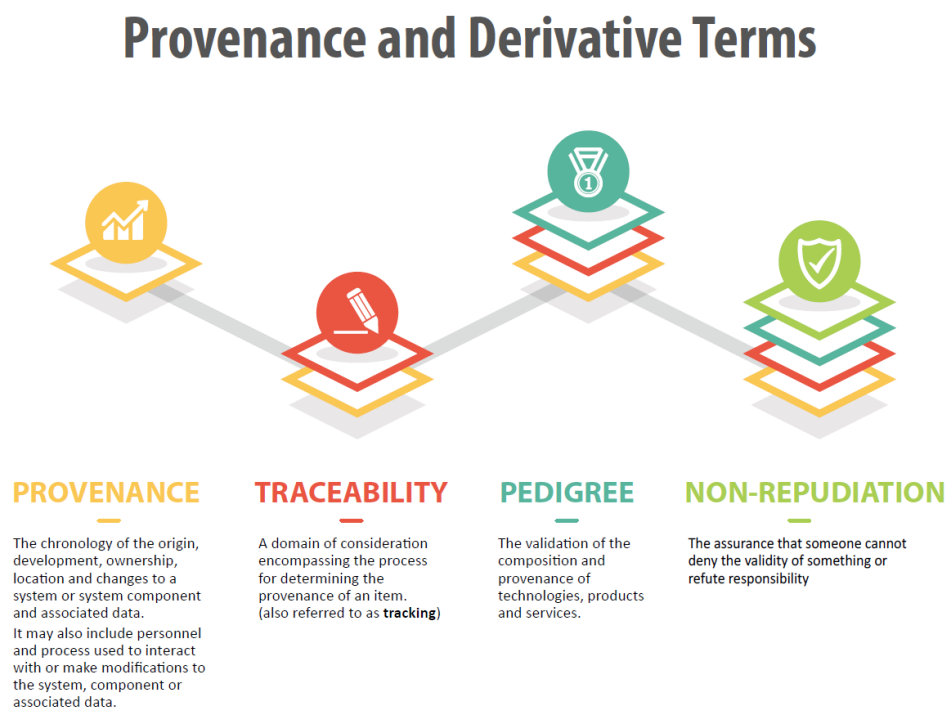


Figure 2 - Non-repudiation and associated terms

The hardware assurance (HwA) and software assurance (SwA) domains of consideration focus on the assurance requirements specific to the components. HwA and SwA include how to verify that the appropriate level of confidence has been demonstrated (i.e., the CPSS risks of the CPS have been identified and addressed, as planned through the implementation of the functional and non-functional requirements associated with the applicable domains of consideration).

NOTE 1: There may be some overlap and hierarchical relationships among the domains of consideration.

NOTE 2: This document does not provide guidance or requirements specific to individual domains of consideration. See [Appendix A](#) for a list of standards associated with them.

The CPSSEP or an equivalent document or process required by an industry accepted standard shall address the following domains of consideration:

- a. Electronic security objectives and associated compliance that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Electronic security (see definition) examples include protection of a CPS resulting from measures designed to prevent unauthorized access of information derived from weaknesses and vulnerabilities such as the interception and analysis of side channels through unintended emanations or power consumption. Examples also include protection against electronic intrusion wherein electronic emanation impacts system operations (this includes intentional and unintentional radiators).

- b. Physical security that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Physical security (see definition) examples include physical access control (including boundaries, installation, etc.) of hardware and software items that compose or support a CPS throughout the product life cycle. It addresses weaknesses and vulnerabilities associated with physical, technical, and administrative controls including system privileges for authorized access. Examples also include measures designed to deny unauthorized access to facilities, equipment, and resources, and to protect personnel and property from intentional or unintentional threats, vulnerabilities, or consequences (e.g., espionage, tampering, theft, or terrorist attacks).

- c. Information protection that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE 1: Information protection (see definition) examples include measures that protect and defend data, information, and information systems associated with a CPS by ensuring that weaknesses and vulnerabilities for exploiting availability, integrity, authentication, confidentiality, and non-repudiation are mitigated. Examples also include protection of information from unauthorized (accidental or intentional) modification, destruction, access, use, disruption, inspection, recording, or disclosure.

NOTE 2: Information protection should include management systems with specific and detailed measures to ensure that secure products and the supporting confidential information is managed appropriately such as specified in ISO 15408, NIST SP 800-171, and/or ISO/IEC 62443.

- d. Data and information security that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Data and information security (see definition) examples include processes and systems to (1) address weaknesses and vulnerabilities that inhibit the availability, integrity, and the confidentiality and authentication of data and information, and (2) manage risks related to the development, testing, production, use, processing, storage, configuration management, integrity, and transmission of data and information associated with a CPS. Mitigation examples include measures to ensure unauthorized changes, corruption, destruction, denial in data and information and its behavior are addressed throughout the life cycle. Protections against data and information security apply to data-at-rest and data-in-transit.

- e. Asset management that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Asset management (see definition) examples include the management of critical assets in the CPS that exhibit potential to introduce weaknesses or vulnerabilities through a functional role in the CPS operating environment where interaction with the CPS is required. It provides systems for an inventory of critical assets maintained by monitored access using verification credentials. Examples also include management of information relevant to the operation of the asset (e.g., software revision, firmware revision) and change/configuration management. This includes consolidating the CPS bill of materials (BOM) of software and hardware components with provenance as driven by risk management and defined through legal agreements.

- f. Access control that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Access control (see definition) examples include enabling authorized use of a resource while preventing unauthorized use or use in an unauthorized manner; the process of granting or denying specific requests such as obtaining and using information and related information processing services.

- g. Life cycle support that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Life cycle support (see definition) includes updating a CPS element to address relevant CPSS weaknesses and vulnerabilities and ensuring suitable hardware and software configuration and functionality (e.g., patches in software and updating firmware or hardware to repair or replace obsolete or unsupportable assets).

- h. Obsolescence, unsupportable, disrupted supply, or unavailable items that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Obsolescence (see definition), unsupportable, disrupted supply or unavailable items examples include the loss, or impending loss, of manufacturers or suppliers of items, raw materials, or software. Some industries refer to this domain as “obsolescence” or diminishing manufacturing sources and material shortages (DMSMS). These items represent a target for weaknesses and vulnerabilities associated with malicious insertions into a CPS. Obsolete, unsupportable, or unavailable items management is a multidisciplinary process to identify issues resulting from obsolescence, loss of manufacturing sources, or material shortages; to assess the potential for negative impacts on schedule and/or readiness; to analyze potential mitigation strategies; and then to implement the most cost-effective strategy. Gray market parts that may no longer be available from the original manufacturer present a much higher risk. Risks include but are not limited to legitimate parts that are not designed for the specific market intended, counterfeit parts or parts that have degraded or malicious functionality, which could result in poor performance/reliability as well as possible malicious function.

- i. Anti-counterfeit measures that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Counterfeit parts and materials may contain degraded or malicious functionality that can result in a departure from the system’s intended design and could enable the disruption of its performance or an unauthorized function. Anti-counterfeit (for counterfeit related definitions, refer to AIR6273) examples include approaches that can be applied to protect a CPS from the weaknesses and vulnerabilities introduced by counterfeit parts and materials. Anti-counterfeit measures may be applied to mitigate the risk that the parts and materials introduced during the design, production, and maintenance of a CPS are not authentic. Anti-counterfeit methods/techniques could also be applied to the design to further prevent proliferation of counterfeit parts in the supply chain.

- j. Cyber-supply chain risk management (C-SCRM) that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: C-SCRM (see definition) examples include identifying, assessing, and addressing the risks associated with the distributed and interconnected nature of product and service supply chains that includes protocols of how the system operates. Suppliers that are not known or trusted present a risk of introducing vulnerabilities and weakness to a CPS. Such suppliers can deliver parts and materials that result in a departure from the system’s intended design and could enable the disruption of its performance or an unauthorized function. C-SCRM covers the entire life cycle of a CPS. It ensures that the provenance and pedigree of parts and materials are maintained and that those parts and materials are obtained from or may be directly linked to original manufacturers.

- k. Application security that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: Application security (see definition) applies to operating systems and firmware as well as control flows down to applications and the underlying system where weaknesses and vulnerabilities are enabled through flaws in design, development, deployment, upgrade, or life cycle support of the application for a CPS. It is not limited to software and includes hardware and firmware. It also includes how the development and operational environment (including, but not limited to IT as it interfaces with the OT) will be protected and how changes in the CPS will be integrated during development and operations.

- l. Issues and events management (e.g., forensics, prognostics, vulnerability management, incident management, and recovery response) or process considerations that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE 1: Forensics, prognostics, vulnerability management, incident management, cyber-resiliency (for example, refer to NIST SP 800-160 volume 2) and recovery plans provide processes and tools for gathering of CPS operations data for use in the examination and analysis of cyber-incidents, thereby characterizing the CPS operational cyber-security baseline. The baseline provides the basis for tools used in forensics (internal to the CPS), prognostics, vulnerability management, incident management, and recovery response plans (including cyber-resiliency). An adjacency provision for external forensics serves the cooperative effort with other industrial organizations and government agencies responsible for pursuing root cause of an attack vector external to the CPS and its operating environment. The forensic strategy and tools for external attacks need to be established and documents written, including the collaboration with other industrial organizations and government agencies.

NOTE 2: When the only ways to address a critical vulnerability affecting safety or mission or business operations are to (1) remove the vulnerability when the product is in the possession of the supplier or an affiliate, or (2) sunset the product and provide appropriate remediation to the customer, then the supplier, in collaboration with the stakeholders, may consider a voluntary product recall or comply with regulation for product recall.

- m. Traceability and tracking that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE 1: Traceability (see definition) examples include the tracking of requirements and their drivers through the entire development and sustainment processes throughout the life cycle.

NOTE 2: Traceability and tracking also provide the internal and network-based process and tools for determining provenance and pedigree of components, the current and past locations, and security controls that identify and prevent the introduction of weaknesses, vulnerabilities, or malicious content to CPS software and hardware. There are both physical and virtual aspects. A virtual example is traceability of all requirements or their provenance and pedigree. A physical example could be the chain of custody to avoid counterfeits.

- n. Anti-malicious considerations that include a process for managing (identifying, assessing, and addressing) the CPSS risks. This includes known functionality that is not disclosed by the supplier that introduces exploitable weaknesses and vulnerabilities throughout the life cycle.

NOTE: If parts and materials are maliciously introduced into a CPS during design, production, or maintenance, weaknesses and vulnerabilities may result that can impact intended functionality of the system. Such malicious insertions could occur as a result of reverse engineering or due to design features that introduce weaknesses and vulnerabilities that are exploitable. Anti-malicious tools and processes enable the integration and assessment of protective technology features in CPS. These tools and processes can mitigate the risk of weaknesses and vulnerabilities introduced through malicious attacks. A non-disclosure of a backdoor could be considered malicious. The backdoor could allow data to be extracted from the system without the user's knowledge.

- o. Anti-tamper that includes a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: If tampered hardware or malware is introduced to a CPS anywhere within the entire life cycle, weaknesses and vulnerabilities may result that can impact intended functionality of the system. Anti-tampering tools and processes enable the integration and assessment of protective technology features in a CPS to minimize the risk of tampering. These tools and processes can mitigate the risk of weaknesses and vulnerabilities introduced through tampering attacks.

- p. Information sharing and reporting that include a process for managing (identifying, assessing, and addressing) the CPSS risks.

NOTE: A framework of information sharing and reporting (see definition) examples include mechanisms for exchange of cyber-attack events (e.g., tools and shared database resources) and informs mitigation measures to minimize the breadth of impact of attacks in CPS network(s). It addresses the communications plan and information sharing necessary to report and mitigate potential cyber-events from reoccurring. In addition, it disseminates information about issues (e.g., weaknesses, vulnerabilities, attack vectors) that may not have been exploited or previously reported.

3.2 CPSS Life Cycle Management Processes

NOTE: Designated, skilled personnel, with an understanding of system and software engineering processes, are necessary to effectively accomplish the activities and tasks of [3.2](#). This document maps into system and software processes of ISO/IEC/IEEE 15288 and the security engineering extensions established by NIST Special Publication 800-160 Volume 1.

3.2.1 Planning Process

3.2.1.1 The CPSSEP shall document:

- a. Traceability such that documentation and information is:

1. Referenced in the CPSSEP; or
2. Included in the CPSSEP, such that the CPSS activities are distinguishable.

NOTE: The CPSSEP documentation and information may be consolidated in a single document or section, or else separated; in which case, all the separate data-items will reference and be referenced by one main CPSSEP.

- b. All the CPSS life cycle risk management objectives and activities, including their dependencies on other activities or information.
- c. The CPSS-related assignments of organizational responsibility and corresponding authority for each activity and for the plan in general, along the CPS life cycle.
- d. All the CPSS-related external relations and agreements with entities not under the control of the organization.
- e. All the required resources for meeting all the CPSSEP's objectives and the planned allocation of these resources for the CPSS project.
- f. The following may be incorporated and coordinated into the organizations overall system, enterprise, program, or related project planning but shall include the below elements:
 1. The CPSS project's schedule.
 2. The CPSS project's outcomes and products.
 3. All the enabling and supporting processes for the plan, including their own cybersecurity risk management.

3.2.1.2 The CPSSEP shall be consistent with the following, identifying and justifying all deviations, if any:

- a. This document.
- b. The organization's cybersecurity policy and the organization-specific CPSS rules and processes, including, but not limited to, safety, engineering, and risk management.
- c. All the other CPS plans, including but not limited to the development plans and safety plans.
- d. Any plans for other entities that directly interact with the CPS on aspects affecting cybersecurity, including, but not limited to, any entities or systems of which the CPS is a subset.
- e. Any other CPSS-related plans for the CPS that might be produced outside the scope of the CPSSEP, such as software CPSSEP, hardware CPSSEP, and others.

3.2.1.3 The CPSSEP shall integrate risk management into the technical processes through the entire life cycle. This will support CPS security in the following manner:

- a. Inclusion of only product suppliers and/or service providers which comply with this document or an equivalent in the CPS supply chain and oversight of CPS supply chain by the CPSS project to assure compliance.

NOTE: This objective propagates down the supply chain to the elements of the CPS including system architecture of the manufacturing facilities.

- b. For all CPS elements that were or are developed out of the CPS project context, including but not limited to elements made by providers non-compliant with objective (a) above, commercial-off-the-shelf elements, open-source elements, and re-used elements:
 - 1. Establish trustworthiness for all such elements included within the CPS security perimeter.
 - 2. Assess trustworthiness and manage the resultant cybersecurity risk according to criteria that are pre-defined within the CPSSEP for all elements not included in the CPS security perimeter.

3.2.2 Enabling-Processes

3.2.2.1 The CPSSEP shall:

- a. Assess the CPSSEP objectives, correlate them to the activities required to accomplish these objectives and detail a work plan for the successful completion of these activities.
- b. Specify the domains of consideration of the CPS enabling processes within the entire life cycle of the CPS, as detailed in this document.
- c. Maintain the CPSSEP, by including, as a minimum, a control process, a decision management process, an issues resolution process, and a change management process.

3.2.2.2 The CPSSEP shall define a decision process for the CPSS resources:

- a. Human resources.
- b. Knowledge resources.
- c. People, processes, technology, finance, and execution resources.
- d. Tools and infrastructure.

- e. The allocation, acquisition and/or development of all the required resources, including, but not limited to, the training of personnel and the development of infrastructure.
- f. Constraints and issues that might challenge resources required by the CPSSEP.

3.2.2.3 The CPSSEP shall define how the existing systems shall be utilized to achieve the defined CPSS objectives, including as minimum the following:

- a. A security management system.

NOTE: A security management system is the set of practices used to assure the security of the system through its life cycle with respect to CPSS.

- b. A process/quality management system, including all applicable policies, standards, procedures, and plans.
- c. A configuration management system.
- d. An information management system.

3.2.3 Supporting Processes

The CPSSEP shall include:

- a. Process audits to be conducted throughout the CPSS life cycle along with the objectives and activities pertaining to the audits.
- b. Technical reviews to be conducted throughout the CPSS life cycle along with the objectives and activities pertaining to the reviews.
- c. The required level of independence for all processes, whenever used for enhancing the assurance rigor.

NOTE: Independence may be required for technical activities, such as verification, and/or for process assurance activities, such as audits.

- d. Pre-defined criteria for the advancement from each life cycle phase to the next one.
- e. Issue response management.
- f. Change management, including changes to plans and procedures and changes derived from external events or mandates.
- g. Checklists to support the quality of the process and produce evidence.
- h. Quality control and assurance, including measurement processes and improvement cycles.
- i. Requirements traceability upstream and downstream the life cycle phases, according to this document.

3.2.3.1 The CPSSEP shall specify, as a minimum, the following CPSS aspects of configuration management:

- a. Identifying all the items to be managed, including, as a minimum, the processes, products, infrastructure, artifacts, data items, plans, procedures, standards.
- b. Defining the baseline version for each managed item.
- c. Determining the configuration management objectives and activities.
- d. Determining the change management objectives and activities.

- e. Establishing an issue reports management system.
- f. Retaining the configuration management records throughout the entire life cycle.

NOTE 1: Use of an existing plan that addresses these elements is acceptable.

NOTE 2: Various change control levels may be defined for different risk-based traceability needs, and depending on the business objectives.

3.2.3.2 The CPSSEP shall have an information management process for CPSS, which includes, as a minimum, the following information management aspects:

- a. Identifying all the CPS project information items to be managed and protected.
- b. Establishing an information protection system to protect all such information items.
- c. Managing the security of the CPS project information items using the information protection system throughout the CPS life cycle.

3.2.3.3 The CPSSEP shall specify, as a minimum, the following risk management aspects:

- a. The establishment and utilization of a risk management process for the CPS life cycle.
- b. The identification, assessment, and addressing of risks to an acceptable risk level for all the technical aspects specified for the CPS life cycle phases in this document.
- c. The identification, assessment, and addressing of risks to an acceptable risk level for all the non-technical aspects of the CPS, including, but not limited to:
 - 1. All the infrastructure and tools used in the CPS project for planning, development, process management, information management, production, service support, maintenance, and others.
 - 2. All the personnel related to the CPS project.
 - 3. All the entities interconnected and/or related to the CPS project, internal and external.
- d. The default risk for all CPS entities that have not been assessed for their risk to be set to the highest risk level for the CPS, until and unless otherwise justified.

3.3 CPSS System and Software Engineering Technical Processes Overlay

The organization shall document in their CPSSEP their system and software engineering technical processes listed in [3.3.1](#) through [3.3.14](#). These technical processes may need to be iteratively performed over the life of the system. Each element of this overlay represents a repetitive process represented by [Figure 3](#).

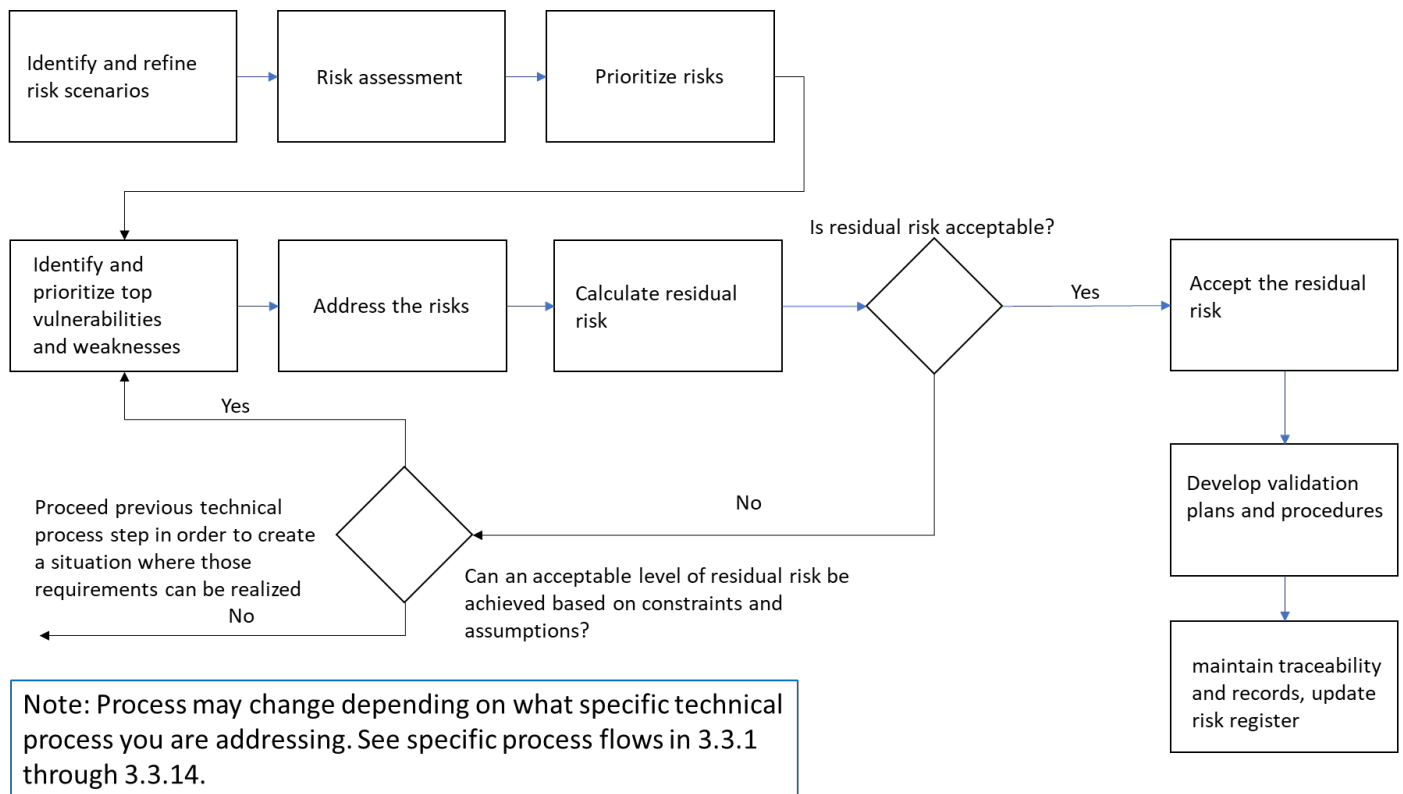


Figure 3 - Overlay loop processes

NOTE 1: Designated, skilled personnel, with an understanding of system and software engineering processes, are necessary to effectively accomplish the activities and tasks of 3.3.1 through 3.3.14. This document considers and compliments into system and software processes of ISO/IEC/IEEE 15288 and the security engineering extensions established by NIST Special Publication 800-160 Volume 1.

NOTE 2: In addressing CPSS common principles of risk management were interwoven into the technical processes. Organizations are free to use different risk assessment methodology and core determinations of traceability where outlined without specific process requirements.

3.3.1 Business or Mission Analysis Process

- a. CPSS purpose: Define and characterize the CPSS threats, vulnerabilities, and weaknesses that, if exploited, could impact the realization of the business or mission objective of the system.

NOTE 1: Exploitation involves violations of availability, loss of data or system integrity, disruption of the system mission, and/or loss of confidentiality.

NOTE 2: The priority order of these types of exploitations is the opposite of the classic order used for IT systems due to the safety-critical nature of CPS. ISA/IEC 62443 provides a more detailed explanation of the rationale.

- b. Identify CPSS stakeholders.

NOTE: Stakeholders may include but are not limited to users, operators, customers, developers, integrators, maintainers, and suppliers. Stakeholders may also include internal functions such as marketing, risk and compliance, sourcing, and legal. The number of CPSS stakeholders might be bigger than the stakeholders for the system, in general.

- c. Define and document the business or mission operations.
 - 1. Identify the CPSS environment in which the system is expected to operate over its life cycle.
 - 2. Identify system business/mission supporting infrastructure and known interconnections that include physical as well as digital (such as a high-level concept analysis).
 - 3. Determine the high-level activities and information flows of the system business/mission operation. Of these activities, determine what is CPSS related or has CPSS impacts.
- d. Characterize the CPSS, considerations should include, but are not limited to, CPSS ownership, CPS security perimeter, CPSS assets, threats (internal and external), and relationships with other assets.
- e. Assess the CPSS risks.

- 1. Identify risks: Develop a set of representative scenarios composed of the CPSS threats and classes of weaknesses and vulnerabilities associated with the critical business/mission activities of the system and its supporting infrastructure. Consider the operating environments and opportunities for attack. Assure that scenarios are holistic by utilizing scenarios across the domains of consideration.

NOTE 1: Scenarios are narratives connecting potential threats exploiting a weakness or vulnerability to impact a critical function or asset leading to a business/mission loss. Scenarios provide a frame of reference for performing the risk assessment.

NOTE 2: Scenarios may be modified or created as one engages in the various CPSS system and software engineering technical processes. These changes may reflect new information or revised understanding of the CPS including, but not limited to, the CPS itself, its components, the operational environment, stakeholders and users, and the mission/business objectives.

NOTE 3: In no particular order, risk considerations include, but are not be limited to, the CPSS aspects of: manufacturing location; company ownership; workforce composition; access during manufacturing, suppliers' design, sourcing, manufacturing, packaging, and distribution processes; facility physical security; reliability of the supply chain; and other matters germane to the product, supply chain, and operational security (e.g., design house location, access during transport, etc.).

- 2. Prioritize risks: Prioritize the risks with respect to severity of consequences and probability/likelihood/frequency of the identified scenarios in accordance with the organization's scale of risk.

NOTE 1: An organization's scale of risk may be qualitative (e.g., green-yellow-red) or quantitative (e.g., a numerical value).

NOTE 2: Consequences may be to, in no particular order, safety, mission/purpose, organization/individuals, national interests.

- f. Establish the high-level CPSS needs and initial objectives
 - 1. Establish which business/mission activities will have CPSS protection based on the prioritized risks.
 - 2. Identify the protection objectives of CPSS needed to ensure that the business/mission activities can be carried out as intended.

NOTE: This is a conceptual CPSS perspective of what protection is needed to carry out the business/mission objectives.