Critical Software

TN02: Analysis of Practices and International Standards Related to Cybersecurity

CYBERSECURITY FOR SPACE

CONTRACT REFERENCE: NOT APPLICABLE.

DATE: 2024-07-31
PROJECT CODE: CSEC4SPACE
DOC. REF.: CSW-2024-TNR-01469
STATUS: APPROVED
PAGES: 63
INFORMATION CLASSIFICATION: PUBLIC
VERSION: 1.0

DISCLAIMER -

The work described in this report was performed under the Master's degree research titled "Cybersecurity for space domain". Responsibility for the contents resides in the author or organization that prepared it.

PARTNERS:

Polytechnic University of Coimbra

APPROVAL

VERSION	NAME	FUNCTION	SIGNATURE	DATE
1.0	Nuno Silva	Industry Supervisor		2024-07-31
1.0	João Carlos Cunha	Academic Supervisor		2024-07-31

AUTHORS AND CONTRIBUTORS

NAME	DESCRIPTION	DATE
Pedro Miguel Sousa	Author	2024-03-19
Nuno Silva	Reviewer	2024-05-30

COPYRIGHT

REVISION HISTORY

VERSION	DATE	DESCRIPTION	AUTHOR
0.1	19/03/2024	First revision of the technical note.	Pedro Sousa
0.2	29/04/2024	First revision of the technical note.	Pedro Sousa
1.0	2024-07-31	Updated document according to internal review comments. Document Approved for delivery.	Pedro Sousa

TABLE OF CONTENTS

TABLE OF TABLES

TABLE OF FIGURES

1. INTRODUCTION

In today's world, we live in two distinct yet intertwined realms: the physical and the digital. Each domain has its own set of rules and guidelines, designed to navigate its complexities and safeguard individuals. In the physical world, we are governed by laws and regulations that regulate our daily interactions, from driving on roads to acquiring goods and services. These mechanisms serve as protective shields, ensuring a safe and orderly society. The digital realm, with its vast and ever-evolving landscape, demands similar safeguards. Just as physical laws guide our interactions in the real world, digital norms and protocols govern our conduct in the virtual sphere. These rules, ranging from cybersecurity protocols to data privacy regulations, are essential for ensuring a secure and equitable digital experience.

1.1. OBJECTIVE

This technical note aims to compile a list of international cybersecurity standards and associated best practices derived from both literature and existing standards.

1.2. SCOPE

This technical note examines software-based cybersecurity standards that focus on practical procedures, organizational considerations, analyses, development processes, and testing methodologies.

1.3. AUDIENCE

The audience of this technical note includes: Critical Software S.A., Coimbra Institute of Engineering, and Engineers/Researchers interested in the field of cybersecurity.

1.4. DEFINITIONS AND ACRONYMS

Table 1 presents the list of definitions used throughout this document.

NAME	DESCRIPTION
Availability	Ensuring timely and reliable access to and use of information.
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Attack Vector	Attack vector is a path or means by which an attacker or hacker can gain access to a computer or network server to deliver a payload or malicious outcome.
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, and confidentiality.

NAME	DESCRIPTION
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Critical Infrastructure	Critical infrastructure refers to the systems, facilities and assets that are vital for the functioning of society and the economy.
Integrity	Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
Threat Actor	Threat actors, also known as cyberthreat actors or malicious actors, are individuals or groups that intentionally cause harm to digital devices or systems by exploiting vulnerabilities in computer systems, networks and software.
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Reference Document	A document is considered a reference if it is referred but not applicable to this document. Reference documents are mainly used to provide further reading.

Table 1: Definitions

Table 2 presents the list of acronyms used throughout this document.

ACRONYM	DESCRIPTION
AISS	Aeronautical Information System Security
ATT	Attack
ANS	Air Navigation Services
ATM	Air Traffic Management
ARP	Aerospace Recommended Practice
ASPICE	Automotive Software Process Improvement and Capability Determination
CAP	Composition Assurance Package
CCSDS	Consultative Committee for Space Data Systems
CEN	European Committee for Standardization

ACRONYM	DESCRIPTION
CENELEC	European Committee for Electrotechnical Standardization
CERT	Coordination Center of the Computer Emergency Response Team
CIP	Critical Infrastructure Protection
CIO	Chief Information Officer
CLC	CENELEC
COMP	Composite Product Package
COTS	Commercial-off-the-shelf
CPI	Command Link Critical Program/Project Information
CSF	Cybersecurity Framework
CSMS	Comprehensive Cybersecurity Management System
CSW	Critical Software
CTF	Capture the Flag
CUI	Control Unclassified Information
DCS	Distributed Control System
DES	Data Encryption Standard
DREAD	Damage, Reproducibility, Exploitability, Affected Users, and Discoverability
EAL	Evaluation Assurance Level
EASA	European Union Aviation Safety Agency
ECSS	European Cooperation for Space Standardization
EUROCAE	European Organisation for Civil Aviation Equipment
ESA	European Space Agency
FAA	Federal Aviation Administration
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management
FHA	Functional Hazard Analysis
GOTS	Government-off-the-shelf
HSIA	Hardware-Software Interaction Analysis

ACRONYM	DESCRIPTION
IAC	Identification and Authentication Control
IACS	Industrial Automation and Control Systems
IEC	International Electrotechnical Commission
ICAM	Identity, Credential, and Access Management
I&C	Instrumentation and Control
IEEE	Institute of Electrical and Electronics Engineers
IIOT	Industrial Internet of Things
ISA	International Security Alliance
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISVV	Independent Software Verification and Validation
JAXA	Japan Aerospace Exploration Agency
MASTG	Mobile Application Security Testing Guide
MASVS	Application Security Verification Standard
MITRE	Massachusetts Institute of Technology Research Establishment
MOTS	Modified-off-the-shelf
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirements
NPD	NASA Policy Directives
NRB	Non-conformance Reporting Board
NTSS	NASA Technical Standards System
OPS	Office of the Chief Information Officer
OSI	Open Systems Interconnection
OSS	Open-Source Software

ACRONYM	DESCRIPTION
OT	Operational Technology
OWASP	Open Web Application Security Project
PDCA	Plan-Do-Check-Act
PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
PNT	Position, Navigation and Timing
PPA	Protection Profile Assurance
RDF	Restricted Data Flow
RTCA	Radio Technical Commission for Aeronautics
SAE	Society of Automotive Engineers
SAR	Security Assurance Requirement
SAISO	Senior Agency Information Security Officer
SASDS	Security Architecture for Space Data System
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SEI	Software Engineering Institute
SOC	Security Operations Center
SPICE	Software Process Improvement & Capability determination
SQL	Structured Query Language
SRTP	Security Risk Treatment Plan
SSA	System Safety Assessment
SSAR	Software Security Analysis Report
SSMP	Software Security Management Plan
SSPR	Space System Protection Requirement
STA	Security Target Assurance
STD	Standard
SUC	System Under Consideration

ACRONYM	DESCRIPTION
TNR	Technical Note Report
TOE	Target of Evaluation
TRE	Timely Response to Events
TSF	Target of Evaluation Security Functionality

Table 2: Acronyms

1.5. DOCUMENT STRUCTURE

Section 1 (Introduction) presents this document.

Section 2 provides details about the studied cybersecurity standards.

1.6. REFERENCE DOCUMENTS

Table 3 presents the list of reference documents.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-1] National Institute of Standards and Technology	https://www.nist.gov/, visited on (2024-01-11)
[RD-2] International Organization for Standardization	https://www.iso.org/home.html, visited on 2024-01-23.
[RD-3] Institute of Electrical and Electronics Engineers	http://ieee.org, visited on 2024-04-08.
[RD-4] NASA Technical Standards Systems	https://standards.nasa.gov/, visited on 2024-04-08.
[RD-5] European Cooperation for Space Standardization	https://ecss.nl/, visited on 2024-04-08.
[RD-6] The Guardian of Quantum Cybersecurity: Cryptography, Algorithms, Threats, and Optimism	https://visao.pt/exameinformatica/noticias-ei/software/2024-01-23-ciberseguranca-quantica-criptografia-algoritmos-michael-osborne/, visited on 2024-01-23.
[RD-7] Introduction to Information Security Management Systems (ISMS)	https://www.bmc.com/blogs/introduction-to-information-security-management-systems-isms/, visited on 2024-01-30.
[RD-8] FIPS 140-3 – Security Requirements for Cryptographic Modules	https://csrc.nist.gov/pubs/fips/140-3/final , visited on 2024-04-08.
[RD-9] IEC Webstore – IEC 62645:2019	https://webstore.iec.ch/publication/32904, visited on 2024-01-30.
[RD-10] International Society of Automation – ISA/IEC 62443 Series of Standards	https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards, visited on 2024-01-31.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-11] NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations	https://www.nist.gov/privacy-framework/nist-sp-800-53, visited on 2024-04-08.
[RD-12] NIST SP 800-82 – Guide to Operational Technology (OT) Security	https://csrc.nist.gov/pubs/sp/800/82/r3/final , visited on 2024-04-08.
[RD-13] NIST SP 800-171 – Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final , visited on 2024-04-08.
[RD-14] FIPS 199 – Standards for Security Categorization of Federal Information and Information Systems	https://csrc.nist.gov/pubs/fips/199/final, visited on 2024-04-08.
[RD-15] FIPS 200 – Minimum Security Requirements for Federal Information and Information Systems	https://csrc.nist.gov/pubs/fips/200/final, visited on 2024-04-08.
[RD-16] ISO – ISO 9001	https://www.iso.org/standard/62085.html, visited on 2024-05-24.
[RD-17] ISO – ISO 14001	https://www.iso.org/standard/60857.html, visited on 2024-05-24.
[RD-18] ISO/IEC 15408 – Information Security, Cybersecurity and Privacy Protection – Part One: Introduction and General Model	https://www.iso.org/standard/72891.html, visited on 2024-04-09.
[RD-19] ISO/IEC 15408 – Information Security, Cybersecurity and Privacy Protection – Part Two: Security Functional Components	https://www.iso.org/standard/72892.html, visited on 2024-04-09.
[RD-20] ISO/IEC 15408 – Information Security, Cybersecurity and Privacy Protection – Part Three: Security Assurance Components	https://www.iso.org/standard/72906.html, visited on 2024-04-09.
[RD-21] ISO/IEC 15408 – Information Security, Cybersecurity and Privacy Protection – Part Four: Framework for the Specification of Evaluation Methods and Activities	https://www.iso.org/standard/72913.html, visited on 2024-04-09.
[RD-22] ISO/IEC 15408 – Information Security, Cybersecurity and Privacy Protection – Part Five: Pre-defined Packages of Security Requirements	https://www.iso.org/standard/72917.html, visited on 2024-04-09.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-23] Spyro-soft – ASPICE 101 a Guide to Automotive SPICE	https://spyro-soft.com/blog/automotive/aspice-101-a-guide-to-automotive-spice, visited on 2024-05-27.
[RD-24] Spyro-soft – Cybersecurity ASPICE	https://spyro-soft.com/blog/automotive/cybersecurity-aspice, visited on 2024-05-27.
[RD-25] ISO/IEC 18045 - Information Security, Cybersecurity and Privacy Protection – Methodology for IT Security Evaluation	https://www.iso.org/standard/72889.html, visited on 2024-04-09.
[RD-26] ISO/SAE 21434 – Road Vehicles - Cybersecurity Engineering	https://www.iso.org/standard/70918.html, visited on 2024-04-09.
[RD-27] ISO/IEC 27000 Family – Information Security Management	https://www.iso.org/standard/iso-iec-27000-family, visited on 2024-04-09.
[RD-28] ISO – ISO/IEC 42001	https://www.iso.org/standard/81230.html, visited on 2024-05-24.
[RD-29] ISA/IEC 62443 Series of Standards	https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards, visited on 2024-05-24.
[RD-30] IEC 62645 – Nuclear Power Plants – Instrumentation, Control and Electrical Power Systems – Cybersecurity Requirements	https://webstore.iec.ch/publication/32904, visited on 2024-04-09.
[RD-31] NASA-STD-1006 – Space System Protection Standard	https://standards.nasa.gov/standard/nasa/nasa-std-1006, visited on 2024-04-09.
[RD-32] NASA-NPD 2810.1F – NASA Information Security Policy	https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=2810&s=1D, visited on 2024-04-09.
[RD-33] NASA-NPR 2810.1F – Security of Information and Information Systems	https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=2810&s=1A, visited on 2024-04-09.
[RD-34] NASA-STD-8739.8 – Software Assurance and Software Safety Standard	https://standards.nasa.gov/standard/nasa/nasa-std-87398, visited on 2024-04-09.
[RD-35] ECSS-E-ST-40C - Software	https://ecss.nl/standard/ecss-e-st-40c-software-general-requirements/, visited on 2024-04-09.
[RD-36] ECSS-Q-ST-80C – Software Product Assurance	https://ecss.nl/standard/ecss-q-st-80c-rev-1-software-product-assurance-15-february-2017/, visited on 2024-04-09.
[RD-37] Consultative Committee for Space Data Systems	https://public.ccsds.org/about/default.aspx, visited on 2024-04-09.
[RD-38] CCSDS 351.0-M-1 – Security Architecture for Space Data Systems	https://public.ccsds.org/Pubs/351x0m1.pdf, visited on 2024-04-09.
[RD-39] CCSDS 355.0-B-2 – Space Data Link Security Protocol	https://public.ccsds.org/Pubs/355x0b2.pdf, visited on 2024-04-10.

REFERENCE DOCUMENT	DOCUMENT NUMBER
[RD-40] NIST – National Vulnerability Database	https://nvd.nist.gov/, visited on 2024-04-10.
[RD-41] MITRE - Cybersecurity	https://www.mitre.org/focus-areas/cybersecurity, visited on 2024-04-10.
[RD-42] MITRE – ATT&CK	https://attack.mitre.org/, visited on 2024-04-10.
[RD-43] MITRE - Engage	https://engage.mitre.org/defenders/, visited on 2024-04-10.
[RD-44] MITRE - Defend	https://d3fend.mitre.org/, visited on 2024-04-10.
[RD-45] MITRE - Caldera	https://caldera.mitre.org/, visited on 2024-04-10.
[RD-46] MITRE – Common Weakness Enumeration	https://cwe.mitre.org/top25/archive/2023/2023_top25_list.html, visited on 2024-04-10.
[RD-47] SEI CERT Coding Standards	https://wiki.sei.cmu.edu/confluence/display/seccode/SEI+CERT+Coding+Standards, visited on 2024-04-10.
[RD-48] OWASP Foundation	https://owasp.org/, visited on 2024-04-10.
[RD-49] University of Bristol	https://www.bristol.ac.uk/engineering/research/cyber-security/, visited on 2024-04-10.
[RD-50] University of Bristol – CyBOK	https://www.cybok.org/knowledgebase1_1/, visited on 2024-04-10.
[RD-51] CLC/EN 50159 – Railway applications – Communication, signalling and processing systems	https://standards.globalspec.com/std/14256321/EN 50159, visited on 2024-04-10.
[RD-52] CLC/TS 50701 – Railway applications - Cybersecurity	https://www.en-standard.eu/clc/ts-50701-2021-railway-applications-cybersecurity/, visited on 2024-04-10.
[RD-53] AFuzion – DO-326A/ED-202A Aviation Cybersecurity	https://afuzion.com/do-326a-ed-202a-aviation-cyber-security/, visited on 2024-04-10.
[RD-54] LDRA – Aerospace Security Framework	https://ldra.com/aerospace-security-framework/, visited on 2024-04-10.

Table 3: Reference documents

2. Cybersecurity Standards

This section introduces the main cybersecurity standards/frameworks used in various domains and in the space industry.

2.1. CYBERSECURITY ORGANISATIONS

Cybersecurity standards like any other are developed through a collaborative process involving various stakeholders, including industry experts, government agencies. In this field, the main organizations that develop cybersecurity standards are:

- **National Institute of Standards and Technology (NIST)** – U.S. government agency that develops cybersecurity standards and guidelines [RD-1]. Its flagship cybersecurity framework, NIST Cybersecurity Framework (CSF), is used by organizations of all sizes.
- **International Organization for Standardization (ISO)** – non-governmental organizations that develops international standards for a wide range of product, services and processes [RD-2]. Its ISO 27000 standard family is the gold standard for information security management systems (ISMS).
- **Institute of Electrical and Electronics Engineers (IEEE)** – professional organization for engineers, that develops cybersecurity standards for a variety of technologies, such as networking and telecommunications [RD-3].
- **National Aeronautics and Space Administration (NASA) –** United States space agency responsible for space research and exploration, as well as for the development of space technologies and missions. Possess a branch responsible to build its own standards, the NASA Technical Standards System (NTSS) [RD-4]. In relation of cybersecurity, it has the standards for that purpose such as the Space System Protection Standard, while also adhering to standards set by other organizations like NIST.
- **European Space Agency (ESA) –** intergovernmental organization dedicated to space exploration, research, and technology development, with member states across Europe [RD-5]. The ECSS-E-ST-40C and ECSS-Q-ST-80C are the ESA standards that contain cybersecurity concerns.
- **MITRE –** Established as an independent adviser, applying system-thinking approach, providing solutions that enhance security and way of life in more than 65 years.
- **SEI –** Renowned as a leader in software engineering, cybersecurity, and AI engineering, they also provide well-regarded coding standards that guide developers towards secure coding practices.
- **OWASP –** The largest non-profit organization dedicated to software security, it supports the building of impactful projects, fosters communities through events and worldwide meetings, and provides valuable educational publications and resources [RD-48].
- **University of Bristol –** The University of Bristol has a cybersecurity group, that is part of the Centre of Excellence in Cybersecurity Research, that conducts research focus on security of cyber-physical infrastructures, software security and the human factor in cybersecurity [RD-49].
- **CENELEC –** The European Electrotechnical Committee for Standardization responsible for developing standards in electrotechnical field.
- **Federal Aviation Administrations (FAA) -** The Federal Aviation Administration (FAA) is a U.S. government agency operating under the Department of Transportation. They are responsible for regulating all aspects of civil aviation within the United States and surrounding international airspace, including cybersecurity.

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

2.2. National Institute of Standards and Technology

NIST does not work just for the cybersecurity area, it has a wide range of areas including artificial intelligence, climate, communications, health & bioscience, infrastructure, manufacturing, and quantum science.

Focus on cybersecurity, NIST contributes on many topics, like cryptography, cybersecurity measurement, privacy engineering technologies, trustworthy platforms, cybersecurity education and workforce development, identity & access management, risk management and trustworthy networks.

In the realm of cryptography, NIST has conducted a competition over the past seven years with the aim of uncovering novel methods to encrypt information. The objective is to identify encryption techniques that are secure not only in current systems but also in future quantum systems [RD-6].

The National Institute of Standards and Technology (NIST) maintains a real-time updated vulnerability database [RD-40]. This valuable resource empowers companies to stay constantly informed about newly discovered vulnerabilities. This awareness enables them to prioritize efforts, such as focusing on patching vulnerabilities in the hardware and software they use.

2.2.1. FIPS 140 – SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

NIST started in the field of cryptography with the publication of the Data Encryption Standard (DES) in 1977, achieving a significant success at that time. Almost 50 years have passed from the DES publication, and it is still leading the cryptography market, being a reference for most of the cryptography-related standards, such as FIPS 140 (also from NIST).

Federal Information Processing Standard 140 is a standard related to cryptography, currently in its third version [RD-8]. The title of the standard is “Security Requirements for Cryptographic Modules”, its purpose being to outline the security criteria that must be met by a cryptographic module employed in a security system safeguarding sensitive information.

Formatted: Not Highlight

It delineates four progressively escalating levels of security, starting at Level 1 and ending with Level 4. These levels are designed to encompass a broad spectrum of potential applications and environments where cryptographic modules may be utilized. The security requirements encompass various aspects related to the secure design and implementation of a cryptographic module, including module specifications, interfaces, roles, services, authentication, software/firmware security, operating environment, physical security, non-invasive security, sensitive security parameter management, self-tests, life-cycle assurance, and the mitigation of other potential attacks.

The FIPS 140 standard is applicable to all entities that use security systems relying on cryptography, for the purposes of protecting sensitive information in computer and telecommunication systems. These systems interact with applications like data storage, access control and personal identification, and network communication in various environments, for example centralized computer facilities, and hostile environments.

The selection of cryptographic services, such as block ciphers, post-quantum cryptography, and lightweight cryptography, depends on the specific application and environment.

2.2.2. NIST SP 800-53 – SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

NIST SP 800-53 is about to undergo its fifth revision, this standard establishes compulsory controls for both information systems and organizations, as dictated by the Federal Information Security Modernization Act (FISMA), to protect the confidentiality, integrity, and availability of the system and its data [RD-11].

Formatted: Not Highlight

The primary purpose of the SP 800-53 is to enhance cybersecurity practices and protect sensitive information by providing a structured framework for risk management.

These controls are adaptable for implementation in any organization or information system that covers both national security and non-national security systems, by:

- Supplying an adaptable collection of security and privacy controls design to address present protection requirements and adapt to evolving needs arising from changing threats, requirements, and technologies.
- Building the backbone for the development of assessment methods and procedures for evaluating the performance of the controls.
- Enhancing communication across organizations by utilizing a shared vocabulary that facilitates discussion on concepts related to security, privacy, and risk management.

2.2.3. NIST SP 800-82 – GUIDE TO OPERATIONAL TECHNOLOGY SECURITY

In its third revision, NIST SP 800-82 provides guidance for establishing secure operational technology (OT) systems. It considers factors like performance, reliability, and safety requirements [RD-12].

Formatted: Not Highlight

OT is employed across various industry sectors, including critical infrastructure such as the chemical sector, water and wastewater systems, and the nuclear reactors and waste sector.

The document begins with an overview of OT systems, covering their operation, architectures, and key components. It then emphasizes the importance of cybersecurity in OT systems and introduces a process for creating an OT cybersecurity program, including:

- Defining objectives and scope.
- Establishing a cross-functional team with OT and cybersecurity skills.
- Establishing policies and procedures.
- Identifying cyber risk management capabilities.
- Identifying day-to-day operations of event monitoring and auditing for compliance and improvement.

Following the discussion on risk management, the document delves into securing OT environments. It explores strategies for assessing risks and implementing mitigation measures, considering factors like risk tolerance, resource limitations, and organizational priorities.

Furthermore, it sheds light on designing robust security strategies for OT systems.

Such strategy could be the "defence in depth", where emphasizes the importance of implementing multiple security controls at different levels to create a resilient system. Table 4 outlines the key focus areas within each layer of a defence in depth strategy, highlighting the specific controls that contribute to an organization's overall cybersecurity posture.

Layer	Focus
1	•Security management
2	•Protection of physical locations •Physical access control •Access monitoring systems •People and asset tracking
3	•Network architecture principles of segmentation and isolation •Centralize log •Network monitoring •Malicious code protection •Zero trust architecture
4	•Monitoring and analysis •Secure configuration and management

Layer	Focus
	•Endpoint hardening •Integrity protection •Access control •Device identity •Root of trust
5	•Application allowlisting •Patching •Secure code development •Configuration management

Table 4: Defence in depth layer focus

Section 5.3 from NIST SP 800-82 presents additional cybersecurity architectures considerations (distributed control system (DCS)-based, DCS and programmable logic controllers (PLC) based OT with IIOT and SCADA based) should consider various aspects. The aspects to consider include cyber-related safety, availability, geographically distributed systems, and environmental and regulatory requirements as depicted in Table 5.

Formatted: Not Highlight
Formatted: Not Highlight
Formatted: Not Highlight

Consideration	Description
Cyber-related safety	•Additional communication and cybersecurity requirements (segmentation and isolation) •Choose security mechanism based on safety requirements •Employ a Fail-safe design
Availability	•Guarantee availability at multiple levels: data, applications, IT infrastructure, power, and other supporting utilities.
Geographically distributed systems	•Difference in physical security in remote locations create additional risks to OT operational or safety.
Regulatory	•Consider cyber-related regulatory requirements when designing a cybersecurity architecture. (e.g. NERC Standard CIP-005)
Environmental	•Conduct hazard analysis to determine if their processes or equipment pose environmental hazards.
Field I/O security	•Make risk-based decisions to decide where within the OT system, the use of mitigation security controls (digital twins, separate field I/O monitoring network) should be implemented to detect incorrect data.

Table 5: Defence in Depth Considerations

The document ends with a guide on how to apply the NIST cybersecurity framework in OT systems. It consists of five concurrent and continuous functions:

- **Identify** – Establish a cybersecurity risk management to systems, people, assets, data and capabilities.
- **Protect** – Develop strategies to execute when critical services are disrupted.
- **Detect** – Develop means to detect cybersecurity events.
- **Respond** – Develop and implement procedures to take place when a cybersecurity event occurs.
- **Recover** – Develop and implement a set of activities for restoring services disrupted by a cybersecurity event.

2.2.4. NIST SP 800-171 – PROTECTING CONTROLLED UNCLASSIFIED INFORMATION

The NIST SP 800-171 standard, now in its second iteration, concentrates on safeguarding information confidentiality shared between the federal government and its external service providers (e.g., financial, web, electronic mail, healthcare) as well as educational institutions such as colleges and universities, by the recommendation of security requirements [RD-13].

Formatted: Not Highlight

The requirements are organized into fourteen families, each family containing requirements related to the general security topic aligned with the minimum-security requirements for federal information and systems described in FIPS 200. [RD-15] lists the fourteen security requirements families.

FAMILIES	
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Information Integrity

Table 6: Security Requirements Families

Under this standard, the US federal government assumes the responsibility of delineating the types of information that necessitate protection when exchanged with non-federal systems and organizations. It ensures that only information requiring protection is added to the Controlled Unclassified Information (CUI).

The CUI Program addresses deficiencies in managing and protecting unclassified information, including inconsistent markings, inadequate safeguarding, and unnecessary restrictions. It achieves this by standardizing procedures and providing common definitions through an online repository that saves information, guidance, policy, and requirements on handling CUI. The repository is known as the CUI Registry.

The CUI must comply with four other standards:

- **FIPS 199** – Standards for Security Categorization of Federal Information and Information Systems.
- **FIPS 200** – Minimum Security Requirements for Federal Information and Information Systems.
- **NIST SP 800-53** – Security and Privacy Controls for Federal Information Systems and Organizations.
- **NIST SP 800-60** – Guide for Mapping Types of Information and Information System to Security Categories.

2.2.5. FIPS 199 – STANDARDS FOR SECURITY CATEGORIZATION OF FEDERAL INFORMATION AND INFORMATION SYSTEMS

The United States, acknowledging the significance of information security in the economic sector, endorsed the E-Government Act of 2002. In compliance with the Federal Information Security Management Act (FISMA), NIST formulated standards and guidelines for categorizing the information.

FIPS 199, the first of two mandatory security standards, categorizes information and associated systems according to the potential impact of attacks that could compromise the data essential for an organization to achieve its objectives. These categories are designed to safeguard assets, uphold operational functions, and ensure the confidentiality of collaborators [RD-14].

Formatted: Not Highlight

There are three security objectives for information and information systems:

- **Confidentiality** – unauthorized disclosure of information.
- **Integrity** – unauthorized modification or destruction of information.
- **Availability** – disruption of access to or use of information and information systems.

For the categorization, this standard defines three levels of potential impact of attack on organizations or individuals that compromise the three security objectives mention above. The levels are:

- **Low** – limited adverse effects on organization operations (i.e. degradation in mission capabilities), assets (i.e. minor damage to assets) or individuals (i.e. minor harm to individuals).
- **Moderate** – serious adverse effects on organization operations (i.e. significant degradation in mission capabilities), assets (i.e. considerable damage to assets) or individuals (i.e. significant harm to individuals not involving loss of life).
- **High** – severe or catastrophic adverse effects on organization operations (i.e. loss mission capabilities), assets (i.e. major damage to assets) or individuals (i.e. severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries).

	POTENTIAL IMPACT		
SECURITY OBJECTIVE	**LOW**	**MODERATE**	**HIGH**
Confidentiality	Unauthorized disclosure of information leading to **limited** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized disclosure of information leading to **serious** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized disclosure of information leading to **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity	Unauthorized modification or destruction of leading to **limited** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized modification or destruction of leading to **serious** adverse effect on organizational operations, organizational assets, or individuals.	Unauthorized modification or destruction of leading to **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability	Disruption of access to or use of information could lead to **limited** adverse effect on organizational operations, organizational assets, or individuals.	Disruption of access to or use of information could lead to **serious** adverse effect on organizational operations, organizational assets, or individuals.	Disruption of access to or use of information could lead to **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Table 7: Potential Impact Definitions for each Security Objective

Base on Table 7 the categorization can be made by applying a generalized format for expressing the security category (SC), for example:

- **SC** information type = {(**confidentiality**, *impact*), (**integrity**, *impact*), (**availability**, *impact*)}

2.2.6. FIPS 200 – MINIMUM SECURITY REQUIREMENTS FOR FEDERAL INFORMATION AND INFORMATION SYSTEMS

As the second obligatory security standard mandated by FISMA legislation, FIPS 200 outlines the minimum-security requirements for information and information systems [RD-15]. It encourages the creation, implementation, and operation of information systems with robust security by setting minimum levels of due diligence for information security. Additionally, it promotes a more uniform, comparable, and repeatable approach for the selection and specification of security controls in information systems that fulfil the minimum-security criteria.

Formatted: Not Highlight

The minimum-security requirements encompass seventeen security-related areas, with the objective of protecting the three security objectives/principles, including:

- **Access Control** – organizations must limit information system access to authorized users, process, or devices.
- **Awareness and Training** - organizations must ensure that managers and users are trained to carry out their assigned information security-related duties and be aware of the security risks associated with their activities.
- **Audit and Accountability** – organizations are required to maintain records of information system usage to facilitate the monitoring, analysis, investigation, and reporting of any unauthorized or inappropriate activities within the system. This ensures the ability to trace such activities back to the responsible individual, holding them accountable for their actions.
- **Certification, Accreditation, and Security Assessments** – organisations must assess the security controls in their information systems to determine if the controls are effective, if not must have a plan of action designed to correct deficiencies and reduce or eliminate vulnerabilities.
- **Configuration Management** – organizations are required to establish and maintain baseline configurations and inventories of organizational information systems, encompassing hardware, software, firmware, and documentation, throughout the various stages of the system development life cycle. Additionally, organizations must establish and enforce security configuration settings for the information technology products utilized within these systems.
- **Contingency Planning** – organizations must create plans for emergency response, like backup operations, and post-disaster recovery for the information system to ensure the availability and continuity of the operations.
- **Identification and Authentication** – organizations must be able to identify information system users, processes, or devices and authenticate the identities.
- **Incident Response** – organizations are required to possess the ability to prepare for, detect, analyse, contain, recover from, and respond to incidents. Moreover, they must be equipped to track, document, and report incidents to organizational officials and/or authorities.
- **Maintenance** – organizations must maintain the information system regularly, and provide effective control on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.
- **Media Protection** – organizations must safeguard information system media, encompassing both physical and digital formats, by restricting access to authorized users. When disposing of or releasing information for reuse, it is imperative to first sanitize or destroy the media to ensure data security.

- **Physical and Environmental Protection -** organizations must restrict physical access to information systems, equipment, and their corresponding operating environments to authorized individuals. Additionally, they should safeguard the physical plant and support infrastructure for information systems, furnish necessary utilities, shield information systems from environmental risks, and implement suitable environmental controls within facilities housing these systems.
- **Planning** – organizations must formulate a security plan for their information systems, delineating both the current or intended security controls and the protocols governing access to these systems.
- **Personnel Security** – organizations are obligated to designate security personnel with a constant duty to safeguard information systems. Any failure to adhere to security policies and procedures should result in penalties.
- **Risk Assessment** – Organizations are required to regularly evaluate the risks posed to organizational operations, as well as to organizational assets and individuals. This assessment encompasses the operation of organizational information systems and the associated processes, storage, or transmission of organizational information.
- **System and Services Acquisition** – organizations must allocate ample resources to effectively safeguard organizational information systems. They should integrate information security considerations into their system development life cycle processes, enforce restrictions on software usage and installation, and verify that third-party providers implement adequate security measures to protect outsourced information, applications, and/or services.
- **System and Communications Protection** – organizations should possess the capability to monitor, control, and safeguard both internal and external communication within their information systems. Furthermore, they must utilize architectural designs, software development techniques, and systems engineering principles that enhance effective information security throughout the organizational information system.
- **System and Information Integrity** - organizations are required to promptly identify, report, and rectify flaws in information and information systems. They must implement safeguards against malicious code at relevant locations within organizational information systems. Additionally, organizations should monitor security alerts and advisories for information systems and undertake appropriate actions in response.

To fulfil the minimum-security requirements, organizations must choose suitable security controls and assurance requirements as outlined in NIST SP 800-53 [RD-11], discussed in section 2.2.2. This selection is contingent on the impact levels assigned to the organizational information systems, as determined through the security categorization process.

2.3. International Organization for Standardization

The International Organization for Standardization (ISO) is a non-governmental international entity dedicated to formulating and publishing standards. These standards aim to guarantee the quality, safety, efficiency, and interoperability of products, services, and systems across diverse industries. By offering a common language and set of criteria, ISO facilitates adherence for businesses, organizations, and governments, thereby promoting global trade and fostering innovation.

ISO standards offer numerous benefits, such as facilitating international trade by ensuring product compatibility and quality, enhancing safety and reliability, and promoting innovation and sustainability. Some top ISO standards include **ISO 9001** [RD-16] for quality management, **ISO 14001**[RD-17] for environmental management, **ISO 27001** [RD-27] for information security management, and **ISO 42001** [RD-28] for information technology (artificial intelligence management system) [RD-2].

2.3.1. ISO/IEC 15408 – INFORMATION SECURITY, CYBERSECURITY AND PRIVACY PROTECTION

ISO/IEC 15408, commonly known as the Common Criteria (CC), is an international standard consisting of five parts, developed to provide a framework for evaluating and certifying the security features of information technology products. The standard is crucial for establishing a trusted and consistent approach to assessing the security capabilities of various products and systems.

2.3.1.1. PART ONE – INTRODUCTION AND GENERAL MODEL

This part offers a comprehensive summary of all five parts of the standard [RD-18]. It elucidates the various elements within the ISO/IEC 15408 series, provides definitions for terms and abbreviations used across the standard, introduces the fundamental concept of a Target of Evaluation (TOE) — representing the subject of evaluation, which could be an IT product or a component thereof. The section outlines the evaluation context and identifies the intended audience for the evaluation criteria. Moreover, it introduces vital security concepts essential for the evaluation of IT products.

Formatted: Not Highlight

2.3.1.2. PART TWO – SECURITY FUNCTIONAL COMPONENTS

This part outlines the necessary structure and content for security functional components, designed to facilitate security evaluations. It encompasses a catalogue of functional components in form of classes that fulfils the shared security functionality requirements applicable to numerous IT products [RD-19], depicted in Table 8.

Formatted: Not Highlight

COMPONENTS	DESCRIPTION
Security audit	Recognizing, recording, storing, and analysing information related to security relevant activities, to be examined to determine which security relevant activities took place and who is responsible for them.
Communication	Facilitating the management of cryptographic keys across their lifecycle.
Cryptographic support	The TSF (TOE security functionality) may employ cryptographic functionality to help satisfy several high-level security objectives.
User data protection	Specifying requirements related to protecting user data.
Identification and Authentication	Address the requirements for functions to establish and verify a claimed user identity.
Security management	Specify the management of several aspects of the TSF (TOE security functionality) : security attributes, TSF data and functions.
Privacy	Contains privacy requirements to protecting against discovery and misuse of identity.
Protection of the TSF	Contains families of functional requirements that relate to the integrity and management of the mechanisms that constitute the TSF (TOE security functionality) and to the integrity of TSF data.
Resource utilization	Support the availability of required resources such as processing capability and/or storage capacity.
TOE access	Specifies functional requirements for controlling the establishment of a user's session
Trusted path/channels	Provide requirements for a trusted communication path between users and the TSF (TOE security functionality), and for a trusted communication channel between the TSF and other trusted IT products.

Table 8: Component Catalogue

2.3.1.3. PART THREE – SECURITY ASSURANCE COMPONENTS

The third part of the ISO/IEC 15408 is responsible for establishing the assurance requirements [RD-20]. It includes the individual assurance components that form the basis for the evaluation assurance levels and additional packages outlined in the fifth part of the standard. Additionally, the document provides criteria for the evaluation of Protection Profiles (PPs), PP-Configurations, PP-Modules, and Security Targets (STs).

2.3.1.4. PART FOUR – FRAMEWORK FOR THE SPECIFICATION OF EVALUATION METHODS AND ACTIVITIES

By employing a standardized framework, it becomes feasible to define objective, repeatable, and reproducible evaluation methods and activities.

This part outlines how novel evaluation activities can be derived from the generic work units in ISO/IEC 18045. These activities can then be amalgamated into an evaluation method tailored for specific evaluation contexts, such as a particular Target of Evaluation (TOE) type or a distinct technology type [RD-21].

The correlation between the structure of a Security Assurance Requirement (SAR) in ISO/IEC 15408-3 and the corresponding work units in ISO/IEC 18045 is detailed within the standard, with a summarized depiction provided in Figure 1.

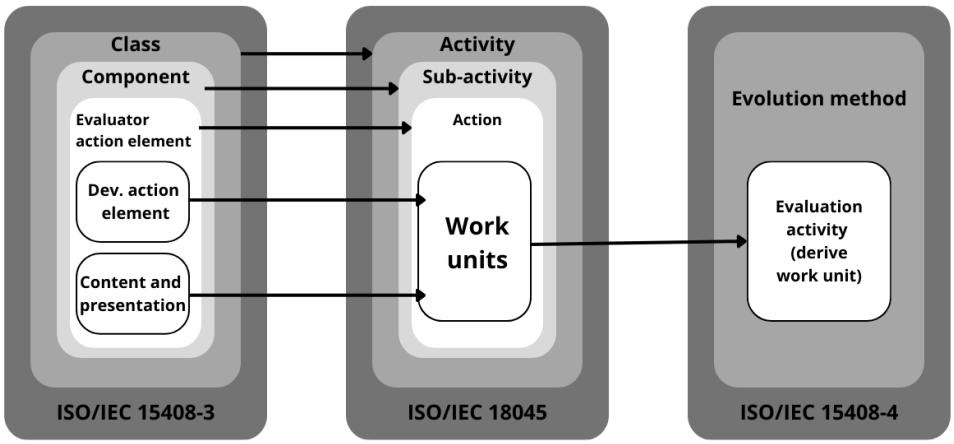

Figure 1: Mapping of ISO/IEC 15408-3 and ISO/IEC 18045

2.3.1.5. PART FIVE – PRE-DEFINED PACKAGES OF SECURITY REQUIREMENTS

In the concluding part of this standard, packages of security assurance and security functional requirements are presented. These packages have been recognized as essential to facilitate common usage by stakeholders [RD-22].

This part covers the following topics:

- A set of seven evaluation assurance level (EAL) family of packages, which delineate pre-defined collections of security assurance components.
    - Level 1 – Functionally tested.
    - Level 2 – Structurally tested.
    - Level 3 – Methodically tested and checked.

Formatted: Not Highlight

Formatted: Not Highlight

Formatted: Not Highlight

- Level 4 - Methodically designed, tested and reviewed.
- Level 5 – Semi-formally verified designed and tested.
- Level 6 - Semi-formally verified design and tested.
- Level 7 - Formally verified design and tested.

- A composition assurance (CAP) family of packages, outlining sets of security assurance components utilized for specifying appropriate security assurances during the evaluation of composed TOEs.
- A composite product (COMP) package, specifying a set of security assurance components for articulating the required security assurances during the evaluation of a composite product TOE.
- A protection profile assurance (PPA) family of packages, defining sets of security assurance components for articulating the necessary security assurances during a protection profile evaluation.
- A security target assurance (STA) family of packages, detailing sets of security assurance components used for specifying the appropriate security assurances during a security target evaluation.

2.3.2. ISO/IEC 18045 – EVALUATION CRITERIA FOR IT SECURITY

This standard is responsible to support the conduction of an evaluation of the implementation according to ISO/IEC 15408 series, by providing the minimum actions to be performed by an evaluator. As such the ISO/IEC 18045 is the companion document to ISO/IEC 15408 [RD-25].

Formatted: Not Highlight

The ISO/IEC 18045 offers a structured approach to guide the evaluation, breaking down the process into a series of steps, namely:

- **Input task** – Involve managing the evaluation evidence, which includes gathering, organizing, and documenting all relevant information related to the evaluation.
- **Output task** – Build the evaluation report, which summarizes the evaluation findings and provides a detailed assessment of the TOE´s security capabilities.
- **Evaluation Sub-activities** – Core of the evaluation process, involving assessment of the security functional requirements and the security assurance requirements of the TOE.
- **Demonstration of Technical Competence to the Evaluation Authority task** – Verifies the technical expertise of the evaluators involved in the evaluation.

2.3.3. ISO/IEC 20214 – SPACE DATA AND INFORMATION TRANSFER SYSTEMS – SECURITY ARCHITECTURE FOR SPACE DATA SYSTEMS

ISO 20214:2015 serves as a high-level reference guide for space system engineers. It aims to enhance their understanding of layered security concepts critical for securing space systems, considering the type of space mission. The standard defines a Security Architecture for Space Data Systems (SASDS).

The Space Data System (SASDS) leverages the views outlined in the CCSDS Magenta Book 351.0-M-1, titled "Security Architecture for Space Data Systems," which was developed by the CCSDS Architecture Working Group.

The book starts by discussing the security aspects of a space data system architecture from five different viewpoints [RD-38]:

- **Enterprise Viewpoint**: Describes the organizations involved in a space data system and their relationships, including roles, responsibilities, policies, agreements, and contracts.
- **Connectivity Viewpoint**: Describes the physical structure and environments of a space data system.
- **Functional Viewpoint**: Describes the functional structure of a space data system and how functions interact with each other.

- **Information Viewpoint**: Focuses on the information objects exchanged between functional objects.
- **Communication Viewpoint**: Describes the protocol stacks and mechanisms used for information transfer among physical entities in space data systems.

By using these viewpoints, the book addresses the three general security principles: physical security, information security, and transmission security. Additionally, it offers a series of recommendations for describing the security aspects of system design for each viewpoint, providing guidance on how to analyse a system design as well.

CCSDS Magenta Book 351.0-M-1 describes key principles of the CCSDS Security Reference Architecture, such as **open standards**, **protection through layered security mechanisms**, **expandability**, **flexibility**, **interoperability**, **key management, selection of encryption algorithms**, **Kerckhoff´s principle** and **fault tolerance**.

The security architecture will vary depending on the type of space mission (human spaceflight, Earth observation, communication, scientific, or navigation). The book offers guidance on how to choose the right security architecture for a specific mission.

Finally, by considering the three general security principles outlined in the Magenta Book and the specific space mission, a series of security requirements for the chosen architecture are formulated.

2.3.4. ISO/IEC 21434 – ROAD VEHICLES – CYBERSECURITY ENGINEERING

ISO/IEC 21434 establishes a comprehensive set of requirements for managing cybersecurity risks throughout the entire lifecycle of electrical and electronic (E/E) systems in road vehicles. This includes all components and interfaces involved in achieving specific functionalities at the vehicle level, from the initial concept stage to decommissioning [RD-26].

Formatted: Not Highlight

The document consists of twelve chapters, each addressing a specific aspect of automotive cybersecurity:

- **Chapter 4 - General Considerations**: This chapter sets the context and defines the approach to cybersecurity engineering for road vehicles.
- **Chapter 5 - Organizational Cybersecurity Management**: This chapter outlines requirements for cybersecurity management at the organizational level, including policies, rules, and processes.
- **Chapter 6 - Project Dependent Cybersecurity Management**: This chapter focuses on the project level and provides requirements for topics such as cybersecurity responsibilities, planning, tailoring, reuse, components-out-of-context, off-the-shelf components, cybersecurity case, assessment, and post-development release.
- **Chapter 7 - Distributed Cybersecurity Activities**: This chapter addresses assigning responsibilities for cybersecurity activities between customers and suppliers to strengthen supply chain protection.
- **Chapter 8 - Continual Cybersecurity Activities**: This chapter establishes requirements for ongoing monitoring for cyber events, risk assessments, and vulnerability management of E/E systems.
- **Chapters 9 - 14: Product Development Lifecycle**: These chapters cover the entire lifecycle of developing a product, starting with the concept phase.
    - **Chapter 9 - Concept Phase**: This chapter focuses on determining cybersecurity risks, goals, and requirements for each vehicle component.
    - **Chapter 10 - Development Phase**: This chapter details cybersecurity requirements and architectural design, as well as integration and verification activities.
    - **Chapter 11 - Cybersecurity Validation**: This chapter outlines activities for performing cybersecurity validation at the vehicle level for each item.
    - **Chapter 12 - Production Phase**: This chapter ensures the manufacturing and assembly processes consider and implement cybersecurity requirements.

- **Chapter 13 - Operation and Maintenance**: This chapter addresses activities related to responding to cyber events and maintaining the security of vehicle components.
- **Chapter 14 - Decommissioning**: This chapter covers communicating the end of cybersecurity support and enabling the decommissioning of items and components with cybersecurity considerations in mind.

- **Chapter 15 - Threat Analysis and Risk Assessment Methods**: This final chapter describes methods for identifying potential cyber threats encountered by road users.

Overall, ISO/IEC 21434 provides a valuable framework for ensuring the security of road vehicles throughout their entire lifecycle.

To tackled even further the cybersecurity problems in automotive, in February 2021 the German Association of the Automotive Industry as issues the Automotive SPICE for cybersecurity guidelines [RD-23], adding an important layer to the traditional V-model depicted in Figure 2, “Cybersecurity Engineering Process Group”.

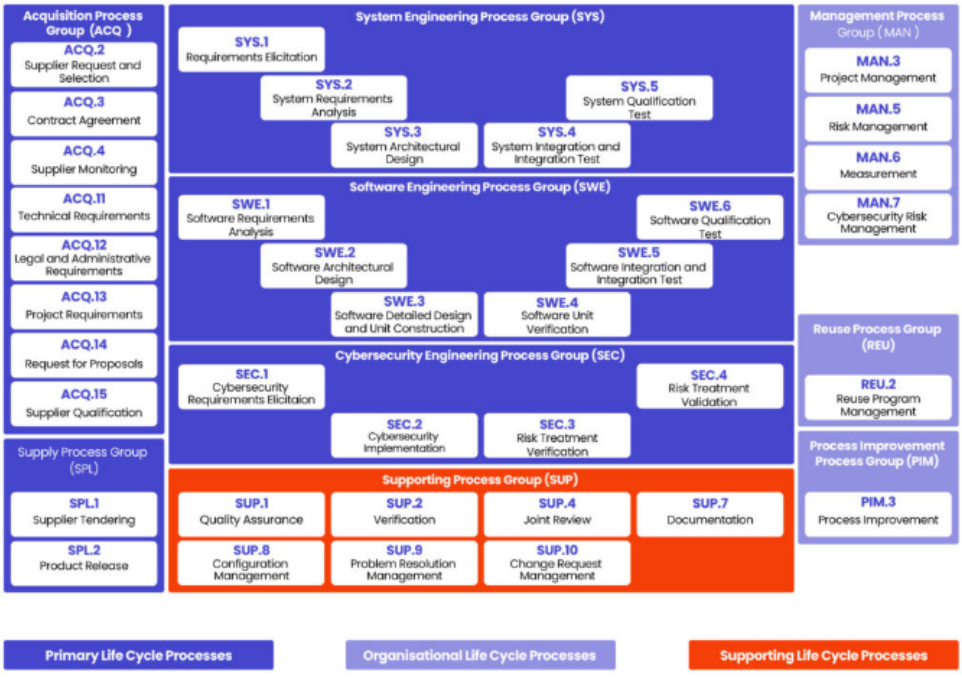

Figure 2: Automotive SPICE V-model [RD-24]

This new layer focuses on **Cybersecurity Requirements Elicitation**, the first step in the process. This step involves identifying cybersecurity requirements and goals based on the risks identified through standard risk management practices.

The next step is **Cybersecurity Implementation**, where cybersecurity controls and other actions are implemented to mitigate the identified risks.

The final two steps, **Risk Treatment Verification** and **Risk Treatment Validation**, focus on evaluating the effectiveness of the process implemented in the previous steps. This evaluation is achieved through various

techniques such as static software analysis, unit testing, integration testing, vulnerability scanning, penetration testing, and fuzz testing.

Automotive SPICE is primarily used by original equipment manufacturers (OEMs) to ensure the development and manufacturing of secure automotive components. It achieves this by focusing on two key areas: robust development processes and the cybersecurity posture of suppliers. Both aspects contribute to the overall safety and security of modern vehicles.

2.3.5. ISO/SAE 27000 FAMILY

The ISO/IEC 27000 family of standards is a set of international standards for information security management systems (ISMS). The family is designed to help organizations of all sizes improve their information security by providing a framework for implementing, managing, and maintaining an ISMS [RD-27].

Formatted: Not Highlight

An ISMS is a systematic approach to managing an organization's information security risks. It is a set of policies, procedures, and controls that are designed to protect an organization's information assets from unauthorized access, use, disclosure, disruption, modification, or destruction.

The family consists of several standards, each of which addresses a specific aspect of ISMS. The core standard, **ISO/IEC 27001**, provides the framework for improve the information security. Other standards in the family provide guidance on specific topics such as risk assessment, security controls, and incident response.

2.3.5.1. ISO/SAE 27001 – INFORMATION SECURITY MANAGEMENT SYSTEMS REQUIREMENTS

ISO/IEC 27001 is the world's leading standard for information security management systems (ISMS). Its primary purpose is to assist organizations in becoming risk-aware and proactively identifying and remediating vulnerabilities. It outlines mandatory criteria that an ISMS must fulfil to achieve the goals of risk management, cyber-resilience and operational excellence.

As organizations evolve, their risk profiles, organizational cultures, and available resources may change, necessitating adjustments to their information security management systems (ISMS). To effectively incorporate these changes, the ISO/IEC 27001 standard advocates for a cyclical approach known as the Plan-Do-Check-Act (PDCA) cycle [RD-7].

- **Plan** – Conduct thorough assessments to identify vulnerabilities and gather relevant information for evaluating security risks, and then establish comprehensive policies and procedures to address the root causes of identified issues.
- **Do** – Integrate the planed security policies and procedures into the organization´s operations, based on the company´s available resources.
- **Check** – Evaluate the performance of the ISMS regarding is policies and controls.
- **Act** – Emphasize continuous improvement throughout the ISMS implementation process, by implementing the PDCA model using past knowledge.

2.3.5.2. ISO/SAE 27002 – INFORMATION SECURITY CONTROLS

ISO 27002 focuses on protecting the Information Security Management System (ISMS) from cyber threats. To do so it offers best practices and control objectives to some cybersecurity aspects including access control, cryptography, human resource security, and incident response. By following this standard, companies ensure a proactive attitude to protect critical information and assets, possessing a reliable cybersecurity risk management.

The benefits for complying with **ISO/SAE 27002** are the following:

- **Security framework** – set of guidelines and best practices in cybersecurity aspects.
- **Risk Management** – give organizations the ability to identify, assess, and manage information security risks.

- **Client´s Trust** – by adhering to this standard, we communicate to our clients that prioritizing security is just as crucial as generating profits.
- **Cyber resilience** – reduces the likelihood of security incidents that disrupts the good function of the business.

2.3.6. ISA/IEC 62443 – SECURITY FOR INDUSTRIAL AUTOMATION AND CONTROL SYSTEMS

It is the world's only consensus-based cybersecurity standard for industrial automation and control systems (IACS), and it is widely recognized as the leading standard for cybersecurity in this domain. The IEC 62443 series is a valuable resource for organizations that are responsible for the cybersecurity of IACS systems. The standard provides a comprehensive set of requirements and guidance that can help organizations to protect their systems from cyberattacks [RD-29].

The IEC 62443 series is divided into eight parts, each of which addresses a specific aspect of IACS cybersecurity. The parts are:

1. **ISA-62443-1-1** – Terminology, concepts, and models
2. **ISA-62443-2-1** – Establish a cybersecurity management system for IACS
3. **ISA-62443-2-3** – Patch management in the IACS environment
4. **ISA-62443-2-4** – Security program requirements for IACS service providers
5. **ISA-62443-3-2** – Security risk assessment for system design
6. **ISA-62443-3-3** – System security requirements and security levels
7. **ISA-62443-4-1** – Secure product development lifecycle requirements
8. **ISA-62443-4-2** – Technical security requirements for IACS components

2.3.6.1. ISA-62443-2-1 – TERMINOLOGY, CONCEPTS, AND MODELS

This technical specification from the IEC 62443 series establishes the foundation for securing Industrial Automation and Control Systems (IACS) by defining essential terminology, concepts, and models. These include security objectives, foundational requirements, defence-in-depth strategies, security levels, threat risk assessments, and more. It serves as the essential groundwork for the remaining standards within the series.

2.3.6.2. ISA-62443-2-1 – ESTABLISH A CYBERSECURITY MANAGEMENT SYSTEM FOR IACS

This portion of the ISA-62443 standard lays forth the fundamental elements required to construct a comprehensive cybersecurity management system (CSMS) for industrial automation and control systems (IACS), imparting the expertise necessary to build these elements. The elements encompass policy, procedures, practices, and personnel, outlining what should be incorporated into the final CSMS for the organization.

The fundamental elements are organized in three main categories:

- Risk analysis.
- Addressing risk with CSMS.
- Monitoring and improving the CSMS.

Each category is divided into elements groups and/or elements, Figure 3 shows the elements of a cybersecurity management system.

Figure 3: Elements of a cybersecurity managements system

Risk Analysis constitutes the initial primary category within the CSMS, addressing the foundational information utilized by other elements in the CSMS. This category comprises two elements:

- **Business Rationale** - Identify and document the needs of an organisation to address cyber risk for the industrial automation and control systems.
- **Identification, Classification, and Assessment of Risks** – Identifying cyber risks within the IACS involves assessing both the probability of occurrence and the potential severity.

The second main category is Addressing risk with the CSMS, containing most requirements and information in the cybersecurity management system (CSMS). It is organized in three groups of elements:

- **Security policy, organization and awareness** – Strategically developing the pillars of cybersecurity policies holds organizations accountable for their cybersecurity and fosters awareness of associated issues.
    - **CSMS scope:** Identifying, assessing, and documenting the entities and activities that are subject to the Cyber Security Management System.

- **Organize for security:** Establish entities for the management, execution, and evaluation of the cybersecurity measures pertaining to the organization's IACS assets.
- **Staff training and security awareness:** Train personnel by furnishing essential information to enable them to identify, assess, address, and mitigate vulnerabilities and threats. Ensure that their work practices incorporate effective countermeasures.
- **Business continuity plan:** Identify protocols for maintaining or restoring business operations in the event of a substantial disruption.
- **Security policies and procedures**: Explain the organization's approach to defining, operating, assessing risk, and refining its security program.

- **Selected security countermeasures**: Engage in a discussion on policy, procedures, and practice issues concerning the chosen security countermeasures.
  - **Personnel security:** Establishing guidelines for ensuring that employees consistently maintain the security of IACS during their tenure with the organization.
  - **Physical and environmental security:** Ensure the security of IACS assets by maintaining a secure physical and digital environment, preventing the information from becoming unusable or damaged.
  - **Network segmentation:** Ensure uniform security levels for all IACS devices, irrespective of their zones, to attain a targeted security level.
  - **Access control – Account administration**: Ensure that access privileges are granted only to appropriate entities with valid accounts.
  - **Access control – Authentication**: Verifying the identities of users, hosts, applications, services, and resources in computerized transactions within the network to align them with their corresponding account privileges.
  - **Access control – Authorization**: Provide users with appropriate access rights based on their verified identity and the predefined account settings.

- **Implementation**: Refers to the implementation of the CSMS.
  - **Risk management and implementation**: Control the risk level in accordance with the organization's risk tolerance.
  - **System development and maintenance**: Sustain current systems and create new ones to effectively manage the risk level in alignment with the organization's tolerance.
  - **Information and document management**: categorize, oversee, protect, and provide information related to the Industrial Automation and Control Systems (IACS) and Cyber Security Management System (CSMS) to authorized personnel when it is deemed appropriate.
  - **Incident planning and response**: Develop a strategy for an organization to detect and respond when targeted by a cyberattack.

The last main category is responsible for monitoring the use of the CSMS, evaluate its effectiveness and make improvements. It´s composed by two elements:

- **Conformance**: Ensure that the Cyber Security Management System (CSMS) is utilized in accordance with the stated policies, implementing procedures at the appropriate times, and generating accurate reports for future reviews.
- **Review, improve and maintain the CSMS**: Ensure the ongoing effectiveness of the CSMS over time.

2.3.6.3. ISA-62443-2-3 – PATCH MANAGEMENT IN THE IACS ENVIRONMENT

ISA-62443-2-3 is tasked with outlining the steps involved in managing patches for industrial automation and control systems (IACS), encompassing all patch types such as security patches, bug fixes, and updates. It also recommends a standardized format for exchanging patch information between asset owners and IACS product suppliers.

2.3.6.4. ISA-62443-2-4 – SECURITY PROGRAM REQUIREMENTS FOR IACS SERVICE PROVIDERS

This portion of ISA-62443 outlines a thorough set of requirements detailing security capabilities that IACS (Industrial Automation and Control System) service providers should possess. These capabilities are intended to be offered to the asset owner during integration and maintenance activities of an Automation Solution.

2.3.6.5. ISA-62443-3-2 – SECURITY RISK ASSESSMENT FOR SYSTEM DESIGN

This section of the standard sets forth specific requirements concerning industrial automation and control systems (IACS).

It offers directives for clearly defining a System Under Consideration (SUC) within an IACS. The standard also establishes procedures for segmenting the defined system into zones and conduits, creating distinct components within the larger system, and then provides guidance on evaluating the risks associated with these zones and conduits, aiding in the identification of potential security vulnerabilities.

It delineates the process of determining a target security level (SL-T) for each zone and conduit, signifying the intended level of security.

Additionally, it underscores the significance of documenting security requirements derived from these assessments, serving as a clear reference for the implementation and maintenance of security measures within the IACS.

2.3.6.6. ISA-62443-3-3 – SYSTEM SECURITY REQUIREMENTS AND SECURITY LEVELS

This section of the standard elucidates on how a project establishes risk-based security levels. The aim is to select products that align with the technical security capabilities outlined within each level with the association of the seven foundational requirements described in IEC 62443-1-1[RD-29].

The seven foundational requirements (FR) for control system capability Security levels (SLs):

1. **Identification and authentication control** (IAC)
2. **Use control** (UC)
3. **System integrity** (SI)
4. **Data confidentiality** (DC)
5. **Restricted data flow** (RDF)
6. **Timely response to events** (TRE)
7. **Resource availability** (RA)

Each foundational requirement is expanded into four Security levels and a set of Security Requirements (SRs). Every SR includes a baseline requirement along with optional requirement enhancements (REs) designed to enhance security further.

The first FR, **Identification and authentication control**, specifying requirements for identification and authentication of users, is composed by the standard four security levels.

Table 9 introduces the security levels of identification and authentication control.

Level	Description
SL 1	Ensure the identification and authentication of all users, including humans, software, and devices, through methods that safeguard against **casual or coincidental** unauthorized access by entities lacking proper authentication.
SL 2	Ensure the identification and authentication of all users, including humans, software, and devices, through methods that safeguard against intentional unauthorized access by entities using **simple** means with **low** resources, skills, and motivation.

Level	Description
SL 3	Ensure the identification and authentication of all users, including humans, software, and devices, through methods that safeguard against intentional unauthorized access by entities using **sophisticated** means with **moderate** resources, motivation, and IACS specific skills.
SL 4	Ensure the identification and authentication of all users, including humans, software, and devices, through methods that safeguard against intentional unauthorized access by entities using **sophisticated** means with **extended** resources, **high** motivation, and IACS specific skills.

Table 9: Identification and authentication control SLs

As for the **system requirements (SR)**, this FR possesses thirteen of them which cover all aspects of identification and authentication of the user, software, and device. The control system shall provide the capability to:

1. **Human user identification and authentication –** provide the capability to identify and authenticate all human users, and on all interfaces that give access to the control system to a human.
2. **Software process and device identification and authentication –** provide the capability to identify and authenticate all software process and devices, and on all interfaces which provide access to the control system.
3. **Account management –** facilitate the management of all accounts through actions such as adding, activating, modifying, disabling, and removing accounts.
4. **Identifier management –** facilitate the management of identifiers by user, group, role, or control system interface.
5. **Authenticator management –** offer the ability to initiate authenticator configuration, modify all default authentication settings during control system installation, update all authenticators, and safeguard them from unauthorized disclosure and alteration during storage and transmission.
6. **Wireless access management –** identify and authenticate all users connected to wireless communications.
7. **Strength of password-based authentication –** ability to identify and authenticate all users, including humans, software processes, or devices, involved in wireless communication.
8. **Public key infrastructure certificates –** operate the public key infrastructure in accordance with accepted best practices at all times or acquire a public key certificate from an existing PKI.
9. **Strength of public key authentication –** validate certificates by either verifying the signature of a given certificate, constructing a certification path to an accepted Certification Authority (CA), checking the revocation status, assigning a user responsible for the corresponding private key, or mapping the authenticated identity to a user.
10. **Authenticator feedback –** obscure feedback of authentication information during the authentication process.
11. **Unsuccessful login attempts –** implement a restriction on the number of consecutive invalid access attempts by any user within a defined time frame. Enable the system to deny access for a specified duration or grant permission to an administrator to unlock access once the maximum number of attempts has been reached.
12. **System use notification –** display a system use notification message before authentication, configurable by authorize personnel.
13. **Access via untrusted networks -** monitor and regulate all access methods to the control system when accessed through untrusted networks.

The **Use Control** FR ensures that authenticated users have the necessary privileges to execute actions on IACS and monitors the utilization of these privileges.

Table 10 introduces the security levels of use control.

Level	Description
SL 1	Limit the utilization of the IACS based on designated privileges to prevent inadvertent or intentional misuse.
SL 2	Limit the utilization of the IACS based on designated privileges to prevent circumvention by entities using **simple** means with **low** resources, motivation, and skills.
SL 3	Limit the utilization of the IACS based on designated privileges to prevent circumvention by entities using **sophisticated** means with **moderate** resources, motivation, and IACS specific skills.
SL 4	Limit the utilization of the IACS based on designated privileges to prevent circumvention by entities using **sophisticated** means with **extended** resources, **high** motivation, and IACS specific skills.

Table 10: Use control SLs

The Use Control FR is composed by twelve security requirements:

- **Authorization enforcement –** on all interfaces, enforce authorizations assigned to all human users to regulate control system usage, thereby supporting the separation of duties and least privilege.
- **Wireless use control –** offer the ability to oversee wireless connections by authorizing, monitoring, and enforcing usage restrictions in accordance with accepted security industry practices.
- **Use control for portable and mobile devices –** provide the capability to automatically apply configurable usage restrictions to prevent the utilization of mobile devices, requiring context-specific authorization and restricting the exchange of code and data between portable and mobile devices.
- **Mobile code –** enforce usage restrictions for mobile code technologies based on the potential to damage the control system.
- **Session lock –** prevent continued access by activating a session lock after a set period of inactivity.
- **Remote session termination –** end a remote session either automatically after a set period of inactivity or at the discretion of the user who initiated the session.
- **Concurrent session control –** Restrict the number of simultaneous sessions per interface for each user to a customizable limit.
- **Auditable events –** generate audit records relevant to security related to access control, errors, events and configuration changes.
- **Audit storage capacity –** must ensure that exist enough space to storage the audit record, according to the recommendations for log management and system configuration.
- **Response to audit processing failures –** if an audit processing fails, it should promptly notify the responsible personnel and prevent the loss of critical services and functions.
- **Timestamps –** use of timestamp when generate audit records.
- **Non-repudiation –** determine the human user responsible for a specific action.

The third foundational requirement, **System integrity**, emphasizes the integrity of the IACS, safeguarding against unauthorized manipulation.

Table 11 introduces the security levels of system integrity.

Level	Description
SL 1	Safeguard the integrity of the IACS from inadvertent or deliberate manipulation.

Level	Description
SL 2	Protect the integrity of the IACS from manipulation by individuals with **limited** resources, motivation, and skills who may employ **simple** methods.
SL 3	Safeguard the integrity of the IACS from manipulation by individuals using **sophisticated** methods with **moderate** resources and motivation and possessing IACS-specific skills.
SL 4	Safeguard the integrity of the IACS from manipulation by individuals using **sophisticated** methods with **extended** resources, **high** motivation and possessing IACS-specific skills.

Table 11: System Integrity SLs

The System integrity FR is composed by nine security requirements, which are:

- **Communication integrity –** ensure data integrity during network data exchange to prevent manipulation.
- **Malicious code protection –** utilize protective mechanisms to prevent, detect, report, and mitigate the impact of malicious code.
- **Security functionality verification –** facilitate the verification of security function and report any anomalies detected during factory acceptance testing, site acceptance testing, and maintenance procedures.
- **Software and information integrity –** offer capabilities to detect, record, report, and safeguard against unauthorized alterations to both software and stored information.
- **Input validation –** analyse both the syntax and content of any input utilized as an industrial process control input or input directly influencing the actions of the control system.
- **Deterministic output –** provide the capability to set outputs to a predefined state if normal operations are disrupted due to a cyberattack.
- **Error handling –** identify and address error conditions in the most efficient remediation manner, while ensuring minimal disclosure of information only when strictly necessary.
- **Session integrity –** the ability to protect the integrity of the sessions, block the invalid ones.
- **Protection of audit information –** protect the audit information and tools from unauthorized access, manipulation and deletion.

Data confidentiality is the fourth fundamental requirement, with the purpose to ensure that data remains confidential on communication channels and in the repository against unauthorized disclosure.

Table 12 introduces the security levels of data confidentiality.

Level	Description
SL 1	Prevent unauthorized disclosure of information through eavesdropping or inadvertent exposure.
SL 2	Prevent unauthorized disclosure of information to an entity conducting active searches using **basic** methods, with **limited** resources, skills, motivation.
SL 3	Prevent unauthorized disclosure of information to an entity conducting active searches using **sophisticated** methods, with **moderate** resources and motivation, and possessing IACS-specific skills.
SL 4	Prevent unauthorized disclosure of information to an entity conducting active searches using **sophisticated** methods, with **extended** resources and **high** motivation, and possessing IACS-specific skills.

Table 12: Data confidentiality SLs

The data confidentiality FR is composed by three security requirements:

- **Information confidentiality –** protect the confidentiality of information.
- **Information persistence –** ability to completely remove all information from components that are being taken out of active service or decommissioned, provided that explicit read authorization is granted for that information.
- **Use of cryptographic –** if necessary, use of cryptographic methods commonly accepted security industry practices and recommendations.

The **Restricted Data Flow** FR, which divides the control system into zones and conduits to restrict unnecessary data flow, constitutes the fifth foundational requirement.

Table 13 introduces the security levels of restricted data flow.

Level	Description
SL 1	Prevent the inadvertent or coincidental bypassing of zone and conduit segmentation.
SL 2	Prevent intentional circumvention of zone and conduit segmentation by entities employing **basic** methods, with **limited** resources, skills, and motivation.
SL 3	Prevent intentional circumvention of zone and conduit segmentation by entities employing **sophisticated** methods, possessing **moderate** resources and motivation, skills related to IACS.
SL 4	Prevent intentional circumvention of zone and conduit segmentation by entities employing **sophisticated** methods, possessing **extended** resources **high** and motivation, skills related to IACS.

Table 13: Restricted data flow SLs

The Restricted Data Flow FR has four security requirements:

- **Network segmentation –** logically divide control system networks from non-control system networks and further segment critical control system networks from other control system networks.
- **Zone boundary protection –** ability to monitor and regulate (routers, firewalls, encrypted tunnels, among others) communications at zone boundaries to uphold the compartmentalization outlined in the risk-based zones and conduits model.
- **General purpose person-to-person communication restrictions –** prevent the reception of general-purpose messages originating from users or systems external to the control system (like X, Facebook, email systems, etc.).
- **Application partitioning –** Enable the establishment of a zoning model by partitioning data, applications, and services according to their criticality.

The sixth foundational requirement, **Timely Response to Events**, involves promptly notifying the relevant authorities in the event of a security breach, providing necessary evidence of the breach, and implementing corrective actions upon identifying incidents in a timely manner.

Table 14 introduces the security levels of timely response to events.

Level	Description
SL 1	Monitor the operation of the IACS and respond to incidents promptly by collecting and furnishing forensic evidence **upon request**.
SL 2	Monitor the operation of the IACS and respond to incidents promptly by **actively** collecting and **periodically** reporting forensic evidence.
SL 3	Monitor the operation of the IACS and respond to incidents promptly by **actively** collecting and **transmitting** forensic evidence to the appropriate authority.
SL 4	Monitor the operation of the IACS and respond to incidents promptly by **actively** collecting and **transmitting** forensic evidence to the appropriate authority in **near real-time**.

Table 14: Timely response to events SLs

The sole security requirement, **Audit Log Accessibility**, enables the control system to grant read-only access permissions to users or tools for accessing audit logs.

The final foundational requirement, **Resource Availability**, ensures the control system's availability is safeguarded against denial-of-service attacks.

Table 15 introduces the security levels of resource availability.

Level	Description
SL 1	Ensure the reliable operation of the control system under normal production conditions and prevent Denial of Service (DoS) situations caused by the inadvertent or coincidental actions of an entity.
SL 2	Ensure the dependable operation of the control system under both normal and abnormal production conditions and prevent Denial of Service (DoS) situations caused by entities employing **simple** means with **low** resources, motivations and skills.
SL 3	Ensure the dependable operation of the control system under both normal and abnormal production conditions and prevent Denial of Service (DoS) situations caused by entities employing **sophisticated** means with **moderate** resources and motivations, with IACS skills.
SL 4	Ensure the dependable operation of the control system under both normal and abnormal production conditions and prevent Denial of Service (DoS) situations caused by entities employing **sophisticated** means with **extended** resources and **high** motivations, with IACS skills.

Table 15: Resource availability SLs

To support this FR, eight security requirements, to ensure that the control system is resilient to denial-of-service attacks, are defined:

- **Denial of service protection –** capability to the control system operate under a denial-of-service attack.
- **Resource management –** restrict the utilization of resources by security functions to avoid resource depletion.
- **Control system backup –** identify and locate critical files and information for backup purposes without impacting system performance.
- **Control system recovery and reconstitution –** capability to recover to a secure state after a disruption or failure event.
- **Emergency power –** capability to manage the power supply in case of emergency, without put in risk the secure state or documented degraded mode.
- **Network and security configuration settings –** set up the control system via an interface, adhering to recommended network security configurations.
- **Least functionality –** ability to forbid or restrict some functionalities (functions, ports, protocols, or services) to guarantee support to the essential ones, in case of some disruption event.
- **Control system component inventory –** provide a list to all installed components and their properties.

2.3.6.7. ISA-62443-4-1 – SECURE PRODUCT DEVELOPMENT LIFECYCLE REQUIREMENTS

This section of the standard outlines a comprehensive framework for securing the development lifecycle of IACS products. It emphasizes a "secure by design" and "defence-in-depth" approach, ensuring robust security throughout the product's life cycle.

The key objectives of this part of the ISA 62443 are as follow:

- **Confidence in Security**: The framework establishes a process that builds confidence in the product's security, ensuring it aligns with its expected risk level.
- **Correct Implementation**: It ensures the proper implementation of security capabilities defined in IEC 62443-4-2 and eliminate or mitigates known vulnerabilities.
- **Meeting Overall Security Level**: Compliance supports achieving the overall capability security level (SL-C) of the product.
- **Alignment with User Needs**: The development process addresses the heightened security requirements of IACS users by producing well-documented items and establishing security configuration and patch management policies and procedures. Additionally, it ensures clear communication regarding any security vulnerabilities discovered in the product.

This framework applies to the development and maintenance of all hardware, software, and firmware used in IACS, regardless of whether they are new creations or updates to existing products.

Figure 4 illustrates how the practices should be implemented to contribute to a defence-in-depth strategy.

Figure 4: Defence-in-depth strategy

Security management forms the foundation of all other security practices. It ensures that activities related to product security are planned, documented, and executed throughout the entire product lifecycle. This comprehensive approach focuses on five key practices within the inner mid-circle:

1. **Specification of Security Requirements**: This practice involves documenting the security capabilities a product needs (e.g., authentication, encryption, auditing). These capabilities are defined based on the product's security context, which includes factors like physical security level and firewall configurations.
2. **Secure by Design**: This practice aims to build resilience into the product from the very beginning. By incorporating multiple layers of defense throughout the design process, from concept to individual components, the product is better equipped to resist attacks.

3. **Secure Implementation**: This practice ensures that all features are implemented with security in mind. Secure coding practices, secure configuration management, and other security controls are essential elements of this process.
4. **Security Verification and Validation**: This practice complements secure implementation by documenting the results of all security testing activities. This testing verifies if the security requirements are being met and ensures the product functions securely in real-world scenarios. Common testing methods include static code analysis, penetration testing, and vulnerability scanning.
5. **Security Guidelines**: This practice provides user documentation that guides them on how to integrate, configure, and maintain the product's defense-in-depth strategy. By following these guidelines, users can ensure they are using the product securely to protect assets and operations.

By implementing all these practices, organizations can build a robust defence-in-depth strategy for their products. This layered approach helps to ensure that assets and business operations are well-protected, even if an attacker breaches one layer of defence.

2.3.6.8. ISA-62443-4-2 – TECHNICAL SECURITY REQUIREMENTS FOR IACS COMPONENTS

The last section of this standard focuses on aligning the technical requirements of control system **components** with the seven foundational requirements (FR) introduced earlier in the ISA-62443-3-3 section. These foundational requirements define the characteristics of a control system with robust security capabilities.

The first FR, **Identification and authentication control**, specifying requirements for identification and authentication of users, is composed by the standard four security levels, discuss in 2.3.6.6.

As for the **component's requirements (CR)**, this FR possesses fourteen of them which cover all aspects of identification and authentication of the user, software, and device. The component shall provide the capability to:

1. **Human user identification and authentication –** provide the capability to identify and authenticate all human users, and on all interfaces that give access to the control system to a human in accordance with IEC 62443-3-3 SR 1.1.
2. **Software process and device identification and authentication –** provide the capability to identify and authenticate other component (software application, embedded devices, host devices and network devices) in accordance with IEC 62443-3-3 SR 1.2.
3. **Account management –** facilitate the management of all accounts directly or integrated into a system responsible for managing accounts in accordance with IEC 62443-3-3 SR 1.3.
4. **Identifier management –** integrate into a system that supports management of identifiers and/or support the management directly in accordance with IEC 62443-3-3 SR 1.4.
5. **Authenticator management –** Component shall offer support to:
    a. **Supporting the Use of Authenticator Content**: Providing guidance and tools to users on how to correctly utilize the information contained within the authenticator.
    b. **Recognizing Changes to Authentication Settings**: Ensuring the system can detect and handle alterations to default authentication settings during installation.
    c. **Maintaining Functionality During Authenticator Updates**: Maintaining uninterrupted functionality throughout the process of periodic authenticator changes or refreshes.
    d. **Safeguarding Authenticators from Unauthorized Access**: Implementing security measures to safeguard authenticator content from unauthorized disclosure and alteration during storage, use, and transmission.
6. **Wireless access management –** Identify and authenticate all users, devices, and software processes connected to wireless communications.
7. **Strength of password-based authentication –** for components that use password-based authentication, the capability to enforce strong password policies shall be built-in or the component shall integrate with a system that enforces strong password policies. These policies should adhere to well-established international password guidelines.

8. **Public key infrastructure certificates –**when using a public key infrastructure (PKI), the component shall provide or integrate into a system that provides the capability to interact and operate in accordance with IEC 62443-3-3 SR 1.8.
9. **Strength of public key-based authentication –** Components that use public key-based authentication within the IACS environment shall provide directly or integrate with a system that provides the following capabilities:
    a. **Certificate Validation**: Verify the authenticity of a certificate by checking the signature of a given certificate against the public key of the issuing Certificate Authority (CA).
    b. **Certificate Chain Validation**: Validate the chain of certificates signed by trusted CAs. In the case of self-signed certificates, verify the deployment of leaf certificates on all relevant hosts.
    c. **Certificate Revocation Checking**: Verify the revocation status of a certificate to ensure it has not been compromised and is still considered valid.
    d. **Private Key User Control**: Establish and maintain user control (human, software process, or device) over the corresponding private key.
    e. **Identity Mapping**: Map the authenticated identity obtained from the certificate to a user within the IACS environment.
    f. **Cryptographic Standards Compliance**: Ensure that the cryptographic algorithms and public keys used conform to well-established international security practices and recommendations.
10. **Authenticator feedback –** In case of the component provide an authentication capability, the component shall obscure feedback of authentication information during the authentication process.
11. **Unsuccessful login attempts –** In case of the component provide an authentication capability, the component shall:
    a. Implement a restriction on the number of consecutive invalid access attempts by any user within a defined time frame.
    b. Enable the system to deny access for a specified duration or grant permission to an administrator to unlock access once the maximum number of attempts has been reached.
12. **System use notification –** If a component offers local human user access, it shall enable the display of a system use notification message before authentication. This message should be configurable by authorized personnel.
13. **Access via untrusted networks –** The requirements for access via untrusted networks are component-specific. A series of these requirements can be found for each component type in Clauses 12 through 15 of the standard.
14. **Strength of symmetric key-based authentication** - Components that utilize symmetric key-based authentication shall meet the following requirements:
    a. **Mutual Trust Establishment**: Enable the establishment of mutual trust through symmetric key-based authentication.
    b. **Secure Key Storage**: Store symmetric keys in a well-secured and confidential location.
    c. **Restricted Key Access**: Implement mechanisms to restrict access to the symmetric keys, ensuring only authorized entities can access them.
    d. **Cryptographic Standards Compliance**: Ensure the cryptographic algorithms and keys used for symmetric encryption conform to well-established international security practices and recommendations.

The **Use Control** FR ensures that authenticated users have the necessary privileges to execute actions on IACS and monitors the utilization of these privileges.

The Use Control FR is composed by eleven component requirements:

1. **Authorization enforcement –** component shall provide an authorization enforcement mechanism for all identified and authenticated users based on their roles.
2. **Wireless use control –** component that support usage through wireless interface, shall offer the ability to oversee wireless connections by authorizing, monitoring, and enforcing usage restrictions in accordance with accepted security industry practices.
3. **Mobile code –** The requirements for use control for mobile code are component-specific. A series of these requirements can be found for each component type in Clauses 12 through 15 of the standard.
4. **Session lock –** If the component provides a human user interface, the component shall:
    a. Protect against access by initiating a session lock after a set period of inactivity or by manual initiation by a user.
    b. Session lock must remain until a user human that owns a session re-establishes access using appropriate identification and authentication procedures.
5. **Remote session termination –** In case a component supports remote sessions, the component shall end a remote session either automatically after a set period of inactivity or at the discretion of the user who initiated the session.
6. **Concurrent session control –** Restrict the number of simultaneous sessions per interface for each user to a customizable limit.
7. **Auditable events –** generate audit records relevant to security related to access control, errors, events and configuration changes.
8. **Audit storage capacity –** must ensure sufficient space to store audit records, according to the recommendations for log management and system configuration and provide component redundancy in case of failure at maximum capacity.
9. **Response to audit processing failures –** prevent the loss of critical services and functions due to audit processing failures. If an audit processing failure occurs, the component should promptly take corrective actions according to well-established international industry practices and recommendations.
10. **Timestamps –** create timestamp when using audit records.
11. **Non-repudiation –** If the component provides a human user interface, the component must determine the human user responsible for a specific action.

The third foundational requirement, **System integrity**, emphasizes the integrity of the IACS, safeguarding against unauthorized manipulation.

The System integrity FR is composed by nine component requirements:

1. **Communication integrity –** Ensure data integrity during network data exchange to prevent manipulation.
2. **Malicious code protection –** The requirements for malicious code protection are component-specific. A series of these requirements can be found for each component type in Clauses 12 through 15 of the standard.
3. **Security functionality verification –** Offer capabilities to verify of the intended operation of security functions according to IEC 62443-3-3 SR 3.3.
4. **Software and information integrity –** Components shall offer the following capabilities:
    a. **Perform or Support Integrity Checks:** The component should provide mechanisms to perform integrity checks on software, configuration data, and other relevant information.
    b. **Record and Report Check Results:** The component should support recording and reporting the results of these integrity checks. This allows for easier monitoring and analysis of potential security issues.

5. **Input validation –** Analyse both the syntax and content of any input utilized as an industrial process control input or input directly influencing the actions of component.
6. **Deterministic output –** Components interacting with the automation process (either physically or logically) shall provide the capability to enter a predefined safe state if normal operations cannot be maintained.
7. **Error handling –** Identify and address error conditions in the most efficient remediation manner, while ensuring minimal disclosure of information only when strictly necessary.
8. **Session integrity –** the ability to protect the integrity of the sessions, including:
   a. Invalidate sessions upon user logout or session termination.
   b. Generate unique session identifier for each session, and only recognize those who are system-generated.
   c. Generate session identifiers with accepted sources of randomness.
9. **Protection of audit information –** Protect the audit information and tools from unauthorized access, manipulation, and deletion.

Data confidentiality is the fourth fundamental requirement, with the purpose to ensure that data remains confidential on communication channels and in the repository against unauthorized disclosure.

The data confidentiality FR is composed by three component requirements:

1. **Information confidentiality –** protect the confidentiality of information in rest and in transit as defines in IEC 62443-3-3 SR 4.1.
2. **Information persistence –** ability to completely remove all information from components that are being taken out of active service or decommissioned, provided that explicit read authorization is granted for that information.
3. **Use of cryptographic –** if necessary, components shall use of cryptographic methods commonly accepted security industry practices and recommendations.

The **Restricted Data Flow** FR, which divides the control system into zones and conduits to restrict unnecessary data flow, constitutes the fifth foundational requirement.

The Restricted Data Flow FR has three component requirements:

1. **Network segmentation –** Support network segmentation with zone and conduit enforcement.
2. **Zone boundary protection –** The requirements for zone boundary protection are network-component-specific. A series of these requirements can be found for each component type in Clause 15 of the standard.
3. **General purpose person-to-person communication restrictions –** The requirements for general purpose person-to-person communication restrictions are network-component-specific. A series of these requirements can be found for each component type in Clause 15 of the standard.

The sixth foundational requirement, **Timely Response to Events**, involves promptly notifying the relevant authorities in the event of a security breach, providing necessary evidence of the breach, and implementing corrective actions upon identifying incidents in a timely manner.

The **Timely Response to Events** FR has two component requirements:

1. **Audit Log Accessibility** - Enables the control system to grant read-only access permissions to users or tools for accessing audit logs.
2. **Continuous Monitoring** – Continuing monitoring using commonly accepted security industry practices and recommendations to detect, characterize and report security breaches.

The final foundational requirement, **Resource Availability**, ensures the control system's availability is safeguarded against denial-of-service attacks.

To support this FR, eight component requirements, to ensure that the control system is resilient to denial-of-service attacks, are defined:

1. **Denial of service protection –** capability to the component operate under a denial-of-service attack.
2. **Resource management –** restrict the utilization of resources by security functions to avoid resource depletion.
3. **Control system backup –** identify and locate critical files and information for backup purposes without impacting system performance.
4. **Control system recovery and reconstitution –** capability to recover to a secure state after a disruption or failure event.
5. **Emergency power –** capability to manage the power supply in case of emergency, without put in risk the secure state or documented degraded mode.
6. **Network and security configuration settings –** set up the component via an interface, adhering to recommended network security configurations.
7. **Least functionality –** ability to forbid or restrict some functionalities (functions, ports, protocols, or services) to guarantee support to the essential ones, in case of some disruption event.
8. **Control system component inventory** – Component shall provide support to a control system component inventory according to IEC 62443-3-3 SR 7.8.

2.3.7. IEC 62645 – NUCLEAR POWER PLANTS – INSTRUMENTATION, CONTROL AND ELECTRICAL POWER SYSTEMS – CYBERSECURITY REQUIREMENTS

This standard is used by the nuclear sector with the premise of establishes cybersecurity requirements needed to prevent and/or mitigate the impact of a cyber-attack against the digital Instrumentation and Control systems [RD-30]. The scope encompasses any unsafe situation, human errors or malicious acts, equipment damage, plant performance degradation that may arise from such actions, including:

- Malicious modifications that compromise system integrity.
- Malicious interference with information, data, or resources that could hinder the delivery or performance of essential I&C programmable digital functions.
- Malicious interference with information, data, or resources that could jeopardize operator displays or lead to loss of I&C programmable digital systems control.
- Malicious changes to hardware, firmware, or software at the programmable logic controller level.

Fundamentally, IEC 62645 is structured into three main sections, namely Programme level, System level, and Security thematic areas, as depicted in Figure 5.

Formatted: Not Highlight

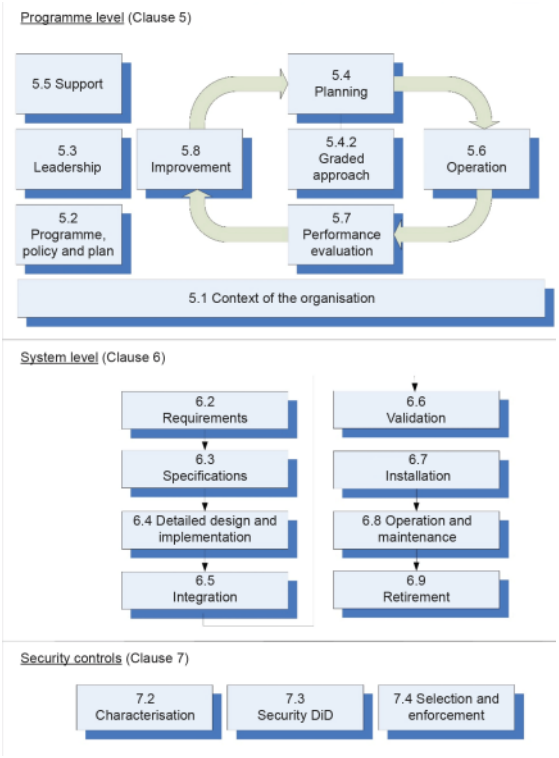

Figure 5: Overall Structure of the IEC 62645 [RD-30]

Formatted: Not Highlight

The first block addresses the overarching program, adopting a structured approach based on the Plan-Do-Check-Act (PDCA) cyclical model. This aligns with the current best practices in cybersecurity management at the international level, as reflected in **ISO/IEC 27001**.

The second block concentrates on the lifecycle of I&C systems, outlining requirements and recommendations across nine distinct phases, commencing with the "Requirement phase" and culminating in the "Retirement phase".

The third block delves into cybersecurity at the security control level, presenting overarching principles that align with the **ISO/IEC 27002**.

2.4. NATIONAL AERONAUTICS AND SPACE ADMINISTRATION (NASA)

NASA is the most recognizable agency around the world, known for its achievements and technological breakthroughs. Its most significant accomplishment was putting the first humans on the Earth's moon using the most powerful rocket at the time, the Saturn V.

Times have changed, and so has technology. In the past, security focused on ensuring that technology, especially hardware, was secure from unwanted access. However, with the digitalization of everything, this approach is no longer feasible.

Therefore, the Office of the NASA Chief Engineer created the NASA Technical Standards System branch with the primary focus of establishing standards for systems and cybersecurity to safeguard those systems.

2.4.1. NASA-STD-1006A – SPACE SYSTEM PROTECTION STANDARD

The main objective of this standard is to establish protection requirements throughout the whole agency, ensuring that all missions, programs and projects are resilient to cyber threats. Supporting this standard are others like NASA Procedural Requirements (NPR) 1058.1, NASA Enterprise Protection Program, NPR 7120.5, NASA Space Flight Program and Project Management, NPR 7120.8, NASA Research and Technology Program and finally Project Management Requirements [RD-31].

This standard contains three objectives, each with its own set of requirements to ensure compliance. These objectives will be organized into the following subsections.

2.4.1.1. MAINTAIN COMMAND AUTHORITY

The premise to this objective is to guarantee command authority all the time, to avoid unauthorized access and to ensure data integrity.

Supporting that end, it has three space system protection requirements (SSPR), as depicted in Table 16.

SSPR	Description
Command Stack Protection	All programs/projects that meet or exceed the FIPS 140 (Level 1) shall protect the command stack using encryption, to avoid incidents that potentially impacts operations.
Backup Command Link Protection	If a project utilize encryption in their primary command link, all backups of that link, at least, must have authentication ensuring the ability to recover from an anomalous condition.
Command Link Critical Program/Project Information (CPI)	All programs/projects shall protect the confidentiality of command link CPI as controlled unclassified information to prevent any leaks of sensitive information to third parties.

Table 16: SSPR for Maintain Command Authority

2.4.1.2. ENSURE POSITIONING, NAVIGATION, AND TIMING (PNT) RESILIENCE

All missions that depend on external positioning, navigation and timing services must be able to recognize each other and survive any type of interference, so that their missions and objectives are not in danger of total failure.

To make this objective possible, all projects must adhere to the only required SSPR, depicted in Table 17.

SSPR	Description
Ensure Positioning, Navigation, And Timing (PNT) Resilience	If projects depend on externa PNT, must ensure all systems are resilient to complete loss or temporary interference, with the external PNT services.

Table 17: SSPR for Ensure PNT Resilience

2.4.1.3. REPORT UNEXPLAINED INTERFERENCE

Missions must be equipped to detect and report unexpected interferences to the agency, making them aware of what transpired in space and enabling them to build solutions to mitigate the effects of those interferences.

The following two space system protection requirements is presented in Table 18.

SSPR	Description
Interference Reporting	Projects, spectrum managers or operations centres must have the responsibility to report any unexplained interference to Mission Resilience and Protection Program or to other designated organization.
Interference Reporting Training	Projects, spectrum managers or operations centres shall conduct training for reporting unexplained interference, to avoid incidents of miss such events, putting the mission endanger.

Table 18: SSPR for Report Unexplained Interference

2.4.2. NASA-STD-8739.8B – SOFTWARE ASSURANCE AND SOFTWARE SAFETY

The purpose of the document is to define requirements for implementing a systematic approach to independent assurance, safety, verification, and validation for software created, acquired, provided, used, or maintained by or for NASA.

The “Software Assurance” and “Software Safety Standard, in accordance with “NPR 7150.2”.

This standard is focused more on safety, but it also contains a section of requirements that also focuses on cybersecurity that a **project engineer** shall follow [RD-34].

Table 19 presents the cybersecurity requirements.

NPR 7150.2 Section	NPR 7150.2 Requirement
3.11.2	The project manager **must perform a cybersecurity software assessment** on software components, complying with Agency security policies and project requirements, including risks from using COTS (Commercial-Off-The-Shelf), GOTS (Government-Off-The-Shelf), MOTS (Modified-Off-The-Shelf), OSS (Open-Source Software), or reused software components.
3.11.3	The project manager **must identify cybersecurity risks**, along **with their mitigations**, in ground or flight systems and plan mitigations for those systems.
3.11.4	The project manager **must implement protections for software systems using communications** against unauthorized access, in accordance with the requirements listed in the “Space System Protection” standard (**NASA-STD-1006**).
3.11.5	The project manager **must test the software and document the results** for the necessary cybersecurity mitigation implementations identified by the vulnerability analysis and security weaknesses.
3.11.6	The project manager **must identify, document, and implement safe programming practices.**
3.11.7	The project manager **must check whether the software code meets the standards of safe programming practices**, using the results of the analysis carried out by static tools.
3.11.8	The project manager **must identify the software requirements for collecting, documenting and storing data** related to adverse action detection.

Table 19: Cybersecurity requirements for a project engineer

2.4.3. NPD 2810.1F NASA INFORMATION SECURITY POLICY

This NASA policy directive focuses on protecting both classified and unclassified information. This policy aims to achieve several key objectives [RD-32]:

- **Protect All Information Assets**: Secure both classified and unclassified information and information systems at all levels based on a comprehensive assessment of sensitivity, value, and criticality.

- **Leverage NIST Standards**: Follow the guidance provided in NIST Special Publication 800 series for computer security policies, procedures, and guidelines.
- **Integrate Security Throughout the Lifecycle**: Incorporate information security considerations throughout the entire system lifecycle, prioritizing the protection of information and information systems.
- **Manage Cybersecurity for NASA Systems**: Manage the cybersecurity of all information systems (classified and unclassified) used to support NASA missions, projects, and partnerships across their entire lifecycle.
- **Implement Risk Management**: Implement and maintain a comprehensive risk management and cybersecurity process.
- **Ensure Compliance**: Conduct regular monitoring and reviews of information systems to ensure compliance with relevant laws and policies.
- **Learn from Incidents**: Investigate past security incidents and develop comprehensive after-action reports following significant events. These reports should address identified issues and guide improvements in future response efforts.
- **Standardize Security Practices**: Ensure consistent implementation of information security policy requirements, audits, and forensic investigations across all NASA centres and contracts.
- **Implement Best Practices**: Integrate cybersecurity policy best practices and guidance into NASA's security posture.
- **Secure Software Assets**: Ensure that all software supporting NASA missions, programs, projects, and information systems is developed, procured, and maintained with security in mind.
- **Authorize Information Systems**: Guarantee that all information systems (classified and unclassified) operate under valid authorizations granted by an Authorizing Official following the established Assessment and Authorization process.

To achieve those key objectives, it assigns some responsibilities to key personnel, as show in Table 20.

NASA Key Personnel	Responsibilities
Administrator	•Implement information security controls that align with the potential risks and severity of impacts associated with unauthorized access, use, disclosure, disruption, modification, or destruction of information. •Ensure all information systems comply with the requirements of FISMA (Federal Information Security Management Act) and other relevant federal laws. •Integrate information security management processes into NASA's strategic and operational planning processes to ensure a holistic approach to security.
CIO	•Enforce Security Compliance: Ensure consistent compliance with all applicable information security requirements. •Develop and Maintain Security Program: Implement a comprehensive information security program that incorporates cybersecurity policies and procedures. •Protect Unclassified Information: Develop and maintain effective information security policies and procedures to safeguard unclassified information.
Assistant Administrator for Office of the Chief Information Officer (OPS)	•Supports the NASA CIO in establishing a security program aligned with NPD 1600.2, the NASA Security Policy. •Ensures that OPS fulfils its responsibilities regarding Identity, Credential, and Access Management (ICAM) as outlined in NPR 2841.1. •Develops and implements insider threat program processes and procedures that support information security objectives.
Officials in charge of Mission Directorates and Mission Support Offices	•In conjunction with NASA CIO and Assistant Administrator for OPS, develop information security policies, standards, best practices and guidance that protects both information and information systems. •Conduct thorough information security risk management planning and design to facilitate effective cost-benefit analysis of alternative security postures and risk acceptance decisions. •Throughout the system lifecycle, from design, development, testing, and evaluation to decommissioning, apply security policies and requirements aligned with sound systems engineering

NASA Key Personnel	Responsibilities
	practices and prudent risk management. This includes encryption for embedded software and other embedded IT components.
Senior Agency Information Security Officer	•Implements the Agency CIO's information security directives. •Leads the development and management of the Agency Cybersecurity and Privacy Program, including associated performance metrics. •Maintains a dedicated office responsible for information security operations, cybersecurity governance, architecture and engineering, and threat analysis. This office supports Agency compliance with federal information security laws, directives, policies, standards, and guidelines.
Center Directors and the Director for Headquarters Operations	•Ensure compliance with the NPD 2810.1F, NASA policies, procedures, requirements, and the Federal information security policies for activities under their purview. •These policies and requirements, aligned with sound systems engineering and prudent risk management practices, shall be applied throughout the entire system lifecycle for encryption, embedded software, and other embedded IT components. This includes all phases from design, development, testing, and evaluation to decommissioning.
Center CIOs and the Headquarters CIO	•Protect both information and information systems under their purview and follow NASA information security policies, procedures, and Federal information security laws, directives, policies and standards.
Center Chief Information Security Officer	•Ensures the successful implementation of information security policies throughout their Center. •In collaboration with the SAISO and Center CIO, this office will provide the necessary resources to implement this directive. This includes enforcing the NASA Cybersecurity and Privacy Program, along with adherence to federal information security laws, directives, standards, and applicable guidelines. •Provides the primary channel for information exchange between SAISO and Center information security functions.
Users	•Follow to all NASA information security policies, processes, and procedures

Table 20: NASA personnel and their responsibilities (summary)

2.4.4. NPR 2810.7 SECURITY OF INFORMATION TECHNOLOGY

NASA Information Security Policy Directive [RD-33] establishes information security requirements and responsibilities for NASA, aligning with the NASA Information Security Policy (NPD 2810.1) [RD-33].

The document is organized into six chapters following the NIST Cybersecurity Framework (CSF) v1.1 functional areas:

- Identify
- Protect
- Detect
- Respond
- Recover

The **Identify function** is the first step in securing an organization against cyberattacks. It focuses on proactively managing risks to systems, people, assets, and data that could be exploited by malicious actors (threat actors). This function covers a comprehensive range of topics, including asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management, and appoint requirements and process to secure information. Table 21 presents examples of requirements and procedures to each topic.

Topics	Description	Requirements
Asset Management	Identifying and managing data, devices, systems, and facilities to meet information security objectives,	•Ensure maintenance of an information system inventory in the system of record. •Ensure that all information system components are identified and well documented. •Develop and maintain a cybersecurity and privacy program.

Topics	Description	Requirements
	considering risk profile and risk posture.	
Business Environment	Define information security roles, responsibilities, and risk management processes.	•Work with internal and external stakeholders to identify and communicate their roles within the supply chain to inform Supply Chain Risk Management (SCRM). •Lead Center-wide contingency planning for information systems. These plans should address notification, activation, response, recovery, and reconstitution procedures in the event of disruptions caused by natural or man-made disasters. •Develop and maintain Agency-level information system contingency planning policies, procedures, and guidance for NASA, coordinating with OPS for alignment.
Governance	Develop policies, procedures, and processes for managing and monitoring NASA's information security posture, encompassing regulatory, legal, and risk considerations.	•Develop and document a comprehensive Cybersecurity and Privacy Program, that cover topics of measures of performance, enterprise information security architecture, critical infrastructure, risk management strategy, and an information security assessment and authorization process. •Oversee the implementation of the NASA Cybersecurity and Privacy Program plan, policy, and requirements. •Develop and maintain a System Security Plan for information systems.
Risk Assessment	Assessment of cybersecurity risks and their potential impact on NASA's operations, assets, and individuals	•Identify and manage common cybersecurity threats. •Perform system-wide security assessments. •Verify the appropriate application of information system categorization criteria and requirements for organizations.
Risk Management Strategy	Essential requirements for a successful cybersecurity risk management strategy.	Develop and implement a Cybersecurity Risk Management Strategy, including: •Risk management priorities and constraints for assets, missions and systems. •Documentation criteria as a basis for determine risk tolerance and assumptions. •Accurate and timely assessments of threat likelihood and consequence severity are crucial for effective information security.
Supply Chain Risk Management	Defines essential criteria for effective Supply Chain Risk Management	•Conduct cyber supply chain risk assessments to identify, prioritize, and assess risks from information system suppliers and third-party partners. •Contracts with suppliers and third-party partners shall require them to implement measures designed to meet the objectives of this directive and comply with the Cyber SCRM process. •Suppliers and third-party partners undergo routine assessments, including audits, test results, or other evaluations, to verify compliance with their contractual obligations.

Table 21: Identify Functional Requirements

The **Protect function** prioritizes implementing appropriate safeguards to ensure the continued operability of critical infrastructure services during a cyber event. This function encompasses a comprehensive set of topics, starting with identify management and access control, awareness and training, data security, information protection processes and procedures, maintenance, and protective technology. Table 22 presents examples of requirements and procedures to each topic.

Topics	Description	Requirements
Identity Management and Access Control	Establishes requirements for identity management and access control to	•Enforce strict controls to ensure only authorized and approved devices can access the information system remotely. •All public-facing login services must be secured by multi-factor authentication.

Topics	Description	Requirements
	ensure only authorized users can access NASA systems and information.	•Implement a "deny by default, permit by exception" configuration for all network ports, protocols, and services on all systems.
Awareness and Training	Establishes information security awareness and training requirements to ensure that NASA personnel and partners possess the necessary knowledge and skills to perform their cybersecurity-related duties and responsibilities, aligning with NASA policies, procedures, and agreements.	•Develop and deliver information security awareness training programs •Develop educational courses and materials. •Grant access to information systems only to users who have completed all Agency information security awareness and training requirements.
Data Security	Establishes data security requirements to ensure information and records are managed in accordance with NASA's risk management policies and procedures. This safeguards the confidentiality, integrity, and availability of information.	•Ensure that stationary and in transit data are protected by encryption in accordance with NIST approve algorithms. •Implements and maintains robust data leakage protection mechanisms for the Agency's common systems and communications infrastructure. •Enforce shared resource policies, denial-of-service protections, boundary protection, and measures for transmission integrity and confidentiality.
Information Protection Processes and Procedures	Establishes security controls, processes, and procedures to manage the protection of information systems and assets.	•Develop and manage processes for the creation, approval, distribution, and verification of information security configuration baselines. •Back up user-level and system-level information. •Ensure that necessary equipment and services are in place to facilitate thorough media sanitization and data destruction.
Maintenance	Requirements related to the maintenance and repair (including remote) of information systems.	•Implement and maintain a risk-based maintenance program. •Ensure that all maintenance activities performed on their system are documented and logged. •Oversee authorized information system maintenance personnel.
Protective Technology	Requirements for Managing Technical Information Security Solutions to ensure cyber resilience of systems and assets.	•Develop and maintain information system logs. •Ensure audit logs protection from tempering and data leak, throughout the life cycle of the log entry (creation, transmission, aggregation, reduction, analysis, storage, and disposal). •Ensure that sensitive data are protected by encryption in accordance with NIST approve algorithms.

Table 22: Protect Functional Requirements

Following the implementation of protective safeguards, the **Detect function** comes into play. This function focuses on actively identifying and responding to ongoing cyber events. It achieves this through a comprehensive approach that encompasses anomalies and events, security continuous monitoring, and detection processes. Table 23 presents examples of requirements and procedures to each topic.

Topics	Description	Requirements
Anomalies and Events	Requirements and processes for detecting and analysing anomalous activity.	•Implement capabilities to detect anomalous events on information systems and networks. •Develop documented procedures for detecting, analysing, and responding to anomalous events. •Define event containment and remediation strategies to minimize the potential impact on information systems.
Security Continuous Monitoring	Requirements for continuous monitoring of information systems.	•Develop and implement strategies for continuous monitoring of information systems.

Topics	Description	Requirements
		•Establish clear guidelines for approve and use cybersecurity monitoring tools. •Periodically evaluate and authorize the use of vulnerability scanning tools.
Detection Processes	Requirements for detection process and procedures.	•Implement detection processes and procedures that adhere to all relevant requirements (e.g. law, regulations, NPDs and NPRs). •Implement a continuous improvement program for testing and refining detection processes and procedures.

Table 23: Detect Functional Requirements

The **Respond function** springs into action upon the detection of a cyber event. Its primary focus is on executing activities to contain and minimize the potential damage caused by the attack. It achieves this through a well-defined response plan that addresses various aspects, including asset management, business environment, governance, risk assessment, risk management strategy and supply chain risk management, and appoint requirements and process to secure information. Table 24 presents examples of requirements and procedures to each topic.

Topics	Description	Requirements
Respond Planning	Requirements for effective cyber incident response processes and procedures.	•Establish and Manage a Security Operations Center (SOC). •Appoint an Agency Incident Response Manager for cybersecurity incidents. •Develop and maintain a comprehensive Incident Response Plan.
Communications	Defines requirements for incident response communication and coordination	•Establish mechanisms to facilitate coordination with internal and external stakeholders. •Collaborate with law enforcement and intelligence agencies on investigations into information security incidents related to criminal activity, counterintelligence, or counterterrorism. •Report all suspected or actual information security incidents to the SOC immediately, following the guidelines outlined in the incident response and management handbook(s).
Analysis	Analytical requirements for effective response and recovery activities.	•The Incident Response Plan shall incorporate dedicated procedures for analysing information security incidents
Mitigation	Requirements for incident response activities to stop the expansion of a cyber event, mitigate its effects, and solve it.	•The Incident Response Plan shall incorporate elements specifically designed to contain and mitigate information security incidents.
Improvements	Requirements for improving the overall response to cyberattacks, including detection and associated activities.	•Incorporate lessons learned from past information security incidents into the Incident Response Plan.

Table 24: Respond Functional Requirements

The **Recovery function** represents the culmination of all prior efforts. It focuses on restoring normal operations to capabilities or services impacted by a cyberattack. This critical function ensures the organization's resilience by implementing pre-defined recovery plans. It achieves this through a comprehensive approach that encompasses recovery planning, improvements, and communications. Table 25 presents examples of requirements and procedures to each topic.

Topics	Description	Requirements
Recovery Planning	Requirements for incident recovery processes and procedures	• Develop and maintain a comprehensive Incident Recovery Plan that incorporates lessons learned from incident response activities to continuously improve its effectiveness.
Improvements	Requirements for enhancing incident recovery capabilities	•Integrate lessons learned from current and prior incidents into the Incident Recovery Plan.
Communications	Communication requirements for recovery from a cyber incident.	•Public relations strategy to rebuild trust. •Communication procedures for internal and external stakeholders, including executives and management

Table 25: Recovery Functional Requirements

2.5. European Space Agency (ESA)

The European Space Agency objectives are to develop the space capability of the European members and from that share benefits to the citizens of the old continent and the rest of the world.

About standards, ESA cooperates with the European Cooperation for Space Standardization (ECSS), making coherent set of user-friendly space standards for use by the agency. With regards to cybersecurity, ECSS have included some requirements in ECSS-E-ST-40C and ECSS-Q-ST-80C, which are still ongoing a public review in the case of the second standard.

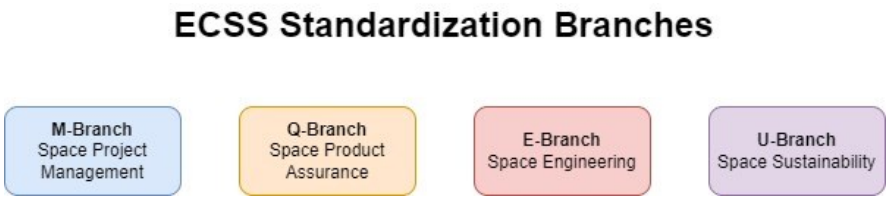

Figure 6: ECSS Standardization Branches

2.5.1. ECSS-E-ST-40C – SPACE ENGINEERING SOFTWARE

ECSS-E-40 focuses on software that belongs to space systems and is developed within the scope of space projects. Its applicability encompasses all segments of space systems, including space, launch, and ground segments. Furthermore, it covers the entire software engineering lifecycle, including requirements definition, design, production, verification and validation (V&V), transfer, operations, and maintenance.

Its primary purpose is to assist stakeholders in formulating their **software requirements** by leveraging the ECSS-E-ST-40C framework, which combines methods and requirements from other branches of ECSS. Additionally, the standard guides suppliers in implementing these requirements [RD-35].

It is currently on review and are being introduced new security aspects that will make this standard more robust in cybersecurity.

The changes are as follows:

- Introduction of a new definition and abbreviation of threats.
- New section added to cover the **Software Security Process** (section 5.11).
  - Process implementation
  - Software security analysis
  - Security risk treatment
  - Security activities in the software lifecycle

- Requirements added (sections 5.x) and updated to introduce the consideration of security in the complete development process.
- Introduction of a **Security File** and related documentation.
  - Software security management plan (SSMP)
  - Software security analysis report (SSAR)
  - Security risk treatment plan (SRTP)

2.5.2. ECSS-Q-ST-80C – SOFTWARE PRODUCT ASSURANCE

Through the Q-80 standard, users leverage a set of **software product assurance requirements** for developing and maintaining the software component of firmware in space systems, including space, launch, and ground segments [RD-36].

Like the E-40 standard in the past, Q-80 is currently undergoing review and updates to align with ECSS-E-ST-40C and incorporate new software security assurance requirements.

The primary focus of these changes is on enhancing security, as evidenced by the following revisions:

- Added security aspects (5.1.5.4 b) to the Training section.
- Removed security from the Software Problems section (5.2.5.1 a), as it is already covered by E-40.
- Introduced a security representative to the Non-conformance Reporting Board (NRB) (5.2.6.1 d) in the Non-conformance Reports (NCRs) section.
- Added a new chapter 5.4.5 based on high-level security analysis in the Sensitivity Classification section.
- Incorporated two new security-related chapter (5.5.3 and 5.5.6) regarding import/export constraints and information in the Procurement section.
- Introduced an additional chapter to consider security when selecting tools and methods (5.6.1.2).
- Added points 13 and 14 to the chapter 5.6.2.1 in the Development Environment section to assess security aspects.
- Life Cycle (chapters 6.1.3 and 6.1.4): Security considerations have been incorporated.
- Documentation Process (6.2.1.1): Security management has been added.
- HSIA Section (chapter 6.2.2.8): A note has been included to address hardware security-related failures.
- Configuration Management Section (chapter 6.2.4):
  - 6.2.4.7(i): Added guidance for the secure disposal of sensitive documentation.
  - 6.2.4.8(b): Added requirement to ensure software protection.
  - 6.2.4.9(b): Added requirement to ensure software authenticity.
  - 6.2.4.11: Rewritten to include security aspects.
- ISVV Section (chapter 6.2.6.13): Updated to reflect security considerations.
- Reuse of Software Section (chapters 6.2.7.3, 6.2.7.4, and 6.2.7.8): Updated to reflect security aspects.
- Software Security Section (new chapter 6.2.9): Added with new security requirements.
- Handling of Security Sensitive Software Section (new chapter 6.2.10): Added with new security requirements.
- Software Engineering Process (chapter 6.3): Security aspects have been added throughout various subsections.
- Software Product Quality Assurance (chapters 7.1.1, 7.4.4, and 7.5.2): Security aspects have been incorporated.

2.6. Consultive Committee for Space Data Systems

The Consultative Committee for Space Data Systems (CCSDS) was founded in 1982 by multiple space agencies. Its mission is to discuss and develop standards for space data and information systems.

Currently, the CCSDS comprises eleven member agencies, including NASA, ESA, and JAXA, along with 33 observer agencies and over 130 industrial entities [RD-37].

The CCSDS publishes standards and related materials in various areas, such as:

- Space Internetworking Services
- Mission Operations and Information Management Services
- Spacecraft Onboard Interface Services
- System Engineering
- Cross Support Services
- Space Link Services

The CCSDS employs a color-coded system to categorize its publications:

- Blue: Recommended Standards
- Magenta: Recommended Practices
- Green: Informational Reports
- Orange: Experimental Documents

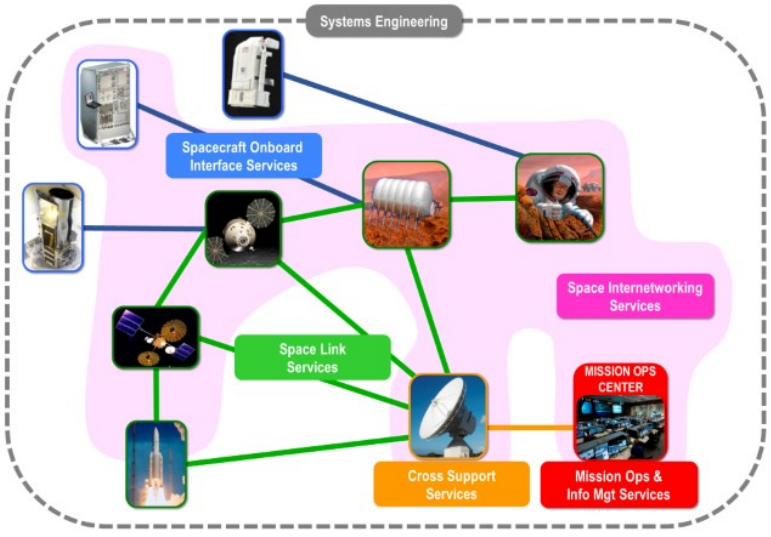

Figure 7: Space Data System Reference Model [RD-37]

2.6.1. CCSDS 351.0-M-1 – SECURITY ARCHITECTURE FOR SPACE DATA SYSTEM

This document is the equivalent of ISO 20214, described in section 2.3.3. It was published in 2012 and subsequently adopted by ISO in 2015 [RD-38].

2.6.2. CCSDS 355.0-B-2 – SPACE DATA LINK SECURITY PROTOCOL

This standard, designated with the blue colour scheme, focuses on the Space Data Link Security Protocol (hereafter referred to as the Security Protocol). One of its primary goals is to provide security at the data link layer, independent of the specific cryptographic algorithms used.

The standard begins by providing an overview of the Security Protocol, including its concepts, features, and service functions. It then defines the services that support the space data link, specifies the constraints associated with these services, lists the managed parameters associated with the identified services, and finally outlines how to verify an implementation's conformance to the Security Protocol [RD-39].

2.7. MITRE

The MITRE Corporation is a non-profit organization that operates as a federally funded research and development centre in the United States. Established in 1958, MITRE works across government and industry, tackling challenges in the following domains:

- Aerospace
- Artificial Intelligence
- Aviation and Transportation
- Cybersecurity
- Defence and Intelligence
- Government Innovation
- Health
- Homeland Security
- Telecommunications

MITRE is a leading force in cybersecurity, drawing on its extensive technical expertise to develop strategies that address the ever-evolving challenges in this field. For over 50 years, the organization has been creating valuable standards, tools, and frameworks to enhance cybersecurity. Let us focus specifically on their frameworks, where MITRE offers four prominent examples [RD-41]:

- **ATT&CK**: A series of tactics and techniques used by hackers based on real-world observations. This knowledge base helps developers create threat models and methodologies for cybersecurity products and services [RD-42].
- **Engage**: This program empowers cybersecurity defenders by making adversary engagement technologies (cyber denial + cyber deception technologies) more accessible and fostering expertise within the community [RD-43]. It offers a variety of tools (engage matrix, mission essential task list) for experienced practitioners, while also providing a starter pack (basics, terminology, methodologies) for those new to the cybersecurity field.
- **D3FEND**: A collection of cybersecurity countermeasures, utilizing well-defined types and relationships to represent key concepts within the cybersecurity countermeasure domain. These concepts and relationships are meticulously linked to relevant references in cybersecurity literature, including five hundred countermeasure patents issued by the U.S. Patent Office. This comprehensive linking ensures a well-grounded foundation for the knowledge base [RD-44].

- **CALDERA**: Cybersecurity framework empowers cybersecurity agents to automate security assessments. This automation reduces time, cost, and manpower, allowing resources to be reinvested in other critical security activities [RD-45].

MITRE maintains a continuously updated list of software and hardware weakness types [RD-46]. This list helps the cybersecurity community identify potential exploit mechanisms, allowing them to become aware of and resolve these vulnerabilities before they can be weaponized.

2.8. Software Engineering Institute

SEI CERT (Software Engineering Institute CERT) is a world-renowned nonprofit organization dedicated to improving the security and resilience of computer systems and networks. Established in 1988 by Carnegie Mellon University's Software Engineering Institute (SEI) with funding from the U.S. Department of Defence, SEI CERT has become a leading authority in cybersecurity research, education, and incident response.

The CERT Secure Coding Standards, developed by a community of experts, cover programming languages like C, C++, Java, Perl, and the Android platform [RD-47]. These standards provide best practices for secure software development, helping developers write code with fewer vulnerabilities.

Figure 8: Standards Development Area [RD-47]

2.9. Open Worldwide Application Security Project

A collaborative effort supporting organizations in developing more secure applications, the OWASP Foundation launched on December 1, 2001. Now boasting tens of thousands of members, it has become the industry leader in hosting educational and training conferences [RD-48]. The foundation spearheads numerous projects, including:

- **OWASP Top 10**: A list highlighting the top ten web application security risks. By understanding these common threats, companies can proactively address vulnerabilities and avoid falling victim to well-known attack methods.
- **Dependency Track**: An intelligence platform to allow organizations to identify and mitigate risk in theirs supply chains, leveraging the capabilities of Software Bill of Materials.
- **Juice Shop**: A web application designed for security training, awareness demos, Capture the Flag (CTF) competitions, and testing the effectiveness of security tools. Written in Node.js, Express, and Angular, it deliberately incorporates a variety of vulnerabilities to provide a realistic environment for practicing and learning secure coding practices.
- **Mobile Application Security**: Focused on mobile application security, this project provides a security standard and testing guides that cover processes, techniques, and tools used during software security testing. The project is divided into two main components: the Mobile Application Security

Verification Standard (MASVS) and the Mobile Application Security Testing Guide (MASTG). Additionally, a Mobile Application Security Checklist is available to support users.

- **ModSecurity Core Rule Set**: A set of generic attack detection rules, compatible with ModSecurity and other web application firewalls, provides protection against a wide range of common attacks. These rules include defences for SQL injection, cross-site scripting, local file inclusion, and vulnerabilities listed in the OWASP Top 10.
- **Software Assurance Maturity Model**: A framework used to analyse and improve the secure development lifecycle, by evaluating companies on existing software security practices.
- **Web Security Testing Guide**: Comprehensive guide to cybersecurity testing of web applications and services, by providing a set of best practices used by penetration testers.

2.10. University of Bristol – CyBOK

The Cybersecurity Body of Knowledge (CyBOK), now in version 1.1, is a project that focuses on mapping existing cybersecurity knowledge. Rather than comprehensively rewriting everything, CyBOK aims to establish a solid foundation and clear learning pathways to facilitate access and education for the cybersecurity community. It draws upon a wealth of information from various sources, including textbooks, academic research articles, technical reports, white papers, and industry standards. CyBOK is comprised of twenty-one knowledge areas, grouped into five distinct categories [RD-50]:

- Human, Organisational and Regulatory Aspects
- Attacks and Defences
- Systems Security
- Software and Platform Security
- Infrastructure Security

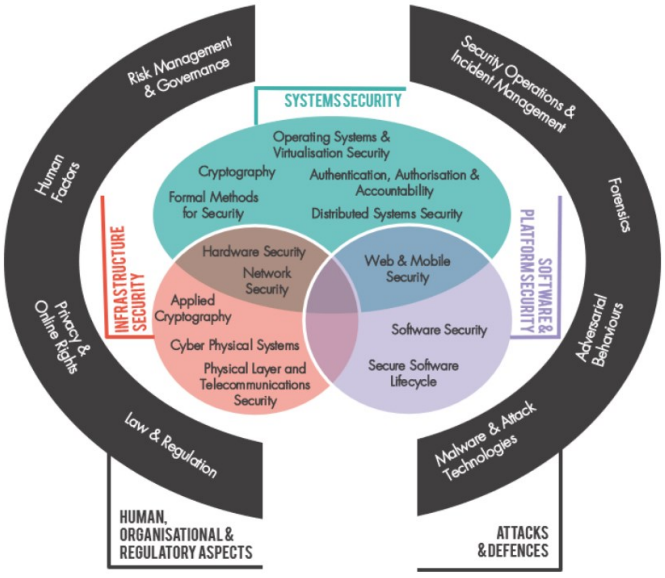

Figure 9: The 21 Knowledge Areas of CyBOK [RD-50]

The first category, Human, Organizational, and Regulatory Aspects, is comprised of four knowledge areas:

- **Risk Management and Governance**: This area focuses on identifying, assessing, and prioritizing potential threats to an organization. It also covers implementing strategies to minimize the impact of these threats.
- **Law and Regulations**: This area focuses on the relevant legal and regulatory requirements that organizations must comply with. This includes data protection laws and doctrines related to cyber warfare.
- **Human Factors**: This area focuses on the impact of human behaviour on cybersecurity. It explores how social engineering attacks work and emphasizes the importance of security culture and awareness among employees.
- **Privacy and Online Rights**: This area focuses on the protection of personal information in the digital age, considering an individual's rights online.

The second category, Attacks and Defences, comprises four knowledge areas centred around cyberattacks and attacker motivations:

- **Malware and Attack Techniques**: This area delves into the details of attacker strategies, exploring how they exploit systems.
- **Adversary Behaviours**: This area focuses on the motivations behind cyberattacks and the methods attackers use to execute them.
- **Security Operations and Incident Management**: This area covers the ongoing practices for maintaining and monitoring an organization's security posture. It involves a combination of people, processes, and technologies to detect, prevent, analyse, and respond to security threats.
- **Digital Forensics**: This area focuses on analysing digital evidence to investigate security incidents and criminal activities.

The third category, Systems Security, comprises five knowledge areas centred around securing systems:

- **Cryptography**: This area delves into the foundations of existing and emerging cryptographic algorithms, as well as techniques for analysing them and their underlying protocols.
- **Operating System and Virtualization Security**: This area focuses on the protection mechanisms for operating systems and securing virtualization environments.
- **Distributed Systems Security**: This area focuses on the protection mechanisms used in large-scale distributed systems, including aspects of peer-to-peer networks, cloud computing, multi-tenant data centres, and distributed ledgers.
- **Formal Methods for Security**: This area focuses on using mathematical models and logic to reason about the security of systems, software, and protocols.
- **Authentication, Authorization, and Accountability**: This area focuses on the technologies and tools used for authentication, identification management, authorization, and accountability.

The fourth category, Software and Platform Security, comprises three knowledge areas focused on software, web, mobile security, and the secure software development lifecycle:

- **Software Security**: This area explores common programming errors that can lead to security vulnerabilities. It also presents coding practices to help developers write more secure code.
- **Web and Mobile Security**: This area focuses on the specific security challenges faced by web applications and mobile applications.
- **Secure Software Development Lifecycle**: This area delves into security engineering techniques that can be integrated throughout the software development lifecycle to build more secure software.

The final category, Infrastructure Security, comprises five knowledge areas focused on securing cyber and physical infrastructure:

- **Applied Cryptography**: This area delves into the practical application of cryptographic algorithms, schemes, and protocols. It also explores the challenges encountered during their implementation.
- **Network Security**: This area focuses on the security aspects of network and telecommunications protocols. This includes the security of routing protocols, network security elements, and the specific use of cryptographic algorithms within network security.
- **Hardware Security**: This area focuses on incorporating security considerations throughout the hardware development lifecycle.
- **Cyber-Physical Systems Security**: This area addresses the security challenges introduced by Fourth Industrial Revolution.
- **Physical Layer and Telecommunications Security**: This area explores the limitations and security concerns associated with the physical layer of the OSI model, including radio frequency encodings, unintended radiation, and interference.

2.11. CENELEC

The railway industry plays a vital role in global transportation, and ensuring the safety, efficiency, and interoperability of rail systems is paramount. This is where CENELEC (Comité Européen de Normalisation Electrique - European Committee for Electrotechnical Standardization) steps in as a key player in developing and promoting harmonized railway standards across Europe.

CENELEC, alongside its partner organization CEN (European Committee for Standardization), works collaboratively with various stakeholders in the railway sector. These stakeholders include manufacturers, operators, infrastructure providers, and regulatory bodies. The following sections present two railway standards containing cybersecurity concerns.

2.11.1. EN 50159 – RAILWAY APPLICATIONS – COMMUNICATION, SIGNALLING AND PROCESSING SYSTEMS

This standard focuses on safety-related electronic systems used for digital communication purposes. While cybersecurity is not its primary focus, it does acknowledge threats involving malicious messages targeting safety-related applications [RD-51]. To protect digital communication, the standard mention various techniques:

- Hash block codes, as specified in ISO/IEC 10118, ensure data integrity by detecting any unauthorized alterations.
- Cryptographic block codes, most known as Message Authentication Codes (MACs) standardized in ISO/IEC 9797, provide message authentication, verifying the sender's identity and preventing message tampering.

2.11.2. CLC/TS 50701 – RAILWAY APPLICATIONS - CYBERSECURITY

The CLC/TS 50701:2023 standard serves as a roadmap for enhancing cybersecurity in railway applications. It provides guidelines and recommendations to protect information technology systems within railways from potential cyberattacks [RD-52].

These are the key areas addressed by the standard:

- **Threat and Risk Management**: Outlines a process for identifying, assessing, and managing cyber threats and risks specific to railway applications.
- **Protecting Critical Functions**: Measures to safeguard critical railway functions. These measures include technical solutions like data encryption, user authentication, access control, and network monitoring.
- **Incident Response**: Procedures for handling cyber incidents in railway applications. This encompasses reporting, investigating, and analysing incidents, along with taking appropriate actions to minimize damage.

- **Secure Development Practices**: Implementation of secure development processes for railway applications. This includes incorporating risk analysis and testing methodologies throughout the development lifecycle.

This standard takes some inspiration, mostly in threat and risk management, to the IEC 62443 series of standards and ISO 27000 family.

2.12. FEDERAL AVIATION ADMINISTRATION

The aviation industry is the backbone of modern global travel, enabling the swift and efficient movement of people and goods across vast distances. Ensuring the safety, efficiency, and security of air travel is paramount. This is where the Federal Aviation Administration (FAA) steps in as a critical player in the United States.

The FAA, a U.S. government agency operating under the Department of Transportation, is responsible for regulating all aspects of civil aviation within the United States and surrounding international airspace. This includes establishing and enforcing safety standards, conducting inspections and certifications, and managing the National Airspace System (NAS). Importantly, cybersecurity has become a vital aspect of the FAA's mission, as cyber threats can potentially disrupt air travel and endanger public safety.

To address these cybersecurity challenges, the FAA works independently and collaboratively with international organizations. While the FAA sets its own standards, it collaborates with its counterparts worldwide, such as the European Union Aviation Safety Agency (EASA), to ensure some level of harmonization in aviation security practices. One prominent example of such collaboration is the development of international standards, the DO-326/ED-202, known as Airworthiness Security Process Specification standards.

2.12.1. DO-326/ED-202 – AIRWORTHINESS SECURITY PROCESS SPECIFICATION

These standards were developed through the collaborative effort of the Aeronautical Systems Security initiative, formed in 2006. This initiative involves EUROCAE, which creates aviation standards for the European Union Aviation Safety Agency (EASA), and RTCA, the organization that collaborates with the FAA to establish industry-approved and endorsed standards [RD-53].

The initial collaboration resulted in the DO-326/ED-202 documents, titled “Airworthiness Security Process Specification”. This standard aimed to guide a more secure development phase of aircraft information security within the overall Aeronautical Information System Security (AISS), from inceptions to certification and deployment.

The core inspiration of the DO-326/ED-202 came from existing standards, ISO/IEC 27005, focus on providing guidance on managing information security risks, and the SAE ARP 4754, offering guidelines for develop civil aircraft and systems [RD-53].

In 2018, the Airworthiness Security Process Specification set expanded to include two distinct standards [RD-53]:

- **DO-326A/ ED-202A** “Airworthiness Security Process Specification”: Maintains the core framework for airworthiness security processes.
- **DO-356A/ ED-203A** “Airworthiness Security Methods and Considerations”: Provides supplemental guidance and considerations for achieving airworthiness security.

Building upon DO-326A/ED-202A, DO-356A/ED-203A offers in-depth guidance for achieving airworthiness security in aircraft systems [RD-54]. It details critical aspects like:

- **Security Objectives**: Specific security objectives to be met throughout the development lifecycle.

- **Risk Assessments**: Methods for assessing cybersecurity risks specific to the aircraft's development stage.
- **Security Assurance**: Levels of rigor applied to ensure the security of a system. These levels range from 0 (least critical) to 3 (most critical), with each level having associated objectives that must be met.
- **Security Architecture**: Principles for implementing security at the aircraft, system, and item levels.

This standard serves as a valuable companion to DO-326A/ED-202A, offering detailed explanations and illustrative examples. An appendix maps activities from DO-326A/ED-202A to the corresponding guidance within DO-356A/ED-203A, promoting a clear and cohesive approach to achieving airworthiness security.

In addition to DO-356A/ED-203A, several other standards complement DO-326A/ED-202A, addressing various aspects of aviation cybersecurity. Here are two examples:

- DO-355/ED-204 "Information Security Guidance for Continuing Airworthiness": This standard details the guidance on information security risks applicable when the aircraft is already in service.
- ED-201A “Aeronautical Information System Security Framework Guidance”: This high-level document outlines the shared responsibility for Aeronautical Information System Security (AISS), identifying and describing areas of concern for stakeholders.
- ED-205, “Process Standard for Security Certification and Declaration of Air Traffic Management/Air Navigation Services (ATM/ANS) Ground Systems”: This standard focuses on ensuring the appropriate security of ATM/ANS ground systems. It describes a process for identifying, evaluating, and managing the potential impact of security breaches.

In summary, to create systems for aviation it must be compliant with the DO-326/ED-202 set, following the process illustrated in Figure 10.

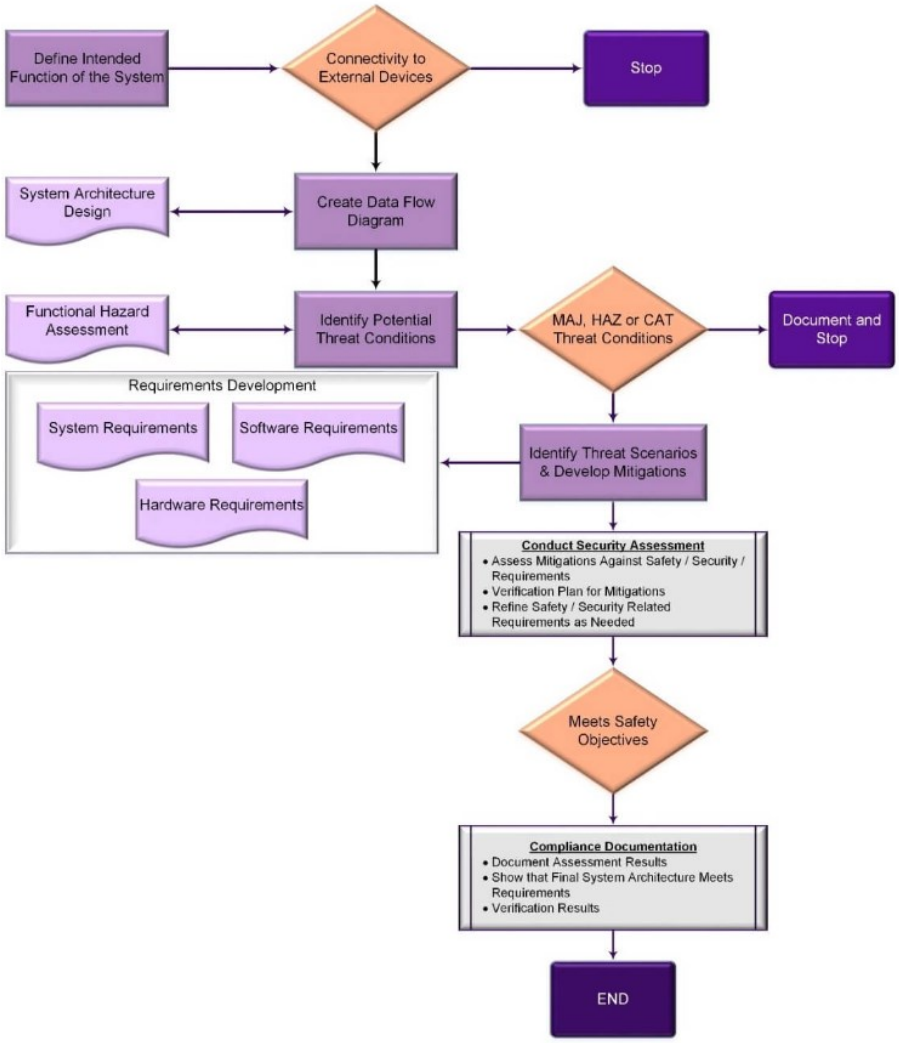

Figure 10: Secure System Design and Implementation Process [RD-54]

The system security assessment process starts with defining the system's intended functions, including both customer-facing features and maintenance/support functionalities. Following this, it's crucial to identify any elements within the system that connect to external devices or networks. If external connections exist, appropriate security measures like authentication, data sharing controls, access restrictions, and protection mechanisms need to be implemented.

The next step involves creating a data flow diagram to illustrate communication flows between internal and external system components. With this diagram in place, threat modelling is conducted in conjunction with functional hazard analysis (FHA) and system safety assessment (SSA) to identify and assess potential threat conditions.

Threat modelling considers the likelihood of occurrence, potential impact (severity), and the cost of mitigation to determine the risk associated with each threat. Identified security threats are then evaluated using methodologies like "DREAD" (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability).

Threats are prioritized based on their risk scores, and proportionate mitigation actions are developed for each one. These mitigations are then incorporated into the system requirements and subsequently verified and validated through various techniques, including:

- Static code analysis
- Known vulnerability scanning
- Penetration testing
- Software composition analysis
- Security requirements testing
- Threat mitigation testing

Critical software

We are CMMI Maturity Level 5 rated.
For a list of our certifications & standards visit our website.

www.criticalsoftware.com