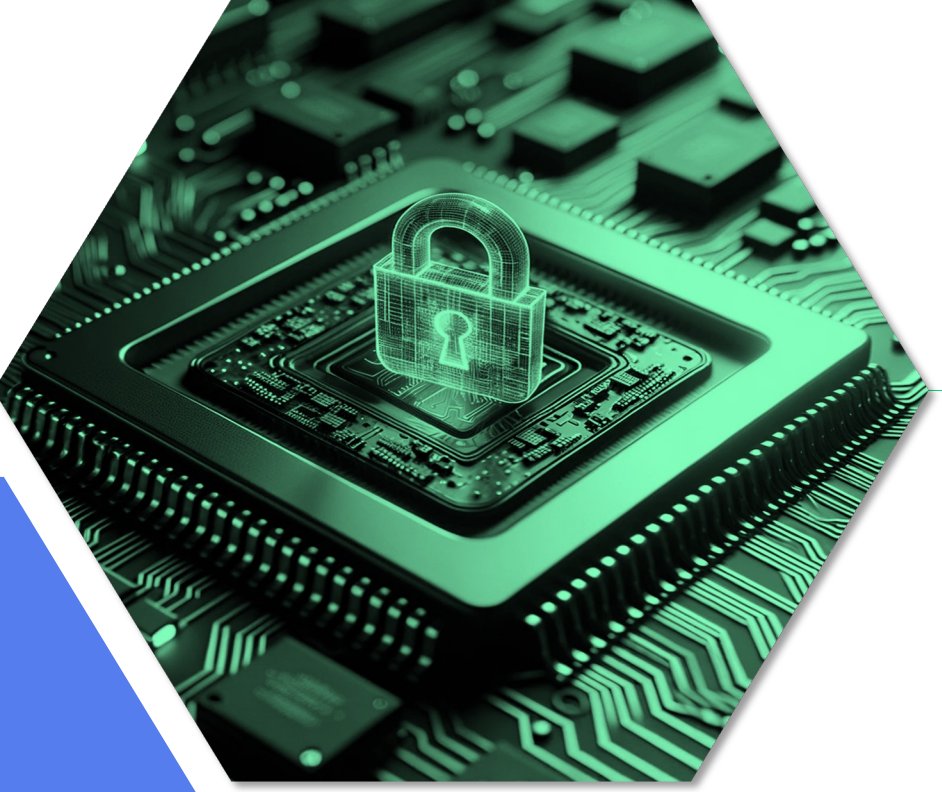
Cycuity

Guide To Hardware Security

Industry Standards, Regulations, and Policies



In an era marked by relentless technological advancements, the significance of **cybersecurity standards**, **regulations** and **guidelines** has emerged as a critical dimension for companies engaged in the manufacturing of electronic devices. As our dependence on interconnected technologies intensifies, ensuring the integrity and resilience of hardware components becomes paramount. Governmental bodies and industry stakeholders are recognizing the escalating threats posed by cyber attacks and unauthorized access to sensitive information through electronic devices.

Consequently, the establishment of robust **hardware security regulations** and **requirements** are becoming increasingly imperative to safeguard not only the interests of manufacturers but also the privacy and security of end-users.

In this dynamic landscape, **semiconductor manufacturers are compelled to navigate a complex web of standards and compliance requirements to ensure hardware security is an integral aspect of chip design, development, and market viability.**

This guide is designed to help companies understand the goals and potential implications of these initiatives, which are aimed at promoting more secure design practices. It also provides information on the requirements for achieving compliance and certification.

ISO/SAE 21434:

Road Vehicles – Cybersecurity Engineering

Automotive

ORIGIN/BACKGROUND:

- Developed in response to the growing cybersecurity threats in the automotive sector, with increasing connectivity and automation.
- Aims to address cybersecurity risks in electrical and electronic (E/E) systems within vehicles.

EFFECTIVE DATE:

- Published in August 2021.

GOAL

- Establish a comprehensive cybersecurity risk management framework for the lifecycle of automotive E/E systems.
- Manage cybersecurity risk by embedding cybersecurity considerations early in the development process.
- Foster cybersecurity culture within the industry.

IMPACT

- **COMPLIANCE:** Automotive manufacturers will increasingly demand that their suppliers comply with relevant cybersecurity standards. Adhering to ISO 21434 helps automotive manufacturers and suppliers demonstrate compliance with cybersecurity regulations and requirements. It serves as a benchmark for industry stakeholders to assess and improve their cybersecurity posture.
- **ADOPTION BY INDUSTRY STAKEHOLDERS:** Industry leaders are quickly adopting ISO/SAE 21434 as the leading approach for cybersecurity. Major suppliers such as Renesas, NXP, and Texas Instruments have certified their Automotive Cybersecurity process compliant to the ISO/SAE 21434 standard.
- **COMPETITIVE ADVANTAGE:** ISO/SAE 21434 certification will provide a competitive advantage over other suppliers and helps ensure trust from customers.

RESOURCES

Naden, C. (n.d.). Cybersecurity in cars. ISO.

ISO/SAE 21434 Certification – Road Vehicles Cybersecurity Engineering. (2021). SGSCorp.

Overview of ISO/SAE 21434. (n.d.). YSEC.

From 2022: increased responsibility due to new automotive standards - CCLab News. (n.d.).

United Nations Economic Commission for Europe (UNECE) Regulation No. 155:

Vehicles – Cybersecurity

Automotive

GOAL

- Mandates the implementation of a Cybersecurity Management System (CSMS) by vehicle manufacturers, covering the entire vehicle lifecycle.
- Ensures systematic management of cybersecurity risks, from prevention and detection to response and recovery.

IMPACT

- **GLOBAL MARKET ACCESS AND COMPLIANCE:** Compliance with UNECE Regulation No. 155 is essential for market access. Non-compliance can lead to a sales ban in the corresponding area of application.
- **SECURE DESIGN PRACTICES:** The regulation emphasizes secure design practices for hardware components, such as Electronic Control Units (ECUs) and sensors, encouraging manufacturers to integrate cybersecurity considerations into the early stages of product development.
- **SECURITY ACROSS THE DEVELOPMENT LIFECYCLE:** The regulation promotes a lifecycle approach to cybersecurity, necessitating ongoing monitoring, updates, and improvements to hardware security throughout the lifespan of the automotive components.
- **GLOBAL STANDARDIZATION:** Since UNECE is a global regulatory body, adherence to Regulation 155 could contribute to global standardization in automotive cybersecurity.

ORIGIN/BACKGROUND:

- Instituted by the UNECE to combat increasing cybersecurity risks due to vehicle connectivity and automation, Regulation 155 outlines requirements for automotive systems, including hardware components. The regulation applies to 54 member countries of the 1958 UNECE Transportation Agreements and Conventions, including the EU, the UK, Japan, and South Korea.
- The regulation mandates comprehensive cybersecurity controls, impacting key aspects of the hardware and software development process, including specifications, testing, and certification, to protect against unauthorized access and cyberattacks.

EFFECTIVE DATE:

- Mandatory for new vehicle types from July 2022; for all new vehicles from July 2024.

RESOURCES

UN Regulations on Cybersecurity and Software Updates to pave the way for mass roll out of connected vehicles | UNECE. (n.d.). Unece.org.

Zastrow, K. (n.d.). UN Regulation 155 on cybersecurity and its impact with regard to electric vehicles. Retrieved February 21, 2024.

Sandler, M. (2022, June 1). UN Regulation No 155 & how to comply? What you need to know. CYRES Consulting.

ISA/IEC 62443:

Security for Industrial Automation and Control Systems

IoT/Industrial

GOAL

- To establish a comprehensive framework for securing IACS across their lifecycle, emphasizing risk assessment, system design, implementation, and maintenance.
- Targets a broad range of stakeholders including asset owners, product suppliers, integrators, and service providers, ensuring tailored cybersecurity strategies.

IMPACT

- **RISK MITIGATION IN INDUSTRIAL ENVIRONMENTS:** The standards provide a framework for identifying, assessing, and mitigating cybersecurity risks specific to industrial environments. Hardware manufacturers need to integrate these risk management practices into the design, production, and maintenance of their components.
- **COMPLIANCE AND CERTIFICATION:** ISA/IEC 62443 defines a secure development lifecycle for developing and maintaining secure products. The lifecycle includes security requirements definition, secure design, secure implementation (including coding guidelines), verification and validation, defect management, patch management and product end-of-life. Compliance with the standard is essential for organizations using IT products in their infrastructure and will need to be demonstrated through certification.
- **GLOBAL APPLICABILITY:** As a widely adopted international standard that sets a global benchmark for cybersecurity in industrial automation and control systems, hardware manufacturers aiming to operate in various global markets must ensure compliance the ISA/IEC 62443 standard to meet regulatory requirements and industry expectations.

ORIGIN/BACKGROUND:

- Developed by the International Electrotechnical Commission (IEC) in response to unique cybersecurity vulnerabilities in industrial automation and control systems (IACS).
- Addresses the gap where traditional IT security solutions fall short in operational technology (OT) environments.

EFFECTIVE DATE:

- In 2021 the IEC approved the IEC 62443 family of standards as “horizontal standards.”

RESOURCES

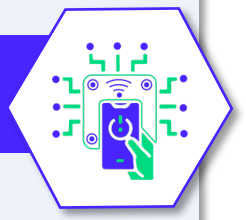
ISA/IEC 62443 Series of Standards - ISA. (n.d.). Isa.org.

What Is the ISA/IEC 62443 Framework? | Tripwire. (n.d.).

Understanding IEC 62443. (n.d.). www.iec.ch.

Cyber Resilience Act (CRA)

IoT/Industrial



GOAL

- Establishes stringent cybersecurity requirements for digital product manufacturers.
- Aims to ensure a high common level of cybersecurity across the EU, protecting consumers and businesses.

IMPACT

- **MANDATORY COMPLIANCE FOR MARKET ENTRY:** The CRA mandates compliance with cybersecurity standards for all digital products entering the EU market, ensuring that products meet high cybersecurity standards before they can be sold.
- **REDUCTION IN CYBERSECURITY RISKS AND INCIDENTS:** By setting stringent cybersecurity requirements, the CRA is expected to significantly reduce the prevalence of cybersecurity risks and incidents, thereby boosting consumer trust in digital services and products.
- **IMPACT ON PRODUCT MANUFACTURING:** Manufacturers may decide to discontinue the production of certain products if retrofitting them to meet the new cybersecurity standards is deemed too costly.
- **GLOBAL INFLUENCE ON CYBERSECURITY PRACTICES:** Given the size and influence of the EU market, the CRA is likely to have a global impact, encouraging manufacturers worldwide to adopt higher cybersecurity standards for their products, even if they are not directly selling in the EU.

ORIGIN/BACKGROUND:

- Initiated by the European Commission to strengthen cybersecurity across the EU.
- Targets enhancing the security of digital products, services, and devices.

EFFECTIVE DATE:

- The regulation is expected to enter into force in early 2024. Manufacturers will have to apply the rules 36 months after their entry into force. This means the first implementation phase for manufacturers to comply with the CRA requirements will start in early 2027.

RESOURCES

EU Cyber Resilience Act | Shaping Europe's digital future. (n.d.). Digital-Strategy.ec.europa.eu.

European Cyber Resilience Act. (n.d.).

Aleksiev, M. Y., Aleksander. (2023, December 1). The EU's Cyber Resilience Act Has Now Been Agreed. Inside Privacy.

Pappas, T. (2023, December 15). Porsche To Kill ICE-Powered Macan In Europe Over Cybersecurity Laws. Carscoops; Carscoops.

Radio Equipment Directive (RED)

IoT/Industrial

GOAL

- Bolsters cybersecurity, personal data protection, and privacy for products using radio technology, many of which are internet-connected and could face increasing security risks.
- Ensures a single market for radio equipment by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum.

IMPACT

- **REGULATORY OVERSIGHT:** RED establishes a framework for regulatory oversight and market surveillance to ensure continued compliance and safety of radio equipment placed on the EU market.
- **ENHANCED CONSUMER PROTECTION:** By setting safety and performance standards, RED aims to enhance consumer protection and confidence in radio equipment available in the EU.
- **ADAPTATION TO TECHNOLOGICAL ADVANCES:** RED allows for updates to keep pace with technological advancements, ensuring that radio equipment remains safe and reliable in the evolving landscape.

ORIGIN/BACKGROUND:

- The European Commission(EU) revised the RED to incorporate new security legislation (2022/30/EU) on January 12, 2022.
- The update necessitates cybersecurity, personal data, and privacy safeguards for devices that can connect to the internet (either directly or through other equipment), handle personal data, traffic data or location data, and allow users to transfer money, monetary value, or virtual currency.
- The goal is to enhance cybersecurity, personal data protection, and privacy for a broad array of products using radio technology, many of which can connect to the internet and may be vulnerable to escalating security threats.

EFFECTIVE DATE:

- The updated provisions of the RED, specifically Articles 3(3)(d), (e), and (f) related to cybersecurity, personal data protection, and privacy, become mandatory on August 1, 2025. Manufacturers of radio connected devices must be compliant by this date to avoid potential regulatory action.

RESOURCES

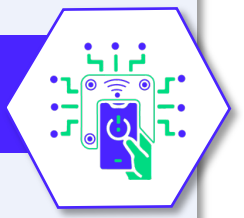
(n.d.). New EU security legislation under the radio equipment directive (RED) TÜV SÜD.

(2023, November 2). EU Commission Extends Effective Date of Expanded Radio Equipment Requirements. InCompliance Magazine.

Cybersecurity and Infrastructure Security Agency (CISA) Hardware Bill of Materials (HBOM):

Framework for Supply Chain Risk Management(SCRM)

IoT/Industrial



ORIGIN/BACKGROUND:

- Developed by CISA to enhance supply chain security.
- Focuses on transparency in the hardware supply chain through detailed component documentation.

EFFECTIVE DATE:

- Published September 25, 2023.

GOAL

- Provides a standardized approach for creating, sharing, and using HBOMs.
- Aims to identify and mitigate risks associated with hardware components and their supply chains.

IMPACT

- **BETTER RISK MANAGEMENT AND SECURITY PRACTICES:** By offering a standardized approach for creating, sharing, and using HBOMs, the framework is expected to improve resilience against supply chain attacks by facilitating better risk management and security practices among manufacturers, suppliers, and consumers.
- **GREATER TRANSPARENCY AND EFFICIENCY:** The framework promotes transparency within the supply chain by providing a consistent naming methodology for attributes of components and a format for identifying and providing information about different types of components. This helps organizations make informed decisions and prioritize vulnerability handling, thereby improving efficiency in managing supply chain risks.
- **SIMPLIFIED COMPLIANCE WITH REGULATORY REQUIREMENTS:** The HBOM Framework assists organizations in complying with regulatory requirements by providing a structured approach to documenting and managing hardware components within the supply chain. This is particularly important in sectors where regulatory compliance is critical for operational continuity.

RESOURCES

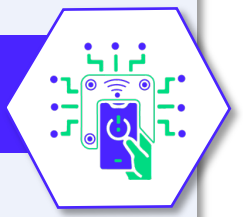
CISA Releases Hardware Bill of Materials Framework (HBOM) for Supply Chain Risk Management (SCRM) | CISA. (2023, September 25). www.cisa.gov.

New CISA framework offers improved hardware supply chain risk assessments. (2023, September 26). SiliconANGLE.

Naraine, R. (2023, September 27). CISA Unveils New HBOM Framework to Track Hardware Components. SecurityWeek.

Hardware Common Weakness Enumeration (CWE™)

IoT/Industrial



ORIGIN/BACKGROUND:

- Common Weakness Enumeration (CWE™) is a community-developed list of common software and hardware weakness types that have security ramifications. Hardware Design CWEs focus on vulnerabilities inherent to hardware design and implementation that could be exploited to compromise security features.
- Addresses the need for a standardized nomenclature and taxonomy for hardware security weaknesses. It reflects the evolving landscape of hardware vulnerabilities in the face of sophisticated cyber threats.

GOAL

- The primary goal of CWE is to catalog and describe hardware security weaknesses in a structured manner, facilitating the identification, understanding, and remediation of common hardware vulnerabilities. This includes issues related to insecure hardware feature design, implementation, and integration that could undermine the security of information systems.
- By providing a comprehensive framework for hardware security weaknesses, CWE aims to foster improved hardware design and development practices, ensuring that security is a core consideration from the earliest stages of hardware conception.

IMPACT

- **REDUCTION IN HARDWARE-RELATED SECURITY INCIDENTS:** The broader adoption of this standard is expected to lead to a reduction in the prevalence and severity of hardware-related security incidents. By highlighting common hardware vulnerabilities and promoting best practices for secure hardware design, CWE contributes to the mitigation of cybersecurity risks.
- **IMPROVED HARDWARE DESIGN AND DEVELOPMENT PRACTICES:** By providing a comprehensive framework for hardware security weaknesses, CWE aims to foster improved hardware design and development practices, ensuring that security is a core consideration from the earliest stages of hardware conception.
- **EMPOWERED HARDWARE CONSUMERS:** CWE standard enables consumers to demand more secure hardware by providing a standardized framework for identifying security weaknesses, leading to improved market offerings.

RESOURCES

CWE - CWE-1194: Hardware Design (4.10). (n.d.).

CWE - CWE Most Important Hardware Weaknesses. (n.d.).

Marchese, S. (2020, December 9). Make Hardware Strong With CWE. Semiconductor Engineering.

Chips and Sciences Act

DoD/Government Initiatives

GOAL

- Aims to revive and expand domestic semiconductor manufacturing capabilities.
- Provides funding and incentives for research, development, and manufacturing of semiconductors in the U.S.

IMPACT

- **STRENGTHENING OF NATIONAL SECURITY:** The focus on domestic chip production and supply chain security aims to strengthen national security. By reducing reliance on foreign manufacturers, the U.S. can ensure the availability of critical components for defense systems, communication infrastructure, and data protection.
- **PROMOTION OF INNOVATION AND GLOBAL COMPETITIVENESS:** By providing funding and incentives for semiconductor research, development, and manufacturing, the Act promotes innovation and competitiveness in the global semiconductor industry. This is expected to secure supply chains and maintain the U.S.'s leadership in chip technology.

ORIGIN/BACKGROUND:

- Enacted to bolster the U.S. semiconductor industry, ensuring leadership in chip technology and manufacturing.
- Addresses national security concerns and the strategic importance of semiconductors in modern technology.

EFFECTIVE DATE:

- Signed into law in August 2022.

RESOURCES

The CHIPS and Science Act: A Game-Changer in its First Year. (n.d.). Energy.gov.

PricewaterhouseCoopers. (2022). The CHIPS Act: What it means for the semiconductor ecosystem. PwC.

The White House. (2022, August 9). FACT SHEET: CHIPS and Science Act Will Lower Costs, Create Jobs, Strengthen Supply Chains, and Counter China. The White House.

About Cycuity

Cycuity gives companies the power to mitigate hardware vulnerabilities before manufacturing, saving time, money—and reputation.

Cycuity was created as Tortuga Logic in 2014 by co-founders with a shared vision: to revolutionize cybersecurity with trusted microelectronics.

Today, we remain committed to the belief that a secure design lifecycle is essential—from the design & verification chain into post-silicon.

Silicon chip vulnerabilities have the potential to exploit weaknesses in chip design and firmware, and cause irreparable damage to companies who build or rely on semiconductor technology.

At Cycuity, we're working towards a world where the products that enrich, inform, and protect our lives aren't just secure—they're backed by the confidence of hardware security assurance.

Our security experts are dedicated to helping clients enhance their security measures, and through our products and consultation, we provide valuable best practices and a methodology for establishing a robust hardware security program.

Learn more at Cycuity.com