D2.3 Cybersecurity measures implementation report

Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and AI

Jul 12, 2025

ITEA Project No: 22006

sintra-ai.eu

ITEA 4

DOCUMENT VERSIONS

Version no	Date	Changes
0.1	July 12, 2025	First concept
0.2	August 15, 2025	Lots of changes
0.3	August 21, 2025	Introduction who, why

CONTENTS

1 INTRODUCTION

In the ITEA - Sintra project, we aim to detect anomalies using various sensors and databases. By employing algorithms and machine learning (artificial intelligence), we want to identify abnormalities in logistical hubs such as seaports, train stations, industrial sites, and airports. The use of sensors is already commonplace and widely implemented. These sensors serve as essential conduits for data collection and control, enabling unprecedented levels of automation, efficiency, and insight. However, this pervasive integration, coupled with increasing connectivity, introduces a complex array of cybersecurity risks. The imperative for organizations to effectively measure and manage these risks is paramount, as sensor compromise can lead to severe consequences, including data integrity issues, operational disruption, significant financial losses, and even direct threats to public safety and human life.

Three question arise when we talk about cyber attacks at the logistic hubs:

1. Who is the attacker?
2. What is the reason to attack?
3. What is the impact?

1.1 Who

The threat landscape for harbours and airports is populated by a diverse range of actors, each with distinct capabilities and objectives. These actors can be broadly categorized into four groups, ranging from well-resourced state-sponsored entities to individuals driven by personal grudges.

1.1.1 Nation-State and State-Sponsored Actors: The Well-Funded Adversary

Nation-state and state-sponsored actors represent the most sophisticated and well-resourced threat to critical infrastructure. Their operations are not typically for financial gain but are strategically aligned with national security, espionage, military, or political objectives. Their primary aim is often to establish a long-term, persistent presence within a target network, allowing them to conduct espionage, steal intellectual property, or prepare for future disruptive or destructive operations.

1.1.2 Ideologically Motivated Hacktivists: The Political Proxy

Hacktivists are groups or individuals who use cyber-attacks to protest or promote a particular political or ideological agenda. Unlike nation-states, their objectives are often short-term and focused on public disruption, embarrassment, or shaming.[15] They serve as a proxy for state-level interests, expanding the battlefield beyond military targets to include civilian infrastructure.[3]

1.1.3 Financially Driven Cybercriminal Organizations: The Economic Predator

Cybercriminal organizations are motivated by a single, clear objective: money. They operate with a "wide net" approach, often targeting critical infrastructure because these sectors' reliance on

time-sensitive data and operations makes them more likely to pay a high ransom to restore services quickly.

1.1.4 The Insider Threat: The Human Element

The insider threat encompasses both malicious and unintentional actions by current or former employees. These actors are a significant vector for security breaches due to their pre-existing knowledge of and access to internal systems. Research indicates that former employees with a "grudge" may attempt to cause embarrassment or pain to their former employers. On the other hand, unintentional human error, such as losing a USB key with confidential data, can also lead to a major security incident. One survey found that 20% of data breaches were caused by former employees, highlighting a persistent risk.

1.2 Why

The incentives behind cyber-attacks on harbours and airports are diverse and often overlapping. A comprehensive understanding of the "why" is crucial for developing effective defensive strategies.

1.2.1 Geopolitical Objectives and Hybrid Warfare

In the modern geopolitical landscape, cyberspace has emerged as a new battlefield where conflicts are waged below the threshold of traditional, conventional warfare. Cyber-attacks on critical infrastructure serve as a powerful tool for achieving strategic objectives, such as retaliation, intimidation, and destabilization. This form of hybrid warfare blurs the lines between military and civilian targets, and between state and non-state actors.

The sources demonstrate a critical transition from intelligence gathering to active sabotage in a conflict-related context. Nation-states have long been focused on espionage and data exfiltration to gain an economic or political advantage. However, as seen in the Russian-Ukraine conflict, the motivation can shift to "inflicting damage" and disrupting services to undermine an adversary's capabilities. This evolution means that the nature of the threat transforms from stealth and persistence to overt disruption and destruction, with the potential for devastating effects on civilian populations.[5] This is exemplified by the Killnet attacks on US airports, which were not about data theft but about a symbolic "declaration of war" and public disruption.[16]

1.2.2 Financial Extortion and Data Monetization

For financially motivated actors, harbours and airports are highly attractive targets due to their time-sensitive operations and the high cost of downtime.[18] These actors use a range of tactics to monetize their intrusions.

- **Ransomware:** This is a prevalent tactic where attackers encrypt a victim's systems and demand a ransom payment to restore access.[25] The average cost of a ransomware attack,

excluding the ransom itself, is estimated at $4.54 million.[18] The Port of Nagoya incident is a clear example, as the LockBit group demanded a ransom for the recovery of the port's system.[19]

- **Data Monetization:** In many cases, attackers will steal sensitive data and either sell it on the black market or use it as leverage in a "double extortion" scheme, threatening to release the data publicly if the ransom is not paid.[15] The 2018 Cathay Pacific and British Airways breaches, which compromised the personal data of millions of customers, illustrate the immense value of this information to criminals.[11]

1.2.3 Espionage and Economic Advantage

Cyber espionage is a key motivation for nation-states and is often a prelude to or a parallel activity with sabotage.[5] The theft of intellectual property, trade secrets, and classified government documents can provide a nation with a significant economic or military advantage over rivals.[5] The FSB's activity of collecting configuration files for thousands of networking devices in critical infrastructure sectors across the globe is a prime example of this reconnaissance-focused espionage.[7] This activity is not necessarily to cause immediate disruption but rather to map out networks, identify vulnerabilities, and maintain persistent access for a future operation. The targeting of private organizations, government personnel, and even cybersecurity companies by state actors suggests a wide-ranging campaign to gain strategic intelligence.

Threat Actor/Group Type	Primary Motivations	Secondary Motivations	Typical Tactics
Nation-State Actors (FSB, APT28, Volt Typhoon)	Political/Geopolitical Influence Espionage Sabotage	Economic Advantage Military Objectives	Advanced Persistent Threats (APTs), Destructive Malware, Supply Chain Compromises, Zero-Day Exploits, Reconnaissance
Ideologically Motivated Hacktivists (Killnet, Cyber Av3ngers)	Ideological/Political Beliefs Public Dissent Retaliation	Shaming/Embarrassment Propaganda	Distributed Denial of Service (DDoS), Website Defacement, Data Exfiltration
Financially Driven Cybercriminals (LockBit, Rhysida, Scattered Spider)	Financial Gain (Ransom, Data Sale)	Espionage (Corporate) Personal Vendettas	Ransomware, Phishing/Social Engineering, Malware, Double Extortion
The Insider Threat (Current or Former Employees)	Revenge Sabotage Financial Gain	Unintentional Error Intellectual Property Theft	Unauthorized Data Access, System Disruption, Misconfiguration

1.3 Impact

A cyberattack on sensors at an airport or harbour could lead to **catastrophic physical and logistical impacts**. While the attack itself is digital, the consequences are very much real, affecting safety, operations, and the economy. These facilities rely on a complex web of interconnected sensors for everything from navigation and security to logistics, making them especially vulnerable.

1.3.1 Impact at an Airport

The aviation industry is a prime target for cyberattacks due to its critical role in global travel and commerce. Compromised sensors can directly affect public safety and bring operations to a standstill.

- **Air Traffic Control (ATC):** A successful attack could manipulate the data used by air traffic controllers. For example, by sending **false sensor readings**, attackers could create ghost planes on radar screens or make real planes appear to be in the wrong location, leading to potential mid-air collisions or runway incidents.
- **Physical Security:** Airports use a vast number of sensors for security, including biometric scanners, access control systems, and surveillance cameras. Hacking these sensors could allow unauthorized individuals to bypass checkpoints, access secure areas, or even plant dangerous materials without being detected.
- **Operational Disruption:** Sensors are vital for managing ground operations. An attack could disrupt baggage handling systems, fuel delivery sensors, or runway lighting controls, causing massive flight delays and cancellations. A ransomware attack could encrypt data from these sensors, locking airport personnel out of critical systems until a ransom is paid.

1.3.2 Impact at a Harbour

Harbors are essential hubs for global supply chains. A cyberattack on their sensors can create widespread economic disruption and security risks.

- **Cargo and Logistics:** Harbors use sensors to track and manage cargo containers. An attacker could manipulate this data to misroute cargo, steal valuable goods, or cause delays by creating false inventory records. This can bring port operations to a halt, affecting global supply chains and causing significant financial losses.
- **Navigation and Positioning:** The maritime industry relies heavily on GPS and other navigation sensors. A cyberattack could **spoof** these signals, leading to ships veering off course, potentially causing collisions or grounding in a busy harbour. A ship's Automated Identification System (AIS), which transmits its position, could be manipulated to hide a vessel or create a false one, posing a serious security threat.

- **Physical Infrastructure:** Harbours use sensors to monitor the status of cranes, docks, and automated guided vehicles (AGVs). By compromising these sensors, attackers could cause equipment to malfunction, leading to physical damage, accidents, or the inability to load and unload cargo. This type of attack has the potential for both economic and environmental disaster, such as a major oil spill from a compromised tanker.

1.3.3 Case Studies in Impact and Resilience

Examining specific cyber incidents provides a concrete understanding of the threat landscape and the real-world implications of successful attacks. The following table and detailed case studies highlight the diversity of threats and their consequences.

Incident/Victim	Threat Actor	Primary Motivation	Attack Vector/Vulnerability	Operational Impact	Financial Impact
NotPetya on Maersk (2017)	NotPetya (Russian-affiliated)	Disruption/Sabotage	Supply Chain Compromise, Unpatched Systems (EternalBlue, Mimikatz)	76 global port terminals shut down. Maersk's systems crippled for 6-12 days.	~$300 million USD [12]
Port of Nagoya Ransomware (2023)	LockBit (RaaS group)	Financial Gain	Ransomware Attack on OT Systems	Container operations halted for more than 24 hours.	Ransom demanded, but not paid.
Killnet DDoS on US	Killnet (Hacktivist group)	Political Retaliation (Pro-Russian)	Distributed Denial of Service (DDoS) on public-	Website paralysis for over 40 US	High cost in lost revenue

Incident/Victim	Threat Actor	Primary Motivation	Attack Vector/Vulnerability	Operational Impact	Financial Impact
Airports (2022)			facing websites	airports; no impact on flight ops.	s, but no stated figure.
Seattle-Tacoma Airport (SEA) (2024)	Rhysida (Ransomware group)	Financial Gain	Ransomware Attack, Data Exfiltration	Multiple airport services disrupted; 90,000 employee data compromised.	~$6 million USD ransom demanded, not paid. Data leaked online. 21
SITA Data Breach (2021)	Cybercriminal Group	Financial Gain (Data Monetization)	Compromised vendor, Data exfiltration	Sensitive data of 2 million frequent-flyer accounts breached.	Fines and legal costs.

1.4 Conclusion

This report provides a comprehensive guide to understanding and measuring the cyber risks associated with sensors. It delves into the diverse landscape of sensor types and their applications, highlights the unique cybersecurity challenges inherent in these systems, and outlines common threat vectors. The report then explores established cybersecurity risk assessment frameworks,

including those from NIST, ISO, OWASP, ISA/IEC 62443, and FDA, detailing their specific applicability to sensor environments. It differentiates between quantitative and qualitative metrics for robust risk measurement and identifies specialized tools and best practices for effective risk management. Finally, real-world case studies illustrate the tangible impacts of sensor compromise, reinforcing the critical need for a proactive and adaptive approach to securing these vital components.

Digital security has traditionally been viewed as a challenge primarily for administrative organizations. Unfortunately, sensors are now also vulnerable to digital attacks, which can cause massive logistical congestion or disruptions to operational continuity. Especially with the extensive connectivity of sensors—sometimes called the 'Internet of Sensors'—it is crucial to measure and assess the cybersecurity of sensors before they are deployed. This involves identifying and mapping potential risks to prevent security breaches.

Additional Context & Clarification:

This project highlights the importance of cybersecurity in the deployment of sensor networks used in critical logistics and infrastructure. Because sensors are integral to operational processes, any cyber-attack can have severe consequences—from logistical delays to safety hazards. As sensors become more connected and embedded in complex systems, understanding and mitigating these risks is essential.

The distinction between technical risks (vulnerabilities in the hardware/software) and ethical/legal/social risks (privacy issues, misuse, compliance, societal impact) ensures a comprehensive approach to cybersecurity—covering both technological safeguards and responsible usage.

2 UNDERSTANDING THE SENSOR LANDSCAPE AND ASSOCIATED RISKS

2.1 Diversity of Sensors and Their Applications

Sensors are fundamental to modern technological ecosystems, acting as the eyes and ears of interconnected systems. Their diversity is vast, encompassing various types that operate on different principles and serve distinct purposes across numerous sectors. This wide array of applications means that the cybersecurity considerations for one type of sensor or deployment may differ significantly from another.

For **national security and critical infrastructure**, radar sensors are vital electronic security systems. They transmit electronic signals that bounce off objects, returning to a receiver for analysis, and are used to monitor national and international borders, military bases, airports, seaports, refineries, and other critical industries. Radar sensors can detect ground-level movements from several kilometres away and are also deployed in aircrafts, ships, and submarines. Satellite systems, placed in orbit, use cameras for Earth imaging, contributing to national security. Optical sensors like lidar (light detection and ranging), often mounted on Unmanned Aerial Vehicles (UAVs), are employed for efficient and reliable security applications, processing images for analysis.

Within **industrial and commercial settings**, sensors are integral to operations, safety, and access control. Biometric access control systems, typically using fingerprints, are common in industries, commercial establishments, and offices for authentication and time attendance. RFID-based proximity access systems are inexpensive, quick, and widely used for door and gate entry in offices, factories, and banks, sometimes proving more effective than video surveillance. Chemical sensors detect organic compounds in gases, with applications in homeland security, bomb detection, and sensing toxic industrial materials. Magnetic sensors, including anisotropic magneto resistor (AMR), giant magneto-resistance (GMR), and giant magneto-impedance (GMI) sensors, are used in many security and military systems. Industrial security solutions often integrate fire alarms, chemical sensors, access control systems, video surveillance, and intrusion detection systems. Beyond security, industrial applications extensively use accelerometers, gyroscopes, temperature sensors (thermocouples, RTDs, thermistors), vision and imaging sensors, proximity sensors (capacitive, inductive, ultrasonic, optical, acoustic), infrared (IR) sensors, radiation sensors, and particle sensors (e.g., aerosol particle sensors for air quality).

The pervasive and diverse attack surface presented by sensors is a critical consideration. The sheer variety of sensor types (active/passive, analogue/digital), their diverse applications (from consumer to critical infrastructure), and the range of environments they operate in (indoor, outdoor, embedded, connected) mean that a "one-size-fits-all" security solution is impractical. This inherent diversity creates a vast and complex attack surface where vulnerabilities in one type or application can have cascading effects across interconnected systems. The criticality of the

application, such as in medical devices or industrial control systems, directly correlates with the potential impact of a cyber incident. Consequently, measuring cyber risk for sensors must be context-specific, taking into account the sensor's function, its operational environment, its connectivity, and the potential consequences of its compromise. A generic approach will inevitably fail to capture the necessary nuances of risk.

Sensor Type	Typical Applications	Key Data Collected	Potential Impact Categories (Safety, Operational, Financial, Privacy)	Criticality Level
Radar Sensors	National/International Borders, Military Bases, Airports, Seaports, Refineries, Aircraft, Ships, Submarines	Movement, Distance, Speed	High (Safety, Operational, Financial)	High
Lidar Sensors	UAVs/Drones for Security, Autonomous Vehicles	3D Mapping, Object Detection, Distance	High (Safety, Operational, Financial)	High
PIR Sensors	Home Security, Burglar Alarms	Infrared Radiation (Human/Animal Presence)	Low (Privacy, Financial), Medium (Operational)	Low-Medium
Ultrasonic Sensors	Home Security, Motion Detection	Reflected Ultrasonic Waves (Object Movement)	Low (Privacy, Financial), Medium (Operational)	Low-Medium
Tomographic Sensors	Warehouses, Large Storage Units, Home Security	Radio Wave Disturbances (Presence, Movement)	Low (Privacy, Financial), Medium (Operational)	Low-Medium
Biometric Access Control	Industries, Commercial Establishments, Offices	Fingerprints, Other Biometric Data	Medium (Privacy, Financial), High (Operational)	Medium-High
Chemical Sensors	Homeland Security, Industrial Safety, Bomb Detection	Organic Compounds, Toxic Vapours	High (Safety, Operational, Financial)	High
Magnetic Sensors	Security, Military Systems	Magnetic Fields	High (Safety, Operational)	High
Temperature Sensors	Industrial Control, Home Automation, Medical Devices	Temperature (Contact/Non-Contact)	Medium (Operational, Financial), High (Safety in Medical/Industrial)	Medium-High
Vision/Imaging Sensors	Industrial Quality Control, Surveillance, Smart Cities	Visual Images, Object Presence/Colour	Medium (Operational, Financial), High (Privacy, Safety in critical apps)	Medium-High
Proximity Sensors	Industrial Automation, Robotics, Smart Devices	Presence/Absence of Objects without Physical Contact	Medium (Operational, Financial)	Medium
Infrared (IR) Sensors	Thermal Imaging, Gas Detection, Remote Control	Infrared Radiation	Medium (Operational), High (Safety in specific applications)	Medium-High
Radiation Sensors	Nuclear Facilities, Medical Imaging, Security	Radiation Emissions/Levels	High (Safety, Operational, Financial)	High

Particle Sensors	Air Quality Monitoring, Industrial Processes	Aerosol, Solid, Liquid Particle Counts/Sizes	Medium (Health, Operational)	Medium
Smart City Sensors	Traffic, Energy Usage, Pollution, Parking	Traffic Volume, Energy Consumption, Air Quality	Medium (Operational, Financial), High (Privacy, Public Safety)	Medium-High

2.2 Unique Cybersecurity Challenges of Sensor Systems

Sensor systems, particularly those integrated into the Internet of Things (IoT), Industrial Control Systems (ICS), and medical devices, present distinct cybersecurity challenges that differentiate them from traditional IT environments. These challenges are often rooted in the fundamental design and operational characteristics of sensors, which can inherently limit their security capabilities.

A primary challenge stems from **resource constraints**. Many IoT and embedded sensors are designed as low-power devices with minimal processing power, limited memory, and restricted battery life, often expected to last for years. These constraints severely limit the complexity of security measures that can be implemented directly on the device, such as robust encryption algorithms, complex authentication protocols, or comprehensive logging capabilities. For instance, sending even a small amount of temperature data with security measures like TLS encryption can require thousands of additional bytes, significantly impacting power consumption. This often forces a trade-off between security and power efficiency, leading to simplified mechanisms that are more vulnerable to compromise.

Closely related are **limited interfaces and connectivity**. While some sensors may have multiple interfaces like Wi-Fi, Bluetooth, Ethernet, or USB , others are designed with minimal connectivity or rely on gateways and hubs for communication. This can make direct access for traditional security controls, such as direct patching or comprehensive monitoring, challenging.

The prevalence of **legacy systems and outdated components** is a significant concern, particularly in Industrial Control Systems (ICS) and medical devices. ICS often relies on decades-old equipment and outdated operating systems, such as Windows XP, which no longer receive security updates, making them easy targets for attackers. Similarly, medical devices frequently utilize legacy systems that lack modern security controls, have hardcoded credentials, or possess no patching mechanism at all. While still clinically functional, these devices present long-term exposure to preventable risks, and open vulnerabilities in older products can create lingering liability for manufacturers.

A pervasive issue is the **lack of secure update mechanisms**. Many IoT devices lack robust and secure methods for delivering firmware and software updates. Without features like code signing,

encryption during transit, or anti-rollback mechanisms, attackers can intercept updates or inject malicious firmware into devices, leaving them permanently vulnerable.

Furthermore, many devices are shipped with **insecure default settings and hardcoded credentials**. Easily guessable default passwords or hardcoded credentials that cannot be changed provide predictable entry points for attackers, making devices vulnerable "out of the box".

Physical vulnerabilities are also a concern. Sensors are often deployed in environments where physical access is possible, yet they may lack physical hardening, tamper detection, or secure boot mechanisms. This allows attackers to access internal components, extract firmware, or physically manipulate the device, potentially leading to data corruption or system compromise.

Finally, **supply chain risks** introduce vulnerabilities even before deployment. IoT devices frequently incorporate third-party software libraries or hardware components that may be outdated or contain known vulnerabilities. If manufacturers fail to provide timely updates or patches for these components, security risks are introduced. In the healthcare sector, supply chain compromises affecting medical devices are a significant concern, as they can impact multiple organizations simultaneously and are often harder to detect until widespread damage occurs.

These constraints are not minor issues but fundamental vulnerabilities. They directly cause or exacerbate common security flaws, such as weak authentication, lack of encryption, and poor update mechanisms. For instance, a low-power device might be compelled to use simplified cryptography, making it inherently less secure. This implies that risk mitigation strategies cannot simply port traditional IT security controls but must be adapted. This often involves offloading security logic to the network or implementing compensating controls at the system level, shifting the focus from securing the device itself to securing the entire ecosystem around it.

2.3 Common Cyber Threats and Vulnerabilities Targeting Sensors

The unique characteristics of sensors and their operational environments make them susceptible to a specific set of cyber threats and vulnerabilities. Understanding these is crucial for effective risk measurement and mitigation. The OWASP IoT Top 10 provides a widely recognized baseline for identifying critical vulnerabilities in IoT devices.

OWASP IoT Top 10 Vulnerabilities:

1. **Weak, Guessable, or Hardcoded Passwords:** The use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware, provides predictable entry points for attackers.

2. **Insecure Network Services:** Devices often expose unnecessary network services, such as legacy protocols like Telnet or FTP, which may have exploitable vulnerabilities and often run with elevated privileges, allowing attackers to gain control.
3. **Insecure Ecosystem Interfaces:** Web portals, APIs, or mobile applications linked to IoT devices can suffer from poor security practices like weak authentication, poor session management, or lack of encryption, leading to unauthorized access.
4. **Lack of Secure Update Mechanism:** Many devices lack a secure mechanism for delivering updates, making them vulnerable to interception or injection of malicious firmware without features like code signing or encryption.
5. **Use of Insecure or Outdated Components:** Reliance on deprecated or insecure third-party software libraries or hardware components, especially when manufacturers fail to provide timely updates, introduces significant security risks.
6. **Insufficient Privacy Protection:** IoT devices often handle sensitive personal data (e.g., health or location data). Transmitting unencrypted data or insecure storage can expose users to identity theft or surveillance.
7. **Insecure Data Transfer and Storage:** A lack of encryption or access control for sensitive data, whether at rest, in transit, or during processing, can lead to compromise.
8. **Lack of Device Management:** Absence of robust device management capabilities, including centralized control, inventory, and monitoring, leaves devices vulnerable to unaddressed issues.
9. **Insecure Default Settings:** Devices are often shipped with vulnerable default configurations, such as open ports or unnecessary services, which users rarely modify.
10. **Lack of Physical Hardening:** Devices deployed in accessible environments may lack protections like tamper detection or secure boot mechanisms, allowing attackers to access internal components or manipulate the device.

Beyond these vulnerabilities, several common attack methods specifically target sensor-enabled systems:

- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:** These aim to overwhelm the resources of a device or network, making it unavailable to legitimate users. This can halt industrial processes, disrupt communications, or take systems offline. A more severe form, Permanent Denial of Service (PDoS) or "phlashing," can damage devices so badly they require replacement or hardware reinstallation.

- **Man-in-the-Middle (MITM) Attacks:** Attackers breach, interrupt, or spoof communications between two systems. This can lead to unauthorized control or data manipulation, such as altering insulin dosage instructions in medical devices, siphoning energy from smart meters, or remotely controlling water systems in smart cities.
- **Firmware Reverse Engineering and Manipulation:** Attackers can obtain device firmware (e.g., by downloading from a manufacturer's website or physically dumping it from memory) and analyse it to understand device functionality, discover hardcoded credentials, or find vulnerable code paths. Malicious code can then be inserted into the firmware to compromise operations, often remaining undetected until significant damage occurs.
- **Side-Channel Attacks:** These attacks exploit information leaked through the physical implementation of a cryptographic system, such as power consumption, electromagnetic emissions, or timing variations.
- **Botnets:** Compromised IoT devices are often recruited into large-scale botnets, which can then be used to launch distributed attacks against other targets.
- **Credential Harvesting and Theft:** Attackers use phishing campaigns or other methods to trick employees or contractors into revealing credentials, granting unauthorized access to ICS networks or other sensor-dependent systems.
- **Physical Tampering:** Direct physical access to devices allows attackers to extract firmware, tamper with internal components, or manipulate the device's functionality.
- **Rogue Devices and Spoofing:** This involves introducing unauthorized devices into a network or impersonating legitimate ones. Examples include GPS spoofing, where falsified GPS signals are broadcast to manipulate a device's perceived location , or the "illusion attack" where sensing data is purposely manipulated to produce falsified information, potentially leading to accidents or traffic jams.
- **Malware and Ransomware:** These attacks specifically target ICS to disrupt industrial operations, encrypt critical data, or cause widespread damage. The 2017 WannaCry attack, for instance, spread from infected IT systems to connected medical devices, disrupting patient care.
- **Advanced Persistent Threats (APTs):** Sophisticated, long-term attacks designed to infiltrate ICS networks and remain undetected for extended periods, aiming to gather sensitive information, manipulate system operations, or sabotage infrastructure.
- **Zero-Day Vulnerabilities:** Exploiting unknown or newly discovered flaws in ICS software or hardware before patches are available, making them particularly dangerous.

- **Data Theft and Privacy Breaches:** The vast amounts of sensitive personal data collected by smart city sensors (e.g., surveillance cameras, traffic signals, parking meters) or medical devices (e.g., patient health information) are prime targets for identity theft or surveillance.
- **Device Hijacking:** Attackers gain control of a device to exploit other devices on the network, such as exploiting smart meters to launch a ransomware attack on a city's energy management system.

The impact of these compromises extends far beyond traditional data theft. For sensors, especially in Industrial Control Systems (ICS) and medical contexts, the consequences can be severe, including disruption of critical processes, significant financial losses, and potential safety hazards. For medical devices, cyberattacks have a direct impact on patient care, forcing "life-or-death decisions" and compromising "operational continuity". The IEC 62443 standard, which governs ICS security, explicitly prioritizes safety and availability over confidentiality, reflecting the severe physical consequences of compromise. Attacks like DoS, firmware manipulation, and sensor spoofing directly target operational integrity and safety. Therefore, measuring cyber risk for sensors must explicitly incorporate safety and operational continuity as primary impact categories, moving beyond traditional IT risk assessments. The "consequence" factor in risk calculation (Risk = Likelihood x Consequence) must weigh these physical and human safety impacts heavily.

Vulnerability/Attack Vector	Description	Typical Impact on Sensors	Relevant OWASP IoT Top 10 ID
Weak, Guessable, or Hardcoded Passwords	Default, easily brute forced, or unchangeable credentials.	Unauthorized access, device hijacking, data manipulation.	I1
Insecure Network Services	Unnecessary or vulnerable services (e.g., Telnet, FTP) running on device.	Remote control, data exfiltration, device compromise.	I2
Insecure Ecosystem Interfaces	Weak authentication, poor session management, lack of encryption in web/API/mobile interfaces.	Unauthorized access to device/data, system compromise.	I3
Lack of Secure Update Mechanism	No firmware validation, unencrypted delivery, no anti-rollback.	Malicious firmware injection, device bricking, persistent compromise.	I4
Use of Insecure or Outdated Components	Deprecated third-party software/hardware with known vulnerabilities.	Exploitable entry points, supply chain attacks, system instability.	I5
Insufficient Privacy Protection	Unencrypted transmission or insecure storage of sensitive data.	Identity theft, surveillance, privacy breaches.	I6

Insecure Data Transfer and Storage	Lack of encryption/access control for sensitive data at rest, in transit, or during processing.	Data theft, data manipulation, unauthorized access.	I7
Lack of Device Management	Absence of centralized control, inventory, and monitoring.	Unpatched vulnerabilities, unaddressed incidents, rogue devices.	I8
Insecure Default Settings	Open ports, unnecessary services, weak configurations out-of-the-box.	Easy exploitation, unauthorized access.	I9
Lack of Physical Hardening	No tamper detection, secure boot, easy access to internal components.	Physical tampering, firmware extraction, device manipulation.	I10
Denial of Service (DoS/DDoS/PDoS)	Overwhelming device/network resources with traffic.	Device/system unresponsiveness, operational shutdown, physical damage (PDoS).	-
Man-in-the-Middle (MITM)	Intercepting and altering communications between systems.	Data manipulation (e.g., dosage, readings), unauthorized control.	-
Firmware Reverse Engineering/Manipulation	Analysing/modifying device firmware to insert malicious code.	Sabotage, unauthorized control, persistent compromise.	-
Side-Channel Attacks	Exploiting information leaked through physical implementation (e.g., power consumption).	Extraction of cryptographic keys, sensitive data.	-
Botnets	Compromised IoT devices recruited for large-scale distributed attacks.	Device resource exhaustion, launching attacks against other targets.	-
Credential Harvesting/Theft	Gaining access to user/system credentials.	Unauthorized network access, data theft, system control.	-
Rogue Devices and Spoofing	Introducing unauthorized devices or impersonating legitimate ones (e.g., GPS spoofing, illusion attack).	Falsified data, incorrect control actions, safety hazards.	-
Malware/Ransomware	Malicious software disrupting operations, encrypting data, gaining control.	Operational disruption, data loss, financial losses.	-
Advanced Persistent Threats (APTs)	Sophisticated, long-term infiltration for espionage/sabotage.	Extensive data theft, operational manipulation, infrastructure sabotage.	-
Zero-Day Vulnerabilities	Exploiting unknown or unpatched software/hardware flaws.	Immediate exploitation, significant breaches.	-

Data Theft/Privacy Breaches	Unauthorized access to sensitive data collected by sensors.	Identity theft, surveillance, regulatory fines.	-
Device Hijacking	Gaining full control over a sensor device.	Exploiting other network devices, launching further attacks.	-

3 FRAMEWORKS FOR CYBER RISK MEASUREMENT AND ASSESSMENT

Effective measurement of cyber risks for sensors necessitates a structured approach, often guided by established cybersecurity risk assessment frameworks. These frameworks provide methodologies for identifying, analysing, evaluating, and treating risks, ensuring that security controls are implemented strategically.

3.1 Foundational Principles of Cybersecurity Risk Assessment

Cybersecurity risk assessment fundamentally involves evaluating the likelihood of potential cyber threats and the magnitude of their impact on organizational operations, assets, individuals, and other organizations. This process focuses specifically on risks related to the loss of confidentiality, integrity, or availability of information, data, or information systems within cyberspace.

The typical steps in a comprehensive risk assessment include:

1. **Preparation:** Defining the scope, purpose, and context of the assessment, including what assets will be assessed, the methodology, and any assumptions or constraints.
2. **Conducting the Assessment:** This involves identifying potential threat sources and events, recognizing vulnerabilities and predisposing conditions, determining the likelihood of a threat successfully exploiting a vulnerability, and assessing the potential consequences if an exploitation occurs.
3. **Communication:** Documenting and sharing findings with relevant stakeholders to ensure decision-makers understand the risks.
4. **Maintenance:** Continuously monitoring and updating risk assessments as the IT environment and threat landscape evolve.

Risk is commonly determined by combining the likelihood of a threat event occurring with the magnitude of its impact. This foundational understanding underpins most modern cybersecurity risk management practices.

A critical aspect of risk management, particularly for sensors, is recognizing that risk is a dynamic, lifecycle-based process. Multiple frameworks, including ISO 27005 , NIST , IEC 62443 , and FDA guidance , consistently emphasize that risk assessment is not a one-time event but a continuous, iterative process. ISO 27005, for instance, highlights that "risks are dynamic and can change rapidly" and "should be actively monitored". Similarly, the FDA's Secure Product Development Framework (SPDF) is described as a "lifecycle-based approach". This continuous nature is especially critical for sensors, which often have long deployment lifecycles and may receive infrequent updates, making them susceptible to newly discovered vulnerabilities over time. Therefore, measuring cyber risk for sensors requires a commitment to ongoing monitoring, reassessment, and adaptation of security controls throughout the device's operational life, not

merely at the point of deployment. This includes continuous vulnerability monitoring, effective patch management, and robust incident response planning.

3.2 Key Industry Frameworks and Their Applicability to Sensors

Several prominent cybersecurity frameworks offer structured guidance for measuring and managing risks, each with specific strengths and applicability to sensor systems.

3.2.1 NIST Cybersecurity Framework (CSF) and SP 800-213

The National Institute of Standards and Technology (NIST) provides a comprehensive approach to IoT cybersecurity that is outcome-based and adopts an ecosystem perspective. This approach acknowledges that much of the functionality and security for IoT devices often occurs outside the device itself, making it crucial to consider the entire environment rather than just endpoints. The primary goal is to help organizations understand how IoT devices can affect cybersecurity risk and to provide guidance for securely integrating them into existing systems.

NIST's guidance for IoT devices emphasizes a risk-based understanding, recognizing that IoT capabilities, behaviours, and deployment environments significantly influence cybersecurity risk. It also adheres to a "no one size fits all" principle, allowing for flexibility in guidance due to the vast variety of IoT devices and their diverse uses.

NIST Special Publication 800-213 specifically guides organizations in identifying **device cybersecurity requirements**. These requirements encompass both technical features residing on the device (device cybersecurity capabilities) and actions expected from manufacturers or third parties (non-technical supporting capabilities). A catalogue of these requirements, derived from NIST SP 800-53 Rev. 5 security controls, is available in SP 800-213A.

A significant contribution of NIST SP 800-213 is its explicit address of **resource constraints** (e.g., limited storage, memory, or processing power) and **limited interfaces** of IoT devices. It suggests that if a constrained IoT device cannot provide all desired cybersecurity capabilities internally, organizations may need to provide them through other system elements or by implementing compensating controls, such as network segmentation. This reflects the reality that manufacturers might build fewer capabilities into devices due to cost and complexity, shifting security responsibilities to other parts of the ecosystem.

The key goals within the NIST framework for IoT devices are to **Protect Device Security** (preventing devices from being used to conduct attacks like Distributed Denial of Service (DDoS) or eavesdropping on network traffic) and to **Protect Data Security** (ensuring the confidentiality, integrity, and availability of data collected by, stored on, processed by, or transmitted to or from the IoT device). Associated risk mitigation areas include robust asset management (maintaining a

current inventory of IoT devices), comprehensive data protection, effective incident detection, and proactive vulnerability management.

The NIST framework's emphasis on ecosystem-level security for constrained devices represents a crucial understanding. Instead of solely focusing on hardening the sensor itself, which may be impractical or impossible due to inherent limitations, the framework encourages organizations to consider how other system elements—such as gateways, network segmentation, or cloud platforms—can collectively provide the necessary security controls. This directly addresses the challenges posed by low-power, resource-constrained sensors. Therefore, effective risk measurement for constrained sensors involves evaluating the security posture of the *entire system* they are part of, including any compensating controls, rather than just the device's inherent capabilities. This necessitates assessing the security of the network infrastructure, cloud services, and management platforms that interact with the sensors.

3.2.2 ISO/IEC 27005 for Information Security Risk Management

ISO/IEC 27005 is a supporting standard to ISO 27001, providing structured guidance for identifying, assessing, treating, and monitoring information security risks. Its objective is to ensure that all controls within an Information Security Management System (ISMS) are driven by well-defined, risk-based decision-making.

The standard outlines a five-step process for information security risk management:

1. **Context Establishment:** This initial step involves defining the goals and criteria for information security risk management. For sensors, this means understanding their operational role, the sensitivity of the data they handle, potential safety impacts, and aligning these with overall business objectives and regulatory requirements.
2. **Risk Identification:** This step lays out two complementary approaches: **event-based**, which focuses on the organization's overall threat landscape, and **asset-based**, which is more granular, focusing on key risks and vulnerabilities associated with specific information assets. It requires listing all relevant assets (including sensors, their collected data, and supporting systems) and identifying associated risks and vulnerabilities.
3. **Risk Analysis:** This phase aims to narrow down which systems, services, and data are at risk and to determine the severity of each risk or vulnerability. ISO 27005 supports qualitative (e.g., "what-if" scenarios), quantitative (using data and numbers), and semi-quantitative (quantifying likelihood with statistical methods and defining impact subjectively) methods.
4. **Risk Evaluation:** Once risks have been analysed, organizations compare each risk against their predefined risk appetite or tolerance criteria to decide how to respond and prioritize treatment efforts.

5. **Risk Treatment:** This final step involves deciding on appropriate actions for identified risks. Options typically include **mitigation** (implementing controls to reduce likelihood or impact), **avoidance** (preventing circumstances where the risk could occur), **transfer** (sharing or transferring risk to a third party, e.g., through insurance or outsourcing), and **acceptance** (if the risk falls within established tolerance levels). Risk owners are responsible for creating and approving the treatment plan and accepting any residual risks.

Implementing ISO 27005 can present challenges, including resource constraints (time, personnel, budget), the inherent complexity of accurately identifying and evaluating risks, and the continuous effort required to keep pace with evolving cyber threats.

The framework's emphasis on qualitative, quantitative, and semi-quantitative analysis is particularly crucial for sensors. Given that sensor compromises can lead to diverse impacts—from data theft to severe operational disruption and physical harm—a purely quantitative (financial) approach might be insufficient. Qualitative methods allow for assessing impacts like reputational damage or safety risks that are harder to monetize directly. Therefore, measuring sensor risk effectively requires a flexible approach to risk analysis, combining numerical data (e.g., downtime costs) with expert judgment on non-financial impacts (e.g., patient safety, environmental damage). This necessitates cross-functional collaboration involving IT, Operational Technology (OT), safety, and business stakeholders to ensure a comprehensive view of risk.

3.2.3 OWASP IoT Security Guidance and Testing Methodologies

The OWASP (Open Worldwide Application Security Project) Internet of Things Project is designed to help manufacturers, developers, and consumers better understand the security issues associated with IoT and to enable informed security decisions when building, deploying, or assessing IoT technologies. The OWASP IoT Security Testing Guide (ISTG) provides a comprehensive methodology for penetration tests in the IoT field, offering flexibility to adapt to market innovations while ensuring comparability of test results.

Key components of OWASP's guidance applicable to sensors include:

- **OWASP IoT Top 10:** This list identifies the most critical web application security risks in IoT, serving as a baseline for vulnerability identification and risk assessment.
- **Firmware Analysis Project:** This project provides guidance for security testing vulnerabilities within device firmware. It includes steps for extracting file systems from various firmware files, performing static analysis of filesystem contents, emulating firmware, and conducting dynamic and runtime analysis. This is highly relevant for the embedded software often found in sensors.

- **IoTGoat:** A deliberately insecure firmware based on OpenWrt, designed to teach users about common IoT vulnerabilities through hands-on experience.

The ISTG outlines a robust penetration testing methodology for IoT, covering various components such as processing units, memory, firmware, data exchange services, internal interfaces, physical interfaces, wireless interfaces, and user interfaces. A common four-stage IoT risk assessment process, often aligned with OWASP's Application Security Verification Standard (ASVS), includes:

1. **Discovery:** Gaining a deep understanding of assets, likely attackers, and business impact, coupled with a security design review of IoT devices.
2. **Threat Modelling:** Identifying possible threat scenarios, assigning risk levels (impact and likelihood), and defining mitigating controls.
3. **Penetration Testing:** Conducting various activities, including testing physical IoT devices, wireless interfaces, authentication, and access control, to identify security vulnerabilities.
4. **Finalization:** Providing an IoT Security Risk Assessment Report detailing all identified risks and recommended controls, prioritized by impact and likelihood.

OWASP also provides or highlights various tools that aid in sensor security assessment, such as OWASP ZAP (a web application vulnerability scanner), Dependency Check/Track (for identifying vulnerable dependencies), Semgrep (for fast code and dependency scans), SonarQube (for static code analysis and vulnerability detection), and PMD (an extensible source code analyser).

OWASP's focus on firmware analysis, reverse engineering, and penetration testing represents a crucial understanding. This approach directly addresses the "black box" nature of many sensors, where traditional network scans might miss critical vulnerabilities embedded deep within the device. Since sensors often run proprietary embedded software, the ability to analyse firmware for hardcoded credentials, configuration flaws, weak cryptographic keys, and vulnerable code is paramount for measuring deep-seated risks that are not apparent from the network perimeter. Therefore, measuring sensor cyber risk requires specialized technical assessments that go beyond superficial scans, delving into the device's internal workings, firmware, and embedded software components. This often necessitates specialized tools and expertise in reverse engineering and embedded systems.

3.2.4 ISA/IEC 62443 for Industrial Control Systems (ICS)

The ISA/IEC 62443 series of standards provides a comprehensive and holistic approach to securing Industrial Automation and Control Systems (IACS), which are prevalent in critical infrastructure and manufacturing. This framework is distinct from traditional IT security in its prioritization: it places

Safety first, followed by **Availability**, then **Integrity**, and finally **Confidentiality** (SAIC). This prioritization reflects the severe physical, environmental, and public safety consequences that can arise from ICS compromise.

For asset owners, the standard recommends the creation of a **Cybersecurity Management System (CSMS)** to analyse, address, monitor, and continuously improve the system's security posture against risks, aligning with the company's risk appetite.

The risk assessment process within IEC 62443 involves several key steps:

- **Defining the System under Consideration (SuC):** Clearly delimiting the scope and boundaries of the system being assessed.
- **Threat and Vulnerability Identification:** Systematically identifying and analysing potential threats and vulnerabilities.
- **Risk Prioritization:** Prioritizing risks based on their potential consequences, while also defining asset criticality and operational dependencies.
- **Risk Formula:** The standard provides a formula for calculating risk: Likelihood of Event Occurring = Likelihood Threat Realized × Likelihood Vulnerability Exploited. And Risk = Likelihood Event Occurring × Consequence.
- **Types of Assessments:** It distinguishes between high-level risk assessments (supporting business rationale) and detailed risk assessments (ensuring specific technical countermeasures are included in the system design).

A core concept in IEC 62443 is the use of **Security Levels (SL)**, ranging from SL 1 to SL 4, which can be applied to zones, conduits, channels, and products. These levels define the required protection against attacks with varying resources, from casual exposure (SL 1) to intentional attacks with extensive resources (SL 4). The standard also emphasizes a

layered defence strategy, splitting facilities into security zones and linking them through monitored conduits to contain potential threats.

For **device security**, IEC 62443-4-2 defines specific security requirements for component types, including embedded devices (EDR), which are highly relevant to industrial sensors. These requirements cover foundational areas such as identification and authentication control, use control, system integrity, data confidentiality, restricted data flow, timely response to events, and resource availability.

IEC 62443 is particularly valuable because it "zooms in on shop-floor realities" and "speaks directly to the quirks—and risks—of pumps, drives, and PLCs that can't tolerate downtime". It guides risk

reviews that "fit real-world OT constraints". While the standard does not always explicitly detail how it handles resource constraints in the

assessment methodology itself, it implicitly acknowledges the need to apply countermeasures that respect these constraints and the real-time operational demands of industrial systems.

The critical distinction highlighted by IEC 62443 is its prioritization of Safety, then Availability, then Integrity, then Confidentiality (SAIC). This contrasts sharply with traditional IT's Confidentiality, Integrity, Availability (CIA) triad. For industrial sensors, a cyberattack can lead to "production stoppages, equipment damage, environmental disasters, public safety risks, and significant financial losses". The Olympic Pipeline case study, for example, demonstrated how SCADA system unresponsiveness and unmitigated pressure buildup resulted in deaths and environmental damage. This underscores that even if a data breach is considered low-risk in a traditional IT context, a vulnerability that could cause a physical malfunction or shutdown (e.g., sensor spoofing leading to incorrect control actions) must be treated as high-risk within an OT environment. Therefore, measuring risk for industrial sensors must explicitly prioritize potential safety and operational impacts over data confidentiality. Risk metrics and reporting should be designed to reflect this SAIC prioritization.

Framework	Primary Focus	Target Audience	Key Principles/Methodology	Handling Resource Constraints	Impact Prioritization	Key Deliverables/Outputs
NIST CSF (with SP 800-213)	Improving overall cybersecurity posture, especially for IoT integration.	Federal agencies, general organizations, IoT manufacturers.	Outcome-based, ecosystem approach; Identify, Protect, Detect, Respond, Recover functions. SP 800-213 identifies device & non-technical capabilities.	Acknowledges constraints; suggests compensating controls or offloading capabilities to other system elements (e.g., network segmentation).	CIA (Confidentiality, Integrity, Availability) - general IT focus, adapted for IoT.	Risk Assessment Reports, Cybersecurity Requirements Catalog (SP 800-213A), Device Cybersecurity Goals.
ISO/IEC 27005	Information Security Risk Management for ISMS (ISO 27001 compliance).	Organizations implementing an ISMS.	Five-step process: Context, Identification, Analysis (qualitative, quantitative, semi-quantitative), Evaluation, Treatment.	Acknowledges resource constraints as implementation challenges; framework is flexible to adapt.	CIA (Confidentiality, Integrity, Availability).	Risk Assessment Report, Risk Treatment Plan, Statement of Applicability (with ISO 27001/27002).

OWASP IoT Security Guidance	Understanding and testing security issues in IoT devices and applications.	Manufacturers, developers, consumers, penetration testers.	OWASP IoT Top 10 vulnerabilities, Firmware Analysis, 4-stage Penetration Testing (Discovery, Threat Modelling, Pen testing, Finalization).	Acknowledges low-power device vulnerabilities (e.g., power depletion attacks, crypto limitations); focuses on testing inherent device security.	CIA (Confidentiality, Integrity, Availability) - general application security focus.	IoT Security Testing Guide, Vulnerability Lists (Top 10), Firmware Analysis Reports, Penetration Test Reports.
ISA/IEC 62443	Securing Industrial Automation and Control Systems (IACS).	Asset owners, system integrators, product suppliers in OT/ICS.	Holistic approach (People, Process, Technology); CSMS; Risk Assessment (SuC, threats, vulnerabilities, criticality); Security Levels (SL 1-4) for zones/products.	Acknowledges "shop-floor realities" and "real-time constraints"; guides risk reviews that fit OT constraints; defines Embedded Device Requirements (EDR).	SAIC (Safety, Availability, Integrity, Confidentiality) - prioritized for OT.	Cybersecurity Management System (CSMS), Risk Assessment Reports, Security Level Targets, Device Security Requirements (IEC 62443-4-2).

4 QUANTITATIVE AND QUALITATIVE METRICS FOR RISK MEASUREMENT

Measuring cyber risks for sensors requires a blend of quantitative and qualitative approaches to capture both the numerical aspects of security posture and the nuanced understanding of potential impacts, especially those related to safety and operational continuity.

4.1 Quantitative Metrics and Key Performance Indicators (KPIs)

Quantitative metrics utilize data and numbers to define levels of risk, providing objective, measurable insights into the effectiveness of cybersecurity controls and the overall risk posture of an organization. These metrics are crucial for data-driven decision-making and demonstrating the return on investment (ROI) of security initiatives.

General cybersecurity metrics that are highly applicable to sensor systems include:

- **Level of Preparedness:** This metric assesses an organization's readiness to prevent, detect, and respond to cyber threats, encompassing technology, processes, and personnel.
- **Unidentified Devices on the Network:** Quantifying the number of unrecognized IoT devices connected to the network helps in understanding the scale of potential risk exposure. Maintaining a comprehensive device inventory log is essential for tracking this.
- **Intrusion Attempts:** Documenting the count and analysing the frequency of breach attempts provides insight into the level of interest from cybercriminals and the effectiveness of perimeter defences.
- **Data Loss Prevention (DLP) Effectiveness:** This gauges the system's ability to prevent unauthorized data access or leaks, calculated as the ratio of successfully thwarted data incidents to total attempts. Response time of the DLP system is also a key indicator.
- **Mean Time Between Failures (MTBF):** The average time interval between two successive system or component failures. A longer MTBF indicates more robust and reliable cybersecurity infrastructure, which is crucial for sensor systems that require high uptime.
- **Mean Time to Detect (MTTD):** The average duration it takes for the cybersecurity team to detect a potential security incident. A shorter MTTD implies quicker detection, allowing for faster response to mitigate risks.
- **Mean Time to Respond/Resolve/Mitigate (MTTR/MTTM):** This measures the average duration between the initial detection of an incident and when it is formally acknowledged or logged (MTTR), or the average time to repair/resolve the issue (MTTM). For medical devices, patch latency and mean time to mitigation are specifically tracked.

- **Uptime/Availability:** The percentage of time critical systems are operational. This is particularly vital for Industrial Control Systems (ICS) and medical devices, where downtime can have severe consequences.
- **Patching Cadence/Vulnerability Remediation:** Metrics include the percentage of devices with the latest security patches installed, the number of high-risk vulnerabilities identified, and the number of systems failing vulnerability scans, along with remediation plans. For medical devices, the percentage of resolved vulnerabilities is tracked.
- **Security Incident Count:** The number of reported cybersecurity incidents. A higher number of reported incidents can indicate that employees and stakeholders are recognizing issues and taking action, suggesting effective security awareness training.
- **Access Management Metrics:** This includes the user authentication success rate and the number of users with administrative access, indicating the strength and control of access policies.
- **Compliance Deficiencies:** The number of cybersecurity-related gaps identified during formal audits provides a direct measurement of regulatory adherence. Fewer deficiencies signal a stronger compliance posture.
- **Post-Deployment Remediation Time:** The average time needed to fix security bugs found after deployment, calculated by dividing total remediation time by the number of post-deployment security vulnerabilities.

Specific quantitative risk models also provide valuable numerical insights:

- **Annualized Loss Expectancy (ALE):** This metric quantifies the monetary value of potential loss from a cyber risk. It is calculated as Single Loss Expectancy (SLE) multiplied by the Annualized Rate of Occurrence (ARO). SLE, in turn, is derived from the Asset Value (AV) multiplied by the Exposure Factor (EF), which represents the negative impact a threat would have on the asset as a percentage.
- **CVSS (Common Vulnerability Scoring System):** A standardized, industry-recognized approach for scoring the severity of vulnerabilities, widely utilized for evaluating cybersecurity threats.

The true value of quantitative metrics, such as MTTD or vulnerability counts, lies in their ability to be translated into business impact. For example, improved uptime, a technical metric, directly translates to reduced financial losses in manufacturing, where downtime can cost upwards of $260,000 per hour. Similarly, medical device downtime directly impacts patient care and billable procedures. Quantitative metrics should be selected and presented in a way that clearly articulates their impact on safety, operational continuity, financial performance, and regulatory

compliance. This requires defining clear, measurable targets that are aligned with broader organizational Key Performance Indicators (KPIs).

Metric	Definition/Formula	Relevance to Sensor Cybersecurity
Level of Preparedness	Readiness to prevent, detect, and respond to cyber threats (technology, processes, people).	Indicates the overall maturity and resilience of the organization's sensor security program.
Unidentified Devices on Network (Count)	Number of unrecognized IoT devices connected to the network.	Quantifies shadow IT risk; highlights potential unauthorized access points and unmanaged attack surface.
Intrusion Attempts (Count/Frequency)	Number of documented attempts to breach networks/devices; analysis of their frequency.	Measures external threat landscape interest and effectiveness of perimeter defenses for sensor networks.
Data Loss Prevention Effectiveness (Ratio)	Ratio of successfully thwarted data incidents to total attempts; DLP system response time.	Gauges ability to protect sensitive sensor data (e.g., PHI, industrial process data) from exfiltration.
Mean Time Between Failures (MTBF)	Average time between successive system/component failures.	MTBF = Total Operating Time ÷ Total of assets in use.
Mean Time to Detect (MTTD)	Average time to detect a security incident.	Crucial for responsiveness; shorter MTTD allows faster mitigation of sensor-related threats (e.g., spoofing, tampering).
Mean Time to Respond/Resolve/Mitigate (MTTR/MTTM)	Average time to acknowledge/log an incident (MTTR), or repair/resolve it (MTTM).	MTTR = Total maintenance time ÷ Number of repairs/replacements.
Uptime/Availability (%)	Percentage of time critical systems are operational.	Uptime = (Total time – Downtime) / Total time * 100.
Vulnerability Remediation Rate (%)	Percentage of identified high-risk vulnerabilities patched/remediated within a timeframe.	Indicates effectiveness of patch management and vulnerability management programs for sensor firmware/software.
Security Incident Count	Number of reported cybersecurity incidents.	Reflects visibility into security issues and effectiveness of internal reporting mechanisms for sensor-related events.
Access Management Success Rate (%)	Percentage of successful user authentication attempts vs. total attempts; number of administrative accounts.	Measures strength of access controls for sensor management interfaces and data access.

Compliance Deficiencies (Count)	Number of cybersecurity-related gaps identified during audits.	Direct measure of adherence to regulatory standards (e.g., FDA, IEC 62443) for sensor deployments.
Post-Deployment Remediation Time	Time needed to fix security bugs found after deployment.	Post-Deployment Remediation Time = Total remediation time / Number of post-deployment security vulnerabilities.
Annualized Loss Expectancy (ALE)	Estimated monetary loss from a specific risk over a year.	ALE = SLE x ARO; SLE = Asset Value (AV) x Exposure Factor (EF).
CVSS Score	Standardized numerical score reflecting vulnerability severity.	Standardized approach for prioritizing remediation efforts for identified sensor vulnerabilities.
Sensor Data Accuracy (%)	Measures the number and types of errors in sensor data sets.	Directly assesses the integrity and trustworthiness of data collected by sensors, crucial for decision-making.
Anomaly Detection Rate (TPR/FPR)	True Positive Rate (TPR) and False Positive Rate (FPR) for detecting unusual sensor behaviour or data patterns.	Measures effectiveness of systems in identifying sensor spoofing, physical tampering, or data manipulation.

4.2 Qualitative Risk Assessment Methods

Qualitative risk assessments offer a rapid and effective means to identify risks, particularly when precise numerical data is scarce or when assessing subjective impacts. These methods typically employ numerical ratings (e.g., 1-5) or color-coded scales (e.g., green, yellow, red) to rank risks based on their likelihood of occurrence and potential impact on the business. They are often ideal for less-mature organizations or for initial, high-level assessments.

The methodology frequently involves subjective expert evaluations, often facilitated through committee discussions where delegates from various parts of the business assess how different teams or operations would be affected by specific risks. Rather than asking for precise monetary losses, a qualitative approach might ask, "How would the productivity of your team be affected if they couldn't access sensor data for a day?".

An illustrative example of a qualitative risk assessment model is the **DREAD model**. This model evaluates risks based on five factors:

- **Damage:** How much are the assets affected?
- **Reproducibility:** How easily can the attack be reproduced?
- **Exploitability:** How easily can the attack be launched?

- **Affected Users:** What is the number of affected users?
- **Discoverability:** How easily can the vulnerability be found?

Each factor is ranked (e.g., high, medium, or low), and these rankings are converted into numerical scores (e.g., high=3, medium=2, low=1) to determine an overall risk rating.

The primary benefits of qualitative assessments include their simplicity, speed, and ease of use, especially when employees possess practical experience with the assets and processes being evaluated. However, a notable drawback is their inherent subjectivity and the potential for bias in the evaluations.

To overcome the limitations of purely qualitative or quantitative approaches, **hybrid models** are increasingly adopted. These models integrate both qualitative and quantitative elements to enhance the accuracy and applicability of risk evaluation processes. ISO 27005:2022, for example, introduces **semi-quantitative risk analysis**, where some aspects (like likelihood) are quantified using statistical methods, while others (like impact) are defined using subjective methods or expert opinions. These hybrid frameworks are designed to adapt to evolving cyber threats and changing environments.

Given the diverse impacts of sensor compromises—some easily quantifiable financially, others more abstract like safety or reputation—a purely quantitative or qualitative approach can be insufficient. The increasing adoption of semi-quantitative or hybrid models, as seen in ISO 27005, and the general recommendation to leverage both, signifies a recognition of this complexity. For sensors, where physical safety is paramount, qualitative expert judgment on "consequence" is often irreplaceable, even if the likelihood of an event is derived quantitatively. Therefore, a robust sensor cyber risk measurement program should adopt a hybrid approach, combining the objectivity of quantitative metrics (e.g., vulnerability counts, Mean Time to Respond) with the nuanced understanding provided by qualitative assessments (e.g., expert opinion on safety impact, DREAD model for exploitability). This ensures a comprehensive view of risk that captures both tangible and intangible consequences.

4.3 Measuring Sensor Data Integrity, Trust, and Reliability

The integrity, trustworthiness, and reliability of sensor data are paramount, as this data forms the foundation for critical decision-making in numerous systems, including industrial control, smart cities, and medical diagnosis. Compromised data integrity can lead to severe consequences such as misdiagnoses, operational failures, and significant safety hazards. User trust in the Internet of Things (IoT) fundamentally hinges on the dependability of the data it provides.

To assess these critical aspects, several data quality metrics are essential:

- **Accuracy:** Ensures that data precisely reflects real-world values, tracking anomalous values, micro-volumes (unusual record counts in a segment), or strings (values not matching predetermined lists).
- **Completeness:** Measures the extent to which all required data fields are available. It is typically expressed as a percentage of total records.
- **Consistency:** Evaluates whether data is uniform and coherent across different databases and systems, preventing contradictions.
- **Timeliness/Currency:** Measures the age of data in a database. More current data is generally more accurate and relevant, especially for dynamic information.
- **Uniqueness:** Tracks duplicate data to prevent undue weighting in analyses. Identifying and merging or deleting duplicates is crucial.
- **Validity:** Measures how well data conforms to established standards, ensuring data is of the proper type and format (e.g., correct date format, two-digit state codes).

Anomaly detection plays a critical role in maintaining data integrity by identifying unusual or unexpected data points or patterns in time-series data collected from sensors. This includes spotting sudden spikes or dips, or deviations from established normal behaviour. Anomalies can be categorized into:

- **Global outliers/point anomalies:** Single data points that significantly differ from the rest.
- **Contextual outliers:** Data points that are anomalous within a specific context but might seem normal individually (e.g., a bulk purchase at an unusual time).
- **Collective outliers:** A group of data points that collectively deviate from the normal pattern.

Various techniques are employed for anomaly detection:

- **Statistical Methods:** Simple and interpretable, relying on mathematical thresholds (e.g., Z-score, Interquartile Range, regression analysis) to identify outliers. While effective for smaller datasets, they have limited adaptability to dynamic or complex data.
- **Machine Learning (ML) Algorithms:** More adaptable, learning underlying patterns in data to identify deviations. Common models include Decision Trees (Isolation Forest), One-Class Support Vector Machines (SVM), and K-Means Clustering. These have shown high accuracy (98-99.79%) in detecting sensor spoofing attacks, such as GPS spoofing in UAVs.
- **Deep Learning (DL) Methods:** A subset of ML that uses neural networks (e.g., Autoencoders, Long Short-Term Memory (LSTM) networks) to analyze large, complex,

high-dimensional datasets. Highly effective at identifying intricate and subtle anomalies, though computationally intensive.

Metrics for evaluating anomaly detection systems include **Sensitivity** (adjusting tolerance for anomaly detection), **MaxAnomalyRatio** (the maximum ratio of anomalies to be detected), and **Precision & Recall** (balancing false positives and negatives).

Indicators of Compromise (IoCs) are forensic data that provide evidence that a system or network may have already been breached. For sensor networks, key IoCs include:

- **Network Traffic Anomalies:** Unusual outbound traffic to unfamiliar or suspicious IP addresses, sudden spikes or dips in network traffic, or activity originating from unusual locations.
- **Unusual User/Device Account Activity:** Accessing files or systems not typically needed, logging in at unusual times, making privilege escalation requests, sign-ins from unusual geographies, or repeated failed sign-in attempts.
- **Unexpected Software Installations or Updates:** The presence of unauthorized malware, ransomware, or unexpected firmware updates.
- **Numerous Requests for the Same File:** May indicate attempted data exfiltration by a malicious actor.
- **Unusual Domain Name System (DNS) Requests:** Can signal command and control (C2) activity from malware.
- **Physical Tampering Indicators:** Detection of physical manipulation of Wi-Fi infrastructure, for example, can achieve high true positive rates (95.89%) with low false positive rates (4.12%).

The core function of a sensor is to collect and transmit accurate data. Therefore, the integrity, trustworthiness, and reliability of this data are direct indicators of the sensor's cybersecurity posture. If data is corrupted, spoofed, or unavailable, it signifies a successful cyberattack, regardless of whether the device itself is "down." Metrics like accuracy, consistency, and timeliness directly assess this. Anomaly detection, particularly for time-series sensor data, becomes a critical real-time measurement tool for detecting compromises that manifest as data manipulation (e.g., illusion attacks, GPS spoofing). This implies that measuring cyber risk for sensors must heavily emphasize data integrity and anomaly detection. Organizations need robust monitoring systems that establish baselines for "normal" sensor data behaviour and alert on deviations. This requires investing in AI/ML-driven anomaly detection tools capable of processing large volumes of time-series data from diverse sensor types.

5 PRACTICAL GUIDE FOR END-USERS

Measuring the cyber risks associated with sensing systems involves assessing various factors that could compromise the confidentiality, integrity, and availability of sensing data or the systems themselves.

The following key approaches and considerations for quantifying and managing these risks:

1. Identify the Assets and Threats

    - Assets: Sensors, communication channels, data storage, and processing systems.
    - Threats: Eavesdropping, data tampering, sensor spoofing, denial of service (DoS), malware, and physical tampering.

2. Assess Vulnerabilities

    - Evaluate weaknesses in sensor design, communication protocols, cryptographic protections, and physical security measures.

3. Determine Impact and Likelihood

    - Impact: How would a breach or failure affect the system? (e.g., safety risks, data loss, privacy breaches)
    - Likelihood: Probability of attack or failure based on threat actor capabilities and vulnerability exposure.

4. Quantitative Risk Metrics

    - Use models like Risk = Likelihood x Impact to quantify risks.
    - Assign scores or monetary values to potential impacts and likelihoods, enabling comparison and prioritization.

5. Security Frameworks and Standards

    - Follow standards such as NIST, ISO 27001, or IEC 62443 tailored to industrial control systems and IoT security.

6. Simulation and Penetration Testing

    - Conduct simulated cyber-attacks on sensing systems to evaluate resilience.

- Use threat modelling to identify potential attack vectors and estimate risk levels.

7. Monitoring and Incident Data

    - Collect data on past security incidents, vulnerabilities exploited, and system downtimes to refine risk assessments.

8. Use of Automated Tools

    - Employ cybersecurity risk assessment tools that can analyse vulnerabilities, scan for weak configurations, and simulate attack scenarios.

The end-users (the logistic hubs) need to trust sensors regarding its cybersecurity posture involves evaluating several factors before making a purchase. Therefore, in the Sintra project, we have taken the initial step towards developing a checklist that end-users can use to evaluate whether a sensor is digitally secure.

For this purpose, a categorization has been made into 5 main items:

1. Hardware

    - Assessing the physical security features, tamper resistance, and robustness of the sensor hardware.

2. Software

    - Evaluating the security measures embedded in the sensor's firmware and software, including update mechanisms, vulnerability management, encryption, and access controls.

3. Data Handling

    - Reviewing how data is collected, stored, transmitted, and protected against tampering, eavesdropping, and unauthorized access. Ensuring data privacy and integrity.

4. Supplier Integrity

    - Ensuring that the sensor supplier adheres to security best practices, provides transparent documentation, and maintains a trustworthy supply chain.

5. User Responsibility

- Clarifying the role of the end-user in maintaining security, including proper configuration, regular updates, secure handling, and awareness of security protocols.

This categorization aims to give end-users a structured way to assess and select sensors based on their cybersecurity robustness. It emphasizes that security isn't solely dependent on the device itself but also involves supply chain integrity and responsible use by users.

6 IMPLEMENTATION OF A CHECKLIST CYBER RISK OF SENSORS

In the SINTRA project we started to built a checklist consisting of 100 questions regarding the earlier previously mentioned items, and once completed, it gives the end-user a good overview of the sensor's cybersecurity.

Component	Category
Hardware	Protection of hardware
	Emergency and Lifecycle Management
	Audits and Monitoring
	Safe Disposal and Maintenance
Software	Software Update Management
	Integrity & Configuration Management
	Logging & Monitoring
	API Security
Data Handling	Data integrity and access control
	Encryption and backup management
	Cloud storage security
	API and Gateway security
Supplier Integrity	Quality Management and certification
	Vulnerability management and technical security
	Supplier management and dependency
	Collaboration and contracts
	Cybersecurity
User Responsibility	Access Management
	User awareness and training
	Data Protection

	System and network security
	External access
	Device Management

This checklist is intended for end users to gain an understanding of the sensor's cybersecurity. It can be used to check before purchasing sensors or sensor systems, and to verify existing sensors. At the Sintra-ai.eu and the Sintra-ai.nl websites we will provide a link where end-users can fill in the checklist. The weblink will be ready in Q1 2026 or earlier.

The checklist is a first version, a study will be made during the Sintra project, and probably also afterwards to improve this checklist.

7 CONCLUSION AND FUTURE OUTLOOK

Measuring cyber risks for sensors is a complex, multifaceted undertaking that demands a nuanced and adaptive approach. The pervasive nature of sensors across diverse critical domains—from industrial control systems to medical devices and smart cities—means that their compromise can lead to impacts far beyond traditional data breaches, encompassing severe safety hazards, operational disruptions, and significant financial losses. This report has underscored the imperative for context-specific risk measurement, leveraging a blend of quantitative and qualitative metrics, and implementing continuous, lifecycle-based risk management strategies. A critical understanding that has emerged is the necessary shift from an IT-centric security mindset to one that prioritizes safety and availability, particularly for Operational Technology (OT) and medical sensors.

Looking ahead, several emerging trends will continue to shape the landscape of sensor cybersecurity risk management:

- **Increasing AI/ML Integration:** The sheer volume and complexity of data generated by IoT devices, coupled with the dynamic nature of cyber threats, are outpacing traditional manual security methods. Consequently, there will be an increasing adoption of AI-driven analytics for dynamic risk estimation, predictive analytics, and security automation. This will be crucial for handling the "vast volumes of data" produced by IoT devices , enabling real-time threat detection, vulnerability analysis, and anomaly identification. Organizations that fail to adopt these technologies will struggle to keep pace with the evolving threat landscape, leading to increased unmeasured and unmitigated risk.
- **Compliance as a Market Gatekeeper:** Cybersecurity is rapidly becoming a core evaluation criterion in procurement processes, especially for critical applications like medical devices. Vendors without built-in protections and robust security postures face disqualification from market access. This trend will drive manufacturers to prioritize security-by-design from the earliest stages of product development, embedding security features and processes into their Secure Product Development Frameworks (SPDFs).
- **Heightened Focus on Supply Chain Security:** Given the prevalence of third-party components in IoT devices and the increasing incidence of supply chain compromises , Software Bill of Materials (SBOMs) and rigorous vendor risk management will become even more critical requirements. Organizations will demand greater transparency into the software and hardware components of their purchased sensors to assess inherited risks.
- **Convergence of IT and OT Security:** While IT and OT environments have distinct priorities (CIA vs. SAIC), the increasing connectivity of ICS to corporate networks necessitates integrated security strategies. Frameworks like IEC 62443 will continue to provide guidance on bridging these domains, mapping OT-specific controls to broader IT frameworks like the

NIST Cybersecurity Framework. This convergence will require a more unified approach to risk management across the enterprise.

- **Innovative Solutions for Resource-Constrained Devices:** The inherent limitations of low-power, resource-constrained sensors will continue to drive the development of energy-efficient security solutions. This includes offloading complex security logic to network infrastructure or cloud platforms, and the adoption of lightweight communication protocols. These innovations will enable stronger security measures without compromising the operational efficiency or battery life of these devices.

In conclusion, organizations must adopt a proactive, adaptive, and holistic approach to measuring and managing sensor cyber risks. This requires recognizing that sensors are not merely endpoints but integral components of critical systems impacting safety, operations, and business continuity. Continuous investment in specialized expertise, advanced tools, and robust frameworks—particularly those leveraging AI/ML for enhanced visibility and automation—will be paramount to securing the increasingly interconnected world of sensors and ensuring resilience against evolving cyber threats.