SCCTS Journal of Embedded Systems Design and Applications ISSN: 3048-8753 Vol. 2, No. 1, 2025 (pp. 1-11)
REVIEW ARTICLE ECEJOURNALS.IN

# A Review of Security Protocols for Embedded Systems in Critical Infrastructure

**B. Vincentelli[1], K.R. Schaumont[2]***

[1,2]R. B. Annis School of Engineering, University of Indianapolis, Indianapolis, IN 46227, USA

**Keywords:**
Software Optimization in Embedded Systems;
Embedded System Performance Evaluation;
Embedded System Design Challenges;
Ultra-Low Power Embedded Systems

**DOI:** 10.31838/ESA/02.01.01

**Received** : 01.07.24
**Revised** : 01.10.24
**Accepted** : 01.12.24

## Abstract

A broad application of embedded systems into critical infrastructure sectors represents an era of unprecedented connectivity and automation. While this technological revolution has brought us back into the 21st century, it has brought some new vulnerabilities that need robust security protocols in place. This work provides a comprehensive review of the evolution of embedded system security in critical infrastructure, with a focus on key challenges, emerging threats, and the most meaningful solutions of the field. However, as our world gets more and more interlinked, the security of our embedded systems in critical infrastructure becomes of a primary importance. These embedded technologies are critical to power grids and transportation networks as well as healthcare facilities and industrial control systems of modern society. At no other time has the need to protect these systems from cyber threats been needed more, since attacks could tie into widespread disruption, economic losses, and even loss of life. In this article we take a deep look at embedded system security protocol, and the role they play to protect critical infrastructure from malicious actors. In this overview of the key challenges, we'll investigate the special plight of various sectors, examine the latest security techniques, and look at possible paths for future research and development in this critical domain. If we take a deep dive into embedded system security complexities, we could improve our efforts towards building more resilient and secure critical infrastructure for the next generations.

**How to cite this article:** Vincentelli B, Schaumont KR (2025). A Review of Security Protocols for Embedded Systems in Critical Infrastructure. SCCTS Journal of Embedded Systems Design and Applictions, Vol. 2, No. 1, 2025, 1-11

## The Evolving Embedded Systems within Critical Infrastructure

Embedded systems have been integrated into critical infrastructure, changing significantly how essential services are designed, developed, procured, delivered and managed. They have driven the backbone of infrastructure to the present: these specialized computer systems, with certain processing needs, designed to execute certain tasks in real time. E packed with omnipresent embedded technologies, which include supervisory control and data acquisition (SCADA) systems in industrial settings to smart meters in the energy sector.[1-4]

This rapid evolution in the field of microprocessors as well as real-time operating systems (RTOS) and ARM compatible operating systems has greatly contributed to the spread of embedded systems in all different sectors. The growth has enabled, for example, more efficient, automated decision making, in critical infrastructure management driven by data. But it has also made security paramount as it's also expanded the attack surface for potential cyber threats. Due to the growing sophistication and interconnectivity of embedded systems, there is a rapidly increasing number of security challenges facing them. Many critical infrastructure components have such long lifespans that can take up to decades, making security efforts even more difficult. However, we must live in an ecosystem where the legacy systems must coexist with newer more secure technologies, complicating the

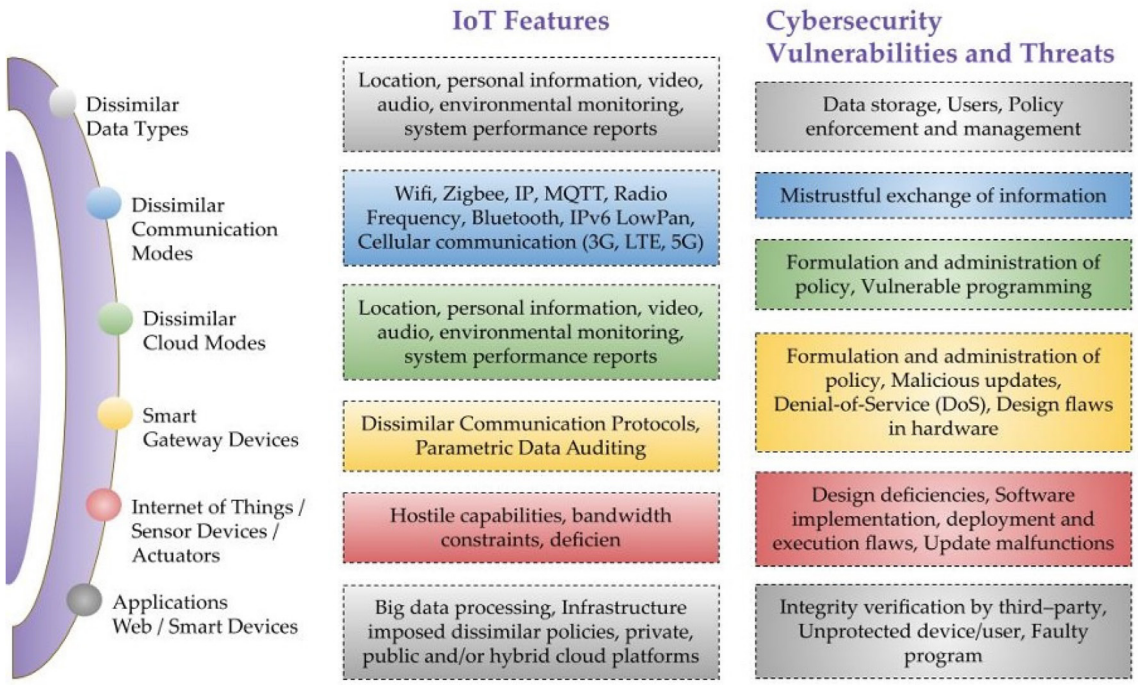


**Fig. 1. Evolving embedded systems within critical infrastructure**

system and needing careful attention and protection. Given the evolution of embedded systems in critical infrastructure, security has a need to be approached holistically. This is on both the technical measures as well as the human factors, regulatory frameworks and economic incentives. We will take a look at the different ways that all of these pieces come together to form an overall embedded systems security strategy for critical infrastructure.[1-4]

## Critical Infrastructure Sectors' Unique Security Challenges

The security challenges that embedded systems need to address are however not identical to all sectors of critical infrastructure. Developing effective security protocols and strategies can require a good understanding of these sector specific issues. Let's examine some of the key challenges faced by different critical infrastructure sectors:

### Energy Sector

Since the energy sector needs to monitor and control power generation, transmission, and distribution systems, embedded technologies play a role in providing these. New vulnerabilities have been introduced with the smart grids and AMI and even these provide benefits. The issue of handling both real time data and control in this sector, while also maintaining robust security measures is one of the main hurdles. The increasing integration of renewable energy sources and increasingly distributed generation also significantly complicates the energy systems as the network expands and increases the potential attack surface. It also applies the long lifespan of many energy infrastructure components, which implies that legacy systems also need to be secured along with newer, more advanced technologies alike.

### Transportation Systems

Transportation systems, of which traffic management systems and autonomous vehicles are examples, are embedded systems with unusually high mobility as well as potential for physical harm to them, which introduces unique security challenges. Vehicle and transportation infrastructure increase connectivity resulting in new attack vectors which threaten safety and could compromise critical services. Often the security measures in transportation systems are deemed too extensive, and the real-time processing requirements are conflicted. But in safety critical applications like autonomous driving or air traffic control, balancing security with performance is one challenge that never ends.

## Healthcare and Medical Devices

The healthcare sector includes embedded systems in medical devices as well as hospital infrastructure, and we must consider the continuous importance of patient safety, while protecting patient data's privacy and security. Medical device safety and effectiveness still have to be scrutinized by the FDA, but under consideration now are cybersecurity threats that could put patient care in jeopardy. In the case of implantable and wearable medical devices, there are particularly stringent constraints on power consumption and size so that there is little room available for security features. Furthermore, emergencies provide a unique set of issues related to authentication and authorization for medical devices.

## Industrial Control Systems

Industrial control systems (ICs) and Supervisory Control and Data Acquisition (SCADA) systems resident in manufacturing, and critical infrastructure, are subject to threats that could damage them physically or seriously affect essential services. Such systems are usually past their operational life and can employ proprietary protocols, which often prevent installation of more modern security safeguards without interrupting service. Increased reliance on operational technology (OT) and information technology (IT) convergence in industrial settings has enhanced existing vulnerabilities as isolated systems merge with a greater network. This sector has been proving to be one of the most conventional to balance the connectivity and data analysis needs with the security concerns.

## Embedded Systems Common Vulnerabilities

Despite security challenges specific to each sector of critical infrastructure, industries of all types are exposed to common vulnerabilities that impact embedded systems in all sectors. This in turn is the basis of creating a comprehensive security strategy based on what are known as the limits of human comprehension. Let's explore some of the most prevalent vulnerabilities in embedded systems:

## Limited Resources

Processed power, memory and energy resource are scarce for many embedded systems especially in legacy infrastructure, and also in resource constrained environments. However, this constraint frequently results in tradeoffs with security features, as there are often excessive resource requirements to deploy robust encryption and authentication mechanisms (Table 1).

Another limitation is that you don't have the resources to update or patch these systems often, which leads to these being vulnerable to known exploits for an extended amount of time. Combining this with the long operational lifespans of many critical infrastructure components that outlive their embedded technologies' support lifetimes, exacerbates this problem. Due to the small form factor and constricted bandwidth of embedded systems many of the communication protocols embedded are not designed with security in mind. Despite the increasing availability of alternative industrial protocols, legacy ones like Modbus – used throughout large numbers of industrial control systems – do not have embedded

**Table 1: Security Measures for Embedded Systems in Critical Infrastructure**

| Measure | Purpose |
|---|---|
| Data Encryption | Data encryption ensures that all transmitted data is securely encoded, preventing unauthorized access or tampering during transmission. |
| Authentication Protocols | Authentication protocols verify the identity of users or systems attempting to access embedded devices, ensuring secure interactions. |
| Access Control | Access control defines permissions and restricts access to critical system functions, protecting embedded systems from unauthorized use. |
| Intrusion Detection | Intrusion detection systems monitor the network and device activity for unusual patterns, helping identify potential security threats in real time. |
| Secure Boot | Secure boot ensures that embedded systems start with authentic firmware, preventing the execution of malicious or unauthorized software during system initialization. |
| Firmware Update Management | Firmware update management ensures that embedded devices can securely receive and install updates, protecting them from vulnerabilities through patching. |

security features like encryption or authentication. Backward compatibility may require us to continue to use insecure communication mechanisms when more secure ones are available. That allows attackers to inject, manipulate, or intercept malicious data in critical systems.

## Lack of Physical Security

Unlike traditional IT systems, many deployed critical infrastructure embedded devices are located in physically accessible locations. This trend will cause more risk of tampering, reverse engineering and side channel attacks. Physical attackers can potentially remove sensitive information and place malware or physical components that will alter the firmware on the device.

Many of the critical infrastructure systems of today are distributed, meaning it is difficult to adhere to consistent physical security of all endpoints. For the same reasons mentioned above, this dispersed architecture creates a lot of potential compromised points which must be secured.

Authentication and access control are not sufficient. However, there are often no robust authentication mechanisms on embedded systems, leaning instead on simple passwords or having no authentication at all. Such a weakness may allow unauthorized users to exploit critical functions or sensitive data.

Finally, emergency access in some particular situations, where medical devices or industrial control systems are concerned can make access control even more difficult. However, balancing security with the necessary need of fast, unencumbered access to people and critical resources in moments of crisis is a challenging problem for the system designer and security professional.

These Emerging Threats and Attack Vectors lead to. Embedded systems in critical infrastructure are under almost constant attack from cyber threats. New technology creates new attack vectors, and attackers get more sophisticated, the range only continues to swell. To prevent these emerging threats, it is of secret importance to grasp them. Let's examine some of the most significant emerging threats and attack vectors:

## Supply Chain Attacks

Embedded supply chain attacks have recently escalated, targeting the convoluted network of suppliers, manufacturers, and distributors that produces embedded systems. Like previous buffer overflow attacks, these attacks seek to compromise a hardware or software component that is never integrated into critical infrastructure. Attackers can infiltration in the supply chain to also introduce back doors, malware, or counterfeit components, which are hard once deployed. Leading to the complication that not all system elements can be guaranteed to be of high integrity, such an abuse continues to be prevalent with the increased global manufacturing due to globalized nature of that manufacturing and reliance on third-party components.

## Advanced Persistent Threat (APTSs)

Advanced Persistent Threats are a class of attack that we designate as sophisticated and long term, and often with the same focus of attack as against critical infrastructure. Attacks of this type are typically performed by sophisticated adversaries that are driven to persistently gain access to sensitive systems; often nation state actors or organized crime groups. Embedder systems in critical infrastructure may be attacked using a mix of social engineering, exploits known to be zero day, and custom malware to avoid detection. These threats are particularly dangerous, as attackers can leech information from your company and do a steady level of damage over a long period of time.[5-8]

## Artificial Intelligence and Machine Learning Attacks are the focus

Artificial Intelligence (AI) and Machine Learning (ML) technologies are increasing in critical infrastructure management, and also, bring new attack vectors. Adversarial machine learning techniques can be applied to AI guided decision making systems, which may misclassify or perform inappropriate actions. For instance, if an attacker would trick an industrial control system into believing it's not under attack, it could go unnoticed, as an AI based intrusion detection system could potentially be fooled. Likewise, the predictive maintenance or resource allocation models you would employ to machine learning systems could be used to inject inefficiencies or disturbances in critical systems.

## Quantum Computing Threats

The development of quantum computing is in its early stages, but it represents a major futur threat to many contemporary cryptographic protocols in use within embedded systems. Encryption algorithms common around today may soon be broken using quantum computers, making our security a hopeless mess.

Because it is so imminent the embedding of quantum resistant cryptographic algorithms is required for critical infrastructure. However, given the resource constraints of many embedded devices, this transition is very difficult.

## Embedded Systems Security Innovation

The threat landscape is changing, and the embedded systems used in critical infrastructure must also change accordingly in keeping with current security measures. Together with advanced technologies and novel solutions, these systems face a unique challenge that is now generating innovative solutions. Let's explore some of the most promising security solutions for embedded systems:

## Hardware-Based Security

However, hardware based security solutions can provide a strong platform on which to build in by protecting against different threats. Typically they are the provider of dedicated security chips or modules that provide a hardware root of trust, secure boot processes, and cryptographic acceleration.

TPMs and HSMs are being integrated increasingly into embedded systems for secure key storage, cryptographic operations and attestation, and trusted health monitoring. Unlike software only solutions, these hardware based solutions, provide a stronger protection against tampering and sidechannel attacks.

## Lightweight Cryptography

Given resource constraints of many embedded systems, researchers and industry professionals are developing lightweight cryptographic algorithms, tailored for low memory, low power environments. The goal of these algorithms is to furnish strong security guarantees with the least computational overhead and energy consumption, respectively.

Examples of such lightweight cryptographic primitives are PRESENT, CLEFIA and SIMON/SPECK for efficient encryption in the presence of resource constraints as employed in low power mobile devices. However, as these algorithms develop and go through rigorous security analysis, they will almost certainly find increased use in critical infrastructure embedded systems.

## Firmware Updates and Security Boot

Secure boot processes and firm ware update mechanisms are mandatory to ensure the integrity of embedded systems throughout its lifecycle. Secure boot guarantees that only authentic, unmodified code is run from system start, and not malicious or corrupted firmware.

OTA update mechanisms provide for running secure remote (over the air) patching against vulnerabilities and adding new features without compromising security. In these systems crypto signatures and cryptography encryption are typically used to verify the authenticity and integrity of firmware updates.

## Network isolation & segmentation

I believe network segmentation and isolation improves potential breach containment and puts bounds on the area of attack of an incident within critical infrastructure systems. Dividing networks into smaller, disconnected 'islands' makes it more difficult for unauthorized users to gain access and reduces the consequences if an attacker is successful.

The creation of more flexible and safer network architectures using embedded systems leverages software defined networking (SDN) and network function virtualization (NFV) technologies. Specifically, these approaches permit network segment reconfiguration on the fly, and granular access controls.

## The Regulatory Frameworks and the Standards.

Part of the role of robust regulatory frameworks and standards is to assure security of embedded systems in critical infrastructure such as the defense and aerospace, transportation, financial services, nuclear power, water and wastewater management and energy sectors, in addition to healthcare. Below is the guidance on security that is common baseline and standard for security practices, interoperability and minimum security requirements for organizations. Let's examine some of the key regulatory frameworks and standards shaping the landscape of embedded system security:

## NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is a complete, complete set of instructions and approaches to help manage and mitigate cybercrime risk. The framework's core functions: Identify, Protect, Detect, Respond, and Recover - are very applicable to the security of critical infrastructure, which is not even specific to embedded systems.

The NIST framework can be adapted by organizations for use as a basis for sector specific security strategies, modified to address the specific challenges of embedded systems. The flexibility of the framework enables its utilization within different critical infrastructure sectors with their risk management of cybersecurity in a similar manner.

## IEC 62443 Series

The International Electrotechnical Commission (IEC) 62443 series of standards specifically address the security of industrial automation and control systems (IACS). These standards specify the industrial embedded systems security requirements and security risk analysis as well as secure system design. In particular, this is relevant for critical infrastructure sectors, like energy, water treatment and manufacturing. On the other hand, it's a solution for the special scenario of operational technology (OT) environments, such as high availability and the assembly of legacy systems.

IT products, including embedded systems, are specified in terms of security functional and assurance requirements in accordance with the framework specified in the Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408. In order to evaluate and certify security features in technology products, this international standard provides.

Common Criteria certification affords assurance for an embedded system in critical infrastructure that a product meets specified security requirements. Yet the expense and time to complete the certification process may limit its applicability to rapidly evolving embedded technologies. Different sectors of critical infrastructure have also designed and adopted their own regulatory frameworks and standards focused on addressing distinctive sector peculiar security problems.• Cybersecurity requirements for the bulk power system in North America are governed in North American through the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection ("CIP") standards.The U.S. Department of Homeland Security's Transportation Systems Sector Cybersecurity Framework Implementation Guidance includes tailored guidance oriented to the application of the NIST Cybersecurity Framework to transportation systems.• Recommendations regarding cybersecurity in medical devices are made in the FDA's "Guidance for Content of Premarket Submissions for Management of Cybersecurity in Medical Devices."mploy cryptographic signatures and encryption to verify the authenticity and integrity of firmware updates before installation. Network segmentation and isolation techniques help contain potential breaches and limit the spread of attacks within critical infrastructure systems. By dividing networks into smaller, isolated segments, organizations can restrict unauthorized access and minimize the impact of a successful attack. Software-defined networking (SDN) and network function virtualization (NFV) technologies are being leveraged to create more flexible and secure network architectures for embedded systems. These approaches allow for dynamic reconfiguration of network segments and the implementation of granular access controls (Table 2).[9-14]

**Table 2: Security Challenges and Countermeasures in Embedded Systems**

| Challenge | Countermeasure |
|---|---|
| Hardware Vulnerabilities | Hardware vulnerabilities can be exploited by attackers; countermeasures include the use of secure hardware modules and encryption at the hardware level. |
| Network Attacks | Network attacks, such as man-in-the-middle or denial-of-service attacks, can compromise data integrity; firewalls and encryption prevent such attacks. |
| Data Integrity | Data integrity ensures that information is not altered or corrupted; hashing and checksums verify the integrity of the data during transmission. |
| Physical Security | Physical security addresses the risk of physical tampering with embedded devices; physical locks, tamper-resistant hardware, and sensors prevent unauthorized access. |
| Resource Constraints | Resource constraints in embedded systems, such as limited processing power and memory, require lightweight cryptographic techniques and optimized security protocols. |
| Regulatory Compliance | Regulatory compliance ensures that security measures adhere to industry standards; regular audits and certifications ensure compliance with security regulations. |

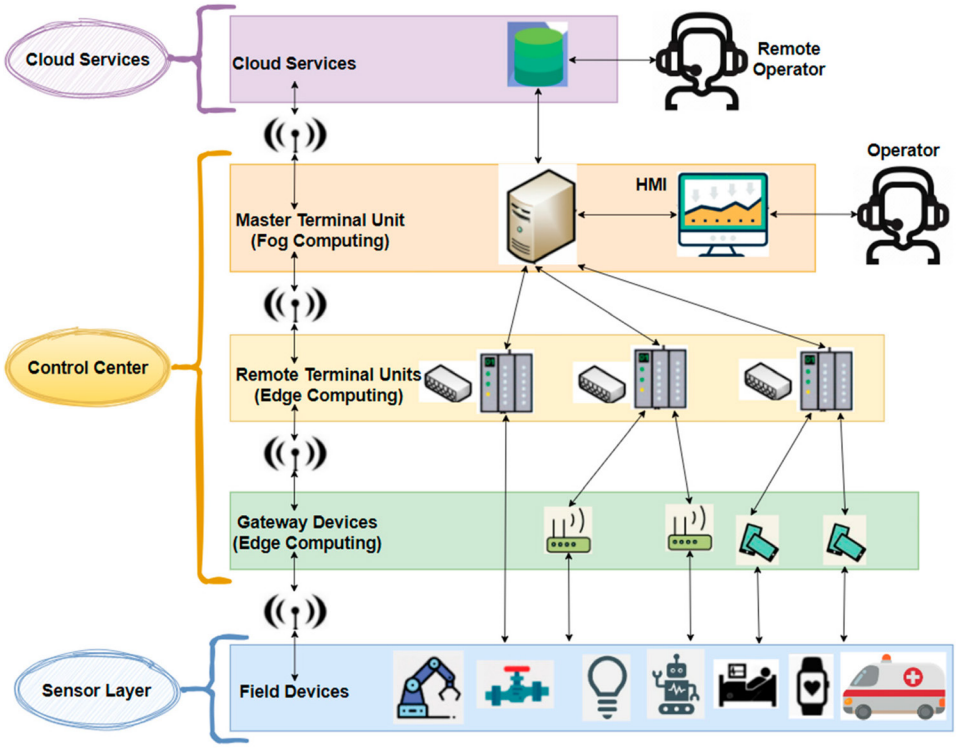


Fig. 2: Security Awareness and Human Factors

## Security Awareness and Human Factors

Although technical solutions can secure embedded systems in critical infrastructure, human elements have to be taken equally seriously. Security depends so much on human factors, such as user behavior, security awareness, and organizational culture. Let's explore the key aspects of human factors and security awareness in the context of embedded system security (Figure 2):

### User Training and Education

And that's why comprehensive training programs are a must for making sure personnel actually working with embedded systems know the risks to security and the most effective security practices.• Basic application of cybersecurity to embedded system• Maintenance and usage of security features of embedded devices. • Different ways to list potential security threats and appropriate response procedures • Relevant regulatory requirements and compliance obligations vulnerabilities and the addition of new features without compromising security. These systems typically employ cryptographic signatures and encryption to verify the authenticity and integrity of firmware updates before installation.

### Network Segmentation and Isolation

Network segmentation and isolation techniques help contain potential breaches and limit the spread of attacks within critical infrastructure systems. By dividing networks into smaller, isolated segments, organizations can restrict unauthorized access and minimize the impact of a successful attack.

Software-defined networking (SDN) and network function virtualization (NFV) technologies are being leveraged to create more flexible and secure network architectures for embedded systems. These approaches allow for dynamic reconfiguration of network segments and the implementation of granular access controls.

### Regulatory Frameworks and Standards

The development and implementation of robust regulatory frameworks and standards play a crucial role in ensuring the security of embedded systems in critical infrastructure. These guidelines provide a common baseline for security practices, promote interoperability, and help organizations meet minimum security requirements. Let's examine some of the key regulatory frameworks and standards shaping the landscape of embedded system security:

## NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive set of guidelines for managing and reducing cybersecurity risk. While not specific to embedded systems, the framework's core functions - Identify, Protect, Detect, Respond, and Recover - are highly relevant to securing critical infrastructure.

Organizations can adapt the NIST framework to address the unique challenges of embedded systems, using it as a foundation for developing sector-specific security strategies. The framework's flexibility allows for its application across various critical infrastructure sectors, promoting a consistent approach to cybersecurity risk management.

## IEC 62443 Series

The International Electrotechnical Commission (IEC) 62443 series of standards focuses specifically on the security of industrial automation and control systems (IACS). These standards provide detailed guidelines for securing industrial embedded systems, covering aspects such as system security requirements, security risk assessment, and secure system design.

The IEC 62443 series is particularly relevant for critical infrastructure sectors such as energy, water treatment, and manufacturing. It addresses the unique challenges of operational technology (OT) environments, including the need for high availability and the integration of legacy systems.

## Common Criteria (ISO/IEC 15408)

The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, provides a framework for specifying security functional and assurance requirements for IT products, including embedded systems. This international standard allows for the evaluation and certification of security features in technology products.

For embedded systems in critical infrastructure, Common Criteria certification can provide assurance that a product meets specific security requirements. However, the certification process can be time-consuming and expensive, which may limit its applicability to rapidly evolving embedded technologies.

## Sector-Specific Regulations

Various critical infrastructure sectors have developed their own regulatory frameworks and standards to address sector-specific security challenges. For example:

- The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) standards provide cybersecurity requirements for the bulk power system in North America.
- The Transportation Systems Sector Cybersecurity Framework Implementation Guidance, developed by the U.S. Department of Homeland Security, offers tailored guidance for applying the NIST Cybersecurity Framework to transportation systems.
- The FDA's guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" provides recommendations for addressing cybersecurity in medical devices.

These sector-specific regulations often complement broader cybersecurity frameworks, providing more detailed guidance on securing embedded systems within particular domains of critical infrastructure.

## Human Factors and Security Awareness

While technical solutions are crucial for securing embedded systems in critical infrastructure, the human element plays an equally important role in maintaining overall security. Human factors, including user behavior, security awareness, and organizational culture, can significantly impact the effectiveness of security measures. Let's explore the key aspects of human factors and security awareness in the context of embedded system security:

## User Training and Education

Comprehensive training programs are essential for ensuring that personnel working with embedded systems understand the potential security risks and best practices for mitigating them. This training should cover:

- Basic cybersecurity principles and their application to embedded systems
- Proper use and maintenance of security features in embedded devices
- Recognition of potential security threats and appropriate response procedures
- Understanding of relevant regulatory requirements and compliance obligations

Staff members can be kept informed on new threats and kept up to date with regular refresher courses.[15-18]

## Usability and Security Trade offs

The challenge is to design secure embedded systems that are also user friendly. Too many security measures can bloat users and tempt them to find a work around that defeats your security. For a protective measure to be effective and sustainable, a necessary balance needs to be found between usability and security.

Human centered design can help develop security interfaces and process that match users' mental models and that are intuitive.• Security notification and alerts which are clear and concise• Secure authentication processes with less users pain.• Helping and guiding in context in performing security related tasks remote patching of vulnerabilities and the addition of new features without compromising security. These systems typically employ cryptographic signatures and encryption to verify the authenticity and integrity of firmware updates before installation.

### Network Segmentation and Isolation

Network segmentation and isolation techniques help contain potential breaches and limit the spread of attacks within critical infrastructure systems. By dividing networks into smaller, isolated segments, organizations can restrict unauthorized access and minimize the impact of a successful attack.

Software-defined networking (SDN) and network function virtualization (NFV) technologies are being leveraged to create more flexible and secure network architectures for embedded systems. These approaches allow for dynamic reconfiguration of network segments and the implementation of granular access controls.

### Regulatory Frameworks and Standards

The development and implementation of robust regulatory frameworks and standards play a crucial role in ensuring the security of embedded systems in critical infrastructure. These guidelines provide a common baseline for security practices, promote interoperability, and help organizations meet minimum security requirements. Let's examine some of the key regulatory frameworks and standards shaping the landscape of embedded system security.

### NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a comprehensive set of guidelines for managing and reducing cybersecurity risk. While not specific to embedded systems, the framework's core functions - Identify, Protect, Detect, Respond, and Recover - are highly relevant to securing critical infrastructure.

Organizations can adapt the NIST framework to address the unique challenges of embedded systems, using it as a foundation for developing sector-specific security strategies. The framework's flexibility allows for its application across various critical infrastructure sectors, promoting a consistent approach to cybersecurity risk management.

### IEC 62443 Series

The International Electrotechnical Commission (IEC) 62443 series of standards focuses specifically on the security of industrial automation and control systems (IACS). These standards provide detailed guidelines for securing industrial embedded systems, covering aspects such as system security requirements, security risk assessment, and secure system design.

The IEC 62443 series is particularly relevant for critical infrastructure sectors such as energy, water treatment, and manufacturing. It addresses the unique challenges of operational technology (OT) environments, including the need for high availability and the integration of legacy systems.

### Common Criteria (ISO/IEC 15408)

The Common Criteria for Information Technology Security Evaluation, also known as ISO/IEC 15408, provides a framework for specifying security functional and assurance requirements for IT products, including embedded systems. This international standard allows for the evaluation and certification of security features in technology products.

For embedded systems in critical infrastructure, Common Criteria certification can provide assurance that a product meets specific security requirements. However, the certification process can be time-consuming and expensive, which may limit its applicability to rapidly evolving embedded technologies.[17-21]

### Sector-Specific Regulations

Various critical infrastructure sectors have developed their own regulatory frameworks and standards to address sector-specific security challenges. For example:

- The North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) stan-

dards provide cybersecurity requirements for the bulk power system in North America.

- The Transportation Systems Sector Cybersecurity Framework Implementation Guidance, developed by the U.S. Department of Homeland Security, offers tailored guidance for applying the NIST Cybersecurity Framework to transportation systems.
- The FDA's guidance on "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices" provides recommendations for addressing cybersecurity in medical devices.

These sector-specific regulations often complement broader cybersecurity frameworks, providing more detailed guidance on securing embedded systems within particular domains of critical infrastructure.

## Conclusion

While technical solutions are crucial for securing embedded systems in critical infrastructure, the human element plays an equally important role in maintaining overall security. Human factors, including user behavior, security awareness, and organizational culture, can significantly impact the effectiveness of security measures. Let's explore the key aspects of human factors and security. Comprehensive training programs are essential for ensuring that personnel working with embedded systems understand the potential security risks and best practices for mitigating them.

The future is arriving, with edge computing, 5G networks, and distributed ledger technologies promising new capabilities and new security considerations to live with. Quantum computing, on the other hand, presents the possibility for its use on current cryptographic methods and thus necessitates ongoing researcher into post quantum cryptography for resource constrained embedded devices. To secure embedded systems in critical infrastructure, the key lies in a comprehensive and collaborative effort among CS, engineering, human factors' and policy 's communities. The goal of enhancement in the resilience and security of critical infrastructure systems on which modern society depends is enhanced by fostering innovation, promoting knowledge sharing, and remaining proactive in dealing with the evolving threats. The growing reliance upon interconnected, embedded technologies throughout the sectors of critical infrastructure is only increasing, and as such robust security measures are more important than ever. This is not a purely technical challenge, much less an ultimately solveable problem, but rather a societal imperative in which the security of our essential services has long term effects on safety, reliability and resilience and thus affects all of us.

## References:


1. Zavitsanou, S., Chakrabarty, A., Dassau, E., & Doyle III, F. J. (2016). Embedded control in wearable medical devices: Application to the artificial pancreas. *Processes*, *4*(4), 35.
2. Zuckerman, D. M., Brown, P., & Nissen, S. E. (2011). Medical device recalls and the FDA approval process. *Archives of internal medicine*, *171*(11), 1006-1011.
3. Afifi, S. M., Verdier, F., & Belleudy, C. (2014, March). Power estimation method based on real measurements for processor-based designs on FPGA. In *2014 International Conference on Computational Science and Computational Intelligence* (Vol. 2, pp. 260-263). IEEE.
4. Afifi, S. M., Verdier, F., & Belleudy, C. (2014, March). Power estimation method based on real measurements for processor-based designs on FPGA. In *2014 International Conference on Computational Science and Computational Intelligence* (Vol. 2, pp. 260-263). IEEE.
5. Swathi, S., Sushma, S., Bindusree, V., Babitha, L., Sukesh, G. K., Venkateswarlu, S. C., ... & Vallabhuni, R. R. (2021, December). Implementation of An Energy-Efficient Binary Square Rooter Using Reversible Logic By Applying The Non-Restoring Algorithm. In *2021 2nd International Conference on Communication, Computing and Industry 4.0 (C2I4)* (pp. 1-6). IEEE.
6. Ananthanarayana, T., Lopez, S., & Lukowiak, M. (2017, May). Power analysis of HLS-designed customized instruction set architectures. In *2017 IEEE International Parallel and Distributed Processing Symposium Workshops (IPDPSW)* (pp. 207-212). IEEE.
7. Varma, A., Debes, E., Kozintsev, I., Klein, P., & Jacob, B. (2008). Accurate and fast system-level power modeling: An XScale-based case study. *ACM Transactions on Embedded Computing Systems (TECS)*, *7*(3), 1-20.
8. Wang, L., Wang, X., Wang, T., & Yang, Q. (2012, November). High-level power estimation model for SOC with FPGA prototyping. In *2012 Fourth International Conference on Computational Intelligence and Communication Networks* (pp. 491-495). IEEE.
9. Zhai, J., Bai, C., Zhu, B., Cai, Y., Zhou, Q., & Yu, B. (2022). McPAT-Calib: A RISC-V BOOM microarchitecture power modeling framework. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, *42*(1), 243-256.
10. Venkateshwarlu, S. C., Khadir, M., Vijay, V., Pittala, C. S., & Vallabhuni, R. R. (2022, February). Optimized Design of Power Efficient FIR Filter Using Modified Booth Multiplier. In *2021 4th International Conference on Recent Trends in*

*Computer Science and Technology (ICRTCST)* (pp. 197-201). IEEE.

11. Marwedel, P. (2021). *Embedded system design: embedded systems foundations of cyber-physical systems, and the internet of things* (p. 433). Springer Nature.
12. Lavagno, L., Sangiovanni-Vincentelli, A., & Sentovich, E. M. (2000). Models of computation for system design. In *Architecture Design and Validation Methods* (pp. 243-295). Berlin, Heidelberg: Springer Berlin Heidelberg.
13. Gup, R. K., & De Micheli, G. (1996). A co-synthesis approach to embedded system design automation. *Design Automation for Embedded Systems*, *1*, 69-120.
14. Wang, S., & Shin, K. G. (2000, November). An architecture for embedded software integration using reusable components. In *Proceedings of the 2000 international conference on Compilers, architecture, and synthesis for embedded systems* (pp. 110-118).
15. Stone, J. E., Gohara, D., & Shi, G. (2010). OpenCL: A parallel programming standard for heterogeneous computing systems. *Computing in science & engineering*, *12*(3), 66.
16. Nagaraju, V. S., Sadgurbabu, B., & Vallabhuni, R. R. (2021, May). Design and Implementation of Low power FinFET based Compressor. In *2021 3rd International Conference on Signal Processing and Communication (ICPSC)* (pp. 532-536). IEEE.
17. Reyes, R., Brown, G., Burns, R., & Wong, M. (2020, April). Sycl 2020: More than meets the eye. In *Proceedings of the International Workshop on OpenCL* (pp. 1-1).
18. Li, X., Gan, C., Gou, K., & Zhang, Y. (2019). A novel WDM-MAN enabling cross-regional reconfiguration and comprehensive protection based on tangent-ring. *Optics Communications*, *430*, 416-427.
19. Marshall, G. J., Mahony, C. P., Rhodes, M. J., Daniewicz, S. R., Tsolas, N., & Thompson, S. M. (2019). Thermal management of vehicle cabins, external surfaces, and onboard electronics: An overview. *Engineering*, *5*(5), 954-969.
20. Mohammedi, M., Kraa, O., Becherif, M., Aboubou, A., Ayad, M. Y., & Bahri, M. (2014). Fuzzy logic and passivity-based controller applied to electric vehicle using fuel cell and supercapacitors hybrid source. *Energy Procedia*, *50*, 619-626.
21. Monmasson, E., Idkhajine, L., Cirstea, M. N., Bahri, I., Tisan, A., & Naouar, M. W. (2011). FPGAs in industrial control applications. *IEEE Transactions on Industrial informatics*, *7*(2), 224-243.
22. Usikalu, M. R., Alabi, D., & Ezeh, G. N. (2025). Exploring emerging memory technologies in modern electronics. Progress in Electronics and Communication Engineering, 2**(2), 31-40. https://doi.org/10.31838/PECE/02.02.04**
23. Prasath, C. A. (2024). Energy-efficient routing protocols for IoT-enabled wireless sensor networks. *Journal of Wireless Sensor Networks and IoT, 1*(1), 1-7. https://doi.org/10.31838/WSNIOT/01.01.01.
24. Ristono, A., & Budi, P. (2025). Next-gen power systems in electrical engineering. *Innovative Reviews in Engineering and Science*, *2*(1), 34-44. https://doi.org/10.31838/INES/02.01.04
25. Rahim, R. (2024). Optimizing reconfigurable architectures for enhanced performance in computing. *SCCTS Transactions on Reconfigurable Computing, 1*(1), 11-15. https://doi.org/10.31838/RCC/01.01.03
26. Prasath, C. A. (2024). Optimization of FPGA architectures for real-time signal processing in medical devices. *Journal of Integrated VLSI, Embedded and Computing Technologies, 1*(1), 11-15. https://doi.org/10.31838/JIVCT/01.01.03
27. Rahim, R. (2023). Effective 60 GHz signal propagation in complex indoor settings. *National Journal of RF Engineering and Wireless Communication, 1*(1), 23-29. https://doi.org/10.31838/RFMW/01.01.03
28. Ramanan, S. V., & Vimal, E. (2015). Minimizing the energy consumption of wireless sensor network by comparing the performances of maxweight and minimum energy scheduling algorithms. *International Journal of Communication and Computer Technologies, 3*(1), 9-15. https://doi.org/10.31838/IJCCTS/03.01.03
29. Mejail, M., Nestares, B. K., Gravano, L., Tacconi, E., Meira, G. R., & Desages, A. (2022). Fundamental Code Converter Block Design Using Novel CMOS Architectures. Journal of VLSI Circuits and Systems, 4(2), 38-45. https://doi.org/10.31838/jvcs/04.02.06
30. Barhani, D., Kharabi, P., & Jarhoumi, E. F. (2022). The ubiquitous influence of WiMAX for next-generation applications. *National Journal of Antennas and Propagation, 4*(1), 21-26.