International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

Securing SPI (Serial Peripheral Interface) Data for Field Replaceable Units (FRUs) in Commercial Electronic Devices

Roopak Ingole[1], Siva Sathyanarayana Movva[2]

[1]Technical Advisor – Advanced Embedded Software Corporate Research & Technology, Cummins Inc., Columbus IN, USA
Email: *roopak.ingole[at]cummins.com*

Staff Firmware Engineer Max Linear Inc. Carlsbad CA, USA
Email: *sivasathya[at]gmail.com*

Abstract: ***This paper will delve into the significance of secure communication within commercial embedded systems, focusing on the role of Field Replaceable Units (FRUs), the Serial Peripheral Interface (SPI) and non-volatile storage. It will set the stage for the necessity of securing SPI data to prevent unauthorized access and ensure reliable and confidential communication, especially in critical applications such as public safety, military, and industrial settings. The paper's objectives, including identifying vulnerabilities, exploring security challenges, and proposing robust security strategies, will be outlined. It will introduce the concept of Field Replaceable Units (FRUs) and their significance in maintaining and upgrading electronic systems. Furthermore, it will discuss the Serial Peripheral Interface (SPI) protocol's role in enabling communication between the microcontroller and other peripherals in FRUs along with non-volatile storage on FRU, setting the stage for a discussion on the security implications of SPI data transmission and storage.***

Keywords: SPI, Serial Peripheral Interface, Field Replaceable Unit, FRU

1. Introduction

With the introduction of Internet of Things and more connected solutions, the complexity of commercial electronic devices is increasing. Due to this complexity, companies are making their commercial devices as combination of smaller devices to reduce the cost of service and simplicity in replacing the components. The Field Replaceable Units (FRU) architecture becomes upmost important in maintaining and upgrading these commercial devices. We will delve deeper into the critical role of commercial electronic systems in emergency response, public safety, industrial operations, and transportation emphasizing the necessity for secure operations. Furthermore, it will discuss the Serial Peripheral Interface (SPI) protocol's role in enabling communication between the microcontroller and other peripherals in FRUs, setting the stage for a discussion on the security implications of SPI data transmission. There are certain challenges with SPI data transmission with respect to security of transmission and storage of data on non-volatile memory of FRUs. Later, we will discuss some mitigation strategies, and the impact of these strategies on the overall security posture FRUs.

2. Background

1) Commercial Electronic Devices

Commercial electronic systems have become indispensable in the modern business landscape, revolutionizing the way companies operate, communicate, and deliver services. At their core, these systems encompass a wide array of hardware and software solutions designed to facilitate efficient business processes, enhance customer engagement, and ensure seamless internal and external communications. From sophisticated point-of-sale (POS) systems, enterprise resource planning (ERP) software, to digital marketing platforms and e-commerce websites, each component plays a pivotal role in optimizing operational efficiencies and driving sales. Moreover, with the advent of Internet of Things (IoT) technologies, commercial electronic systems are increasingly becoming more integrated and capable of providing real-time data analytics, thus enabling businesses to make informed decisions swiftly and accurately. The adoption of these electronic systems not only streamlines workflows but also provides a competitive edge by adapting to changing market dynamics and consumer behaviors more effectively. [1]

Field Replaceable Units (FRUs) are critical components within commercial electronic devices, designed for quick and easy replacement in the field without the need for specialized skills or tools. This modular approach to device construction not only streamlines maintenance and repair processes but also significantly enhances the operational efficiency and reliability of electronic systems used in business settings. For instance, in base-station radios or repeaters are equipped with FRUs such as power supplies boards, main control module, chassis module, modem and front panel/human-machine interface, allowing service technician staff to promptly replace failing components and minimize communication downtime. Similarly, in point-of-sale (POS) systems, components like card readers and printers are often designed as FRUs, ensuring retail operations can continue with minimal interruption. [2]

The economic rationale behind implementing FRUs is compelling. By enabling on-site replacements of defective parts, businesses can avoid the costs and delays associated with sending devices back to manufacturers or service centers for repair. This not only reduces repair and shipping costs but also ensures that devices are back in operation much faster, maintaining productivity and service levels.

Additionally, the ability to replace only the faulty component, rather than the entire device, contributes to more sustainable business practices by reducing electronic waste. [2]

Moreover, FRUs play a vital role in minimizing operational downtime, a critical factor for businesses where continuous operation is paramount. The agility offered by FRUs ensures that commercial electronic systems can maintain high availability and reliability, crucial for customer satisfaction and business continuity. [2]

2) SPI in Embedded Systems

a) Introduction to SPI

The Serial Peripheral Interface (SPI) is a synchronous serial communication protocol used for short-distance communication, primarily in embedded systems. Known for its simplicity and speed, SPI operates on a host-device architecture, allowing a host to communicate with one or more devices over four primary wires: MOSI (Master Out Slave In), MISO (Master In Slave Out), SCK (Serial Clock), and SS (Slave Select). [3] [4]

b) SPI in FRUs

Within Field Replaceable Units (FRUs) [5], SPI plays a crucial role in enabling swift and efficient communication between the FRU and the main control module of the device. This is essential for the initial recognition of the FRU by the system and for subsequent operational commands and data exchanges. SPI's high-speed data transfer capabilities ensure that FRUs can quickly become operational and seamlessly integrate into the system's ecosystem. [6]

Upon installation, FRUs often require immediate configuration to align with the system's settings and operational parameters. SPI facilitates this process by enabling the master device (usually the main controller) to send configuration data to the FRU. This process ensures that the FRU can operate according to the specific requirements and constraints of the system, enhancing compatibility and performance.

SPI also plays a vital role in the diagnostics and monitoring of FRUs. Through SPI, the main system can query the FRU for status updates, perform health checks, and retrieve diagnostic data. This capability is critical for proactive maintenance and for diagnosing issues early, thereby minimizing downtime and maintaining system integrity.

3) Non-Volatile Memory Storage on FRU

SPI Flash memory is a type of non-volatile storage medium that can be electrically erased and reprogrammed. It is commonly used in electronic components for storing firmware, due to its high speed, reliability, and efficiency. Connected via the Serial Peripheral Interface (SPI), it allows for simple, yet fast, data transactions between the memory component and the main processor or microcontroller. [7]

In the context of FRUs, SPI Flash serves as an essential repository for firmware—the low-level software that provides the necessary instructions for how the device operates. This is especially critical for components that require specific initialization sequences or operational instructions that are too complex or too large to be stored in the primary controller's limited onboard memory. [7] [8]

SPI Flash memory can also store configuration data for FRUs. This data tailors the operation of the device to the specific requirements and preferences of the system it integrates with. By storing such data in SPI Flash, FRUs can be pre-configured or easily reconfigured post-installation, ensuring seamless integration and optimal performance within the host system. [8]

Another significant use of SPI Flash in FRUs is for system recovery and firmware updates. In scenarios where the system firmware needs to be recovered or updated, SPI Flash can provide a reliable storage location for the recovery code or new firmware version. This feature is crucial for maintaining the integrity and up-to-dateness of the FRU's firmware, especially in the event of corruption or when enhancements are made. [8]

4) **Challenges in Securing SPI Data**

The Field Replaceable Units (FRUs) incorporating SPI Flash, security concerns are increasingly prominent due to the critical role these components play in both the operation and integrity of commercial electronic devices. SPI Flash memory is widely used in FRUs for firmware storage, configuration data, and sometimes, sensitive information that dictates how the FRU interacts with the main system. Key security concerns associated with SPI Flash in FRUs are, unauthorized access, firmware integrity, and data protection.

a) Unauthorized Access

Unauthorized access is a significant security concern for SPI Flash in FRUs. Since SPI Flash is often used to store firmware or configuration data, unauthorized reading of this flash memory can reveal sensitive information about the device's operation, proprietary algorithms, or system configuration. Moreover, if attacker gains write access to the SPI Flash, they could modify the firmware or configuration data, leading to compromised device functionality, insertion of malicious code, or bricking of the device.

b) Firmware Integrity

Maintaining the integrity of the firmware stored on SPI Flash is crucial. Firmware integrity checks are essential to ensure that the firmware has not been tampered with or corrupted. This is particularly important for FRUs, as compromised firmware can lead to vulnerabilities in the device's operation, potentially allowing attackers to exploit these weaknesses. Secure boot mechanisms and cryptographic signature verifications are common strategies to ensure firmware integrity. However, if not implemented or managed correctly, these mechanisms can be bypassed or compromised.

5) **Data Protection**

Data protection is another critical concern, especially for SPI Flash memory that stores sensitive configuration data or

proprietary information. Encryption of the data stored on SPI Flash is a necessary measure to prevent data leakage or unauthorized access. However, the implementation of encryption and key management poses its own set of challenges, including key storage, key exchange, and ensuring that the encryption does not adversely affect the performance or functionality of the FRU.

6) Strategies for Enhancing Security

Encryption Techniques

Encryption in SPI (Serial Peripheral Interface) communication, especially within the context of Field Replaceable Units (FRUs) that utilize SPI Flash, is critical for ensuring the security of data in transit between the master and slave devices. The implementation of encryption can be approached through software algorithms or through hardware-based solutions.

Software-Based Encryption for SPI Communication

a) Symmetric Encryption Algorithms:

AES (Advanced Encryption Standard) is a widely used symmetric encryption algorithm suitable for SPI communication. It can operate in several modes, but for SPI communication, CBC (Cipher Block Chaining) or CTR (Counter) modes are commonly used due to their ability to encrypt data blocks independently. *[9] [10]*

The encryption and decryption processes are implemented in the firmware of both the master and slave devices. Before transmission, data packets are encrypted by the sender, transmitted over SPI, and then decrypted by the receiver.

b) Key Management:

For FRU, Static Key Sharing is preferred and are pre-programmed with a shared secret key. This method, while straightforward, raises concerns about key distribution and storage security. *[9]*

Hardware-Based Encryption for SPI Communication

a) Dedicated Encryption Modules:

Some microcontrollers and processors come with built- in hardware encryption modules designed to offload the computational burden of encryption from the CPU. These modules can directly encrypt or decrypt SPI data streams, significantly increasing the efficiency of the process.

b) Hardware Security Modules (HSMs):

HSMs are external devices or embedded chips that provide advanced security features, including key management, hardware-based encryption/decryption, and secure storage. When used in conjunction with SPI communication, HSMs can ensure that encryption keys never leave the module, providing a higher level of security. *[11] [12]*

c) Trusted Platform Modules (TPMs):

TPMs are secure crypto-processors that can be used to secure hardware through integrated cryptographic keys. For SPI communication, TPMs can secure the SPI bus by providing hardware-based encryption, secure key storage, and ensuring the integrity and authenticity of the devices communicating over SPI. *[13] [14] [15]*

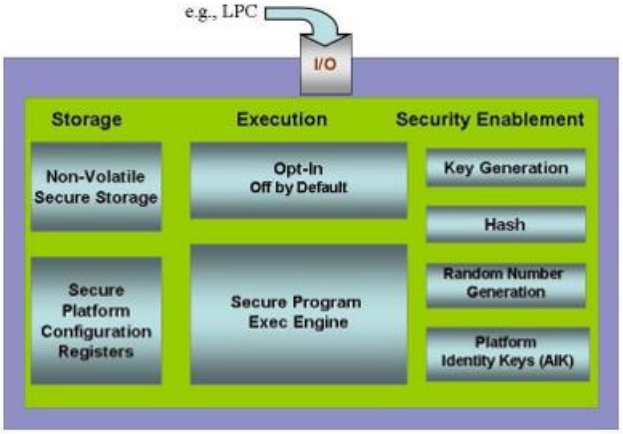

Figure 1: Trusted Platform Module Architecture [13]

d) Access Control and Authentication

Applying access control and authentication in Serial Peripheral Interface (SPI) communication is crucial for protecting the integrity and confidentiality of data transmitted between a master device and its peripherals, including Field Replaceable Units (FRUs). Given SPI's simplicity and widespread use in embedded systems, securing its communication involves implementing mechanisms that prevent unauthorized access and ensure data integrity.

Encrypting data transmitted over SPI ensures that even if an unauthorized party intercepts the communication, the data remains incomprehensible and secure. Symmetric encryption algorithms like AES can be used due to their efficiency in embedded systems. [9]

Secure key exchange mechanisms must be established to securely share encryption keys between the master device and the FRU. This could involve using asymmetric encryption algorithms or hardware security modules (HSMs) for key storage and exchange. [12]

Before any sensitive operation or data exchange, both the master device and the FRU should authenticate each other. This can be achieved through challenge-response mechanisms using pre-shared keys or digital certificates.

Utilize hardware tokens or secure elements that store cryptographic keys and perform authentication operations.

These devices can offer a robust way to authenticate devices in SPI communication, making it difficult for unauthorized devices to mimic legitimate FRUs.

Appending a MAC or digital signature to each SPI message ensures that the integrity of the data can be verified by the receiver. This protects against tampering or unauthorized modification of the data during transmission.

3. Case Studies and Real-World Applications

With the above technical considerations, this section will elaborate detailed case study showcasing implementation of security measures in two-way radio systems. This case study will analyze the specific security challenges faced, the

solutions implemented, and the outcomes of these efforts. The case studies will cover a range of scenarios, including military, public safety, and industrial applications, providing insights into the practical aspects of securing SPI data in FRUs.

The radio system of the base station incorporates several key components: the primary base station board, a board for power management, an HMI interface board, a modem circuit, and the system chassis, all classified as Field Replaceable Units (FRUs). These components utilize the SPI protocol for both recognizing modules and transferring data Figure 2: Typical Base-station Radio FRU Architecture. Embedded in each board is an SPI Flash memory, dedicated to preserving crucial, component-specific data. This data is of paramount importance, both to consumers and the manufacturing entity, serving as a critical element in processing warranty claims and facilitating installations tailored to the product. [16]

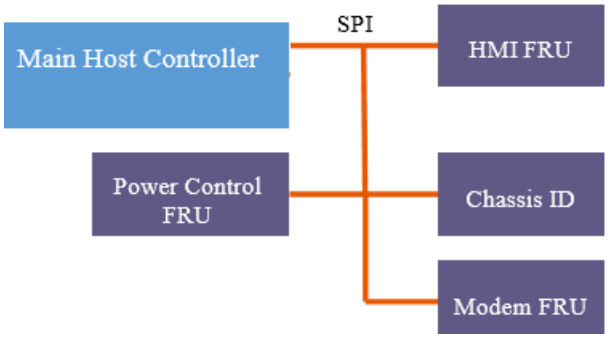

Figure 2: Typical Base-station Radio FRU Architecture

To make the SPI transmission secure and protect the stored data on FRU, we can implement security strategy in base station radio as below.

a) **Security Strategy**

1) *Data Encryption:*
The data to be transmitted over SPI is first passed through the encryption module (software or hardware-based), ensuring that all data on the SPI bus is encrypted and thus protected from eavesdropping or modification. Implementing encryption for SPI communication in FRUs is essential for protecting sensitive data and ensuring secure device operation.

2) *Key Management:*
For systems comprising multiple FRUs, like base-station radios, utilizing static encryption keys is most efficient way to implement. This can be achieved through one-time programmable (OTP) secure storage for key or hardware- based key generation that ensure keys are securely generated and stored.

3) *Continuous Integrity Checks:*
To further secure SPI communication, integrity checks such as HMAC (Hash-based Message Authentication Code) can be implemented alongside encryption. This ensures the data integrity and authenticity of the messages being transmitted.

b) **Security Implementation**

1) *Use of SPI Flash in Base-Station Radio FRUs*
In base-station radio Field Replaceable Units (FRUs), SPI (Serial Peripheral Interface) Flash memory is primarily used to store FRU-specific information. This data is non-volatile and does not require any computational capability directly within the storage medium. The choice of SPI Flash is due to its efficiency in storing structured data that can be easily accessed by the host system when needed.

2) *Choice of Symmetric Encryption*
Symmetric encryption was chosen for securing the data because the host system is responsible for both encryption and decryption processes. This method is straightforward and efficient, particularly when the encryption and decryption occur in the same environment or system. Symmetric encryption allows for the secure storage of data on the SPI Flash, with a predetermined record structure, without adding computational complexity to the FRU itself.

3) *Key Management*
Key management is a critical aspect of data security. In this setup, the host system manages the encryption keys, storing FRU-specific keys in a secure location. This approach ensures that keys are protected and accessible only by authorized entities, significantly reducing the risk of unauthorized data access.

4) *Host Microcontroller and Operating System*
The host microcontroller, based on an ARM architecture, operates using the POSIX-compliant [17] Nucleus Real-time Operating System provided by Mentor Graphics [18]. The POSIX compliance of the operating system facilitates the integration of the OpenSSL library, which is a robust suite of cryptography tools. OpenSSL provides the necessary components for implementing various cryptographic functions, including encryption, decryption, and key management. [19] [20] Figure 3: Class Diagram

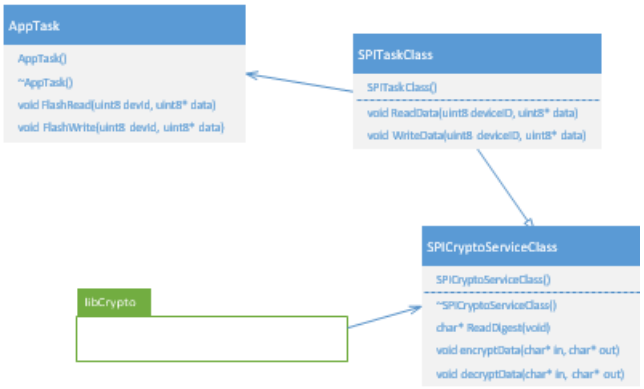

Figure 3: Class Diagram

5) *Encryption Algorithm and Application-Level Implementation*
For securing the data stored on the SPI Flash, the 128-bit AES (Advanced Encryption Standard) algorithm was utilized. AES is a widely recognized and powerful encryption standard that ensures the confidentiality of data. At the application level, specific methods for encryption and decryption are implemented, as indicated in Figure 3: Class Diagram. Additionally, a sequence diagram is referenced to illustrate the sequence of events during the encryption and decryption processes. [19] Figure 4: Message Sequence Diagram

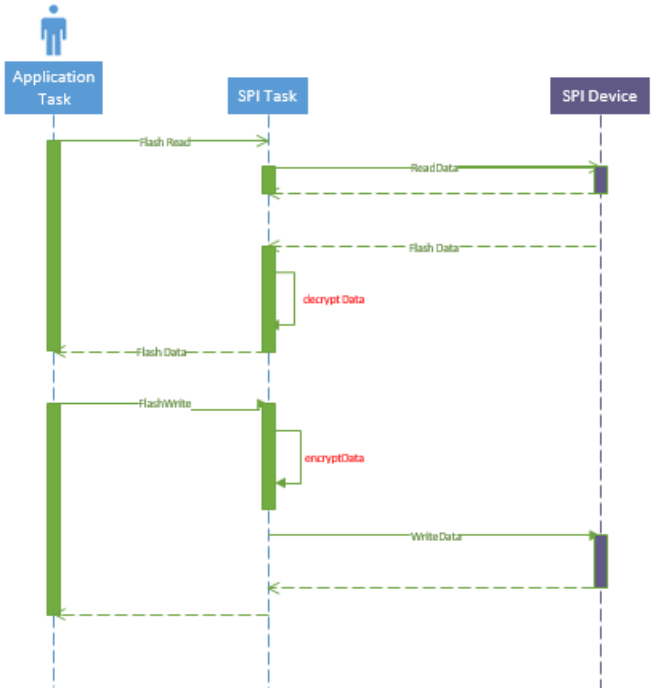

Figure 4: Message Sequence Diagram

c) **Data Transmission and Integrity Checks**

Since the data transmitted to the SPI Flash is already encrypted, there is no need for additional transmission-level encryption. Furthermore, due to the SPI Flash being a storage device without computational capabilities, continuous integrity checks, such as HMAC (Hash-Based Message Authentication Code), was not feasible. However, the use of symmetric cryptography achieves the necessary level of secure transmission over SPI and protects the stored data effectively. [19]

4. Summary

In summary, the secure management of data in base- station radio FRUs involves the use of SPI Flash for storage, symmetric encryption for data security, meticulous key management by the host, and the implementation of cryptographic functions facilitated by a POSIX-compliant operating system and the OpenSSL library. This comprehensive approach ensures the secure storage and handling of FRU-specific information, safeguarding against unauthorized access and ensuring the integrity of the system.

5. Future Use Cases

In the realm of automotive powertrain management, Electronic Control Modules (ECMs) play a pivotal role by leveraging serial flash memory to store essential operational firmware and configuration data. This setup facilitates the efficient control of engine parameters, including but not limited to fuel injection rates and ignition timings, thereby optimizing performance and emissions. Given the critical nature of the data involved, adopting robust security measures for both data transmission and storage becomes imperative. This ensures that sensitive information remains safeguarded against unauthorized access and manipulation, which is essential for maintaining the vehicle's integrity and safety.

Furthermore, the ECM's utilization of the Serial Peripheral Interface (SPI) for facilitating precise communication with Application-Specific Integrated Circuits (ASICs) underscores the importance of secure data exchange protocols. ASICs, which perform specialized functions such as processing sensor inputs and managing actuator outputs, are integral to the vehicle's operational efficiency and safety. Therefore, securing SPI communication is not merely a precaution but a necessity to prevent adverse scenarios such as unintended fuel delivery or improper power generation, which could have dire consequences for vehicle performance and safety. Through the implementation of encryption and secure communication standards, it is possible to ensure the reliability and security of these critical automotive systems.

6. Conclusion and Future Directions

Conclusion

This paper has explored the critical importance of securing Serial Peripheral Interface (SPI) data in Field Replaceable Units (FRUs) within commercial electronic devices. Through a detailed examination of the challenges and vulnerabilities associated with SPI data transmission and storage, alongside the strategies for enhancing security, we have underscored the necessity for robust protection mechanisms in the realm of embedded systems security. The implementation of encryption techniques, secure boot processes, and rigorous access control and authentication measures stand out as pivotal elements in safeguarding SPI data from unauthorized access, ensuring the integrity of firmware, and protecting sensitive configuration data stored on SPI Flash in FRUs.

The adoption of hardware-based encryption solutions, including the use of dedicated encryption modules, Hardware Security Modules (HSMs), and Trusted Platform Modules (TPMs), has been highlighted as offering superior security advantages. These measures not only secure SPI communication but also address key management challenges, thereby enhancing the overall security posture of commercial electronic systems. Furthermore, the case studies presented, particularly the security strategy implementation in base- station radio FRUs, illustrate the practical application of these security measures in real-world scenarios, demonstrating their effectiveness in mitigating risks associated with SPI data security.

Future Directions

Looking ahead, the field of securing SPI data in FRUs presents several promising avenues for further research and development:

Advanced Encryption Techniques: The exploration of more sophisticated encryption algorithms and the development of custom encryption solutions tailored to the specific requirements of SPI communication in embedded systems. This includes researching lightweight encryption methods

that can be efficiently implemented in resource- constrained devices.

Physical Security Measures: The investigation into enhancing the physical security of devices to complement the digital security measures. This involves developing tamper- resistant and tamper-evident designs that protect against physical attacks aimed at compromising device security.

Authentication Mechanisms: The advancement of innovative authentication techniques, particularly those that can securely manage and authenticate the identities of devices and users in SPI communication. This includes the utilization of biometric data, secure tokens, and blockchain technology for heightened security.

Secure Communication Standards: The formulation and adoption of secure communication standards specific to SPI communication in embedded systems. These standards would provide guidelines for encryption, key management, authentication, and secure channel establishment, ensuring a unified approach to securing SPI data.

Interdisciplinary Collaboration: Encouraging collaboration between cybersecurity researchers, hardware manufacturers, and software developers to foster a holistic approach to security. This multidisciplinary effort can lead to the development of integrated security solutions that address both hardware and software vulnerabilities in commercial electronic systems.

In conclusion, as commercial electronic devices continue to evolve and play a pivotal role in modern infrastructure, the security of SPI data in FRUs remains a critical concern. By addressing the challenges outlined in this paper and pursuing the suggested future directions, we can significantly enhance the security and reliability of these systems, thereby contributing to the safety and efficiency of numerous applications across various sectors.

References

[1] EBOXMAN, "The Importance of E-Commerce in Modern Business," [Online]. Available: https://eboxman.com/the- importance-of-e-commerce-in-modern-business/.
[2] K. Kasemsap, "The Importance of Electronic Commerce in Modern Business," [Online]. Available: https://www.igi- global.com/chapter/the-importance-of-electronic-commerce-in- modern-business/183990.
[3] Wikipedia, "Serial Peripheral Interface," [Online]. Available: https://en.wikipedia.org/wiki/Serial_Peripheral_Interface.
[4] Parikh, "SPI: What is the Serial Peripheral Interface Protocol?," [Online]. Available: https://www.engineersgarage.com/spi-what-is- serial-peripheral-interface-protocol/.
[5] Wikipedia, "Field-replaceable unit," [Online]. Available: https://en.wikipedia.org/wiki/Field-replaceable_unit.
[6] TechTarget, "field-replaceable unit (FRU)," [Online]. Available: https://www.techtarget.com/searchdatacenter/definition/field- replaceable-unit.
[7] Adafruit, "Using SPI Flash," [Online]. Available: https://learn.adafruit.com/adafruit-hallowing/using-spi-flash.
[8] Giovino, "Why and How to Expand Microcontroller Program Memory with SPI XiP Flash," [Online]. Available: https://www.digikey.com/en/articles/why-and-how-to-expand- microcontroller-program-memory-with-spi-xip-flash.
[9] L. V. Houtven, Crypto 101. Dynamic Solutions Group, "Software vs. Hardware Encryption: The Pros and Cons," [Online]. Available: https://www.dsolutionsgroup.com/software-vs-hardware- encryption/.
[10] Rawlings, "Hardware Security Requirements for Embedded Encryption Key Storage," [Online]. Available: https://www.design-reuse.com/articles/18803/embedded-encryption-key-storage.html.
[11] Davies and C. McKenzie, "hardware security module (HSM)," [Online]. Available: https://www.techtarget.com/searchsecurity/definition/hardware- security-module-HSM.
[12] Trusted Computing Group, "Trusted Platform Module (TPM) Summary," [Online]. Available: https://trustedcomputinggroup.org/resource/trusted-platform- module-tpm-summary/.
[13] M. Bond and P. Landrock, "THE TRUSTED PLATFORM MODULE EXPLAINED," [Online]. Available: https://www.cryptomathic.com/news-events/blog/the-trusted- platform-module-explained.
[14] S. Gillis, "Trusted Platform Module (TPM)," [Online]. Available: https://www.techtarget.com/whatis/definition/trusted-platform- module-TPM.
[15] Motorola Solutions Inc., "SLR 8000 - SEE ME FIRST BEFORE REPLACING AND INSTALLING A FRU," [Online]. Available: https://video.motorolasolutions.com/detail/video/4920578387001/slr-8000---see-me-first-before-replacing-and-installing-a-fru.
[16] IEEE and The Open Group, "POSIX," [Online]. Available: https://pubs.opengroup.org/onlinepubs/9699919799.2018edition/.
[17] Mentor Graphics, "Nucleus RTOS," Mentor Graphics, [Online]. Available: https://www.plm.automation.siemens.com/global/en/products/embed ded/nucleus-rtos.html.
[18] V. Shirgur, "openssl_example," [Online]. Available: https://github.com/vikramls/openssl_examples.
[19] OpenSSL Project, "OpenSSL," [Online]. Available: https://www.openssl.org/.
[20] Motorola Solutions Inc., "SLR 8000 - REPLACE AND INSTALL THE MODEM FRU," [Online]. Available: https://video.motorolasolutions.com/detail/videos/two-way- radios/video/4923069272001/slr-8000---replace-and-install-the- modem-fru.
[21] Motorola Solutions Inc., "GTR 8000 Base Radio,"

[Online]. Available: https://fcc.report/FCC-ID/ABZ89FC4831/5137942.pdf.
[22] Silicon Storage Technology, "SPI Serial Flash," [Online]. Available: https://ww1.microchip.com/downloads/aemDocuments/documents/ OTH/ProductDocuments/DataSheets/01357A.pdf.
[23] Kidd, "Data Encryption Methods & Types: Beginner's Guide To Encryption," [Online]. Available: https://www.splunk.com/en_us/blog/learn/data-encryption-methods- types.html.
[24] T. Stapko, "Cryptography for embedded systems – Part 1: Security level categories & hashing," [Online]. Available: https://www.eetimes.com/cryptography-for-embedded-systems-part- 1-security-level-categories-hashing/.
[25] Witekio, "Secure Boot in Embedded Systems," [Online]. Available: https://witekio.com/embedded-software-services/embedded- security/embedded-systems-secure-boot/.