Dependable and Secure Embedded Node Demonstrator

Przemysław Osocha[1], João Carlos Cunha[2], and Fabio Giovagnini[3]

[1,3]SESM s.c.a.r.l., Naples, Italy
[1]p.osocha@gmail.com, [3]fabio.giovagnini@gmail.com
[2]Polytechnic Institute of Coimbra / CISUC, Coimbra, Portugal
jcunha@isec.pt

Abstract. The European industry competitiveness in the embedded devices market is threatened by challenges such as cost-effectiveness, interoperability, reliability, and re-usability. This is particularly important now, when the value of embedded electronics components share in the final products is increasing, especially in ICT and health/medical equipment domains.

To address these challenges, the pSHIELD project, co-funded by ARTEMIS JU, was aimed at developing an architecture framework supporting security, privacy and dependability (SPD) as built-in features in a network of embedded nodes. That approach will provide industry with the key improvements such as a faster design, standardized development of SPD solutions and a flexible way to reuse already verified embedded systems.

This paper reports the architecture of an FPGA-based intrusion detection embedded device for a freight train, built to validate the pSHIELD concept at a node level. The use case demonstrates the legacy components integration, dependability, security, self-reconfiguration and the node-level composability.

Keywords: security, dependability, embedded system, FPGA, partial reconfiguration

1 Introduction

In the modern world, embedded devices are present anytime and anywhere. They are distributed ubiquitously, pervasively and unobtrusively in everyday environments in many different forms: small or large, visible or invisible, simple or complex, wired or wireless and so on.

The massive deployment of networked embedded systems, seamlessly interconnected with each other, dealing with sensitive information and acting in critical environments is posing new challenges to developers. Dependability and security of embedded systems cannot be any longer analyzed for separated devices, but rather in a distributed context as systems of systems.

The contemporary market of embedded systems requires a built-in approach where security, privacy and dependability (SPD) functionalities are natively addressed from the design through the entire system life-cycle in contrast with an SPD add-on approach, which is in use today. In particular, the industry needs an approach to SPD which will provide the key improvements such as a faster design, a flexible way to reuse already validated systems and the standardized development of SPD solutions.

To meet these ambitious requirements, ARTEMIS JU [1] co-funded the pSHIELD project [2], addressing the reusability of previously designed solutions and the standardization and interoperability of advanced SPD technologies. This project aims to build a reference model for all the security, privacy and dependability aspects involving networked embedded systems [3]. In fact, the provided architecture will pursue the design and development of a multi-layer/multi-technology framework able to guarantee the composability of SPD functionalities. The project concept development is continued under the new ARTEMIS JU project nSHIELD. To validate the pSHIELD project concept, a global use case scenario based on the monitoring of hazardous materials transported by train has been proposed. This paper presents the architecture and scenarios built to demonstrate the pSHIELD SPD capabilities at the Node level.

2 Embedded Node Architecture

The pSHIELD framework [3] is composed of four layers: Node, Network, Middleware and Overlay. The Node layer implements intelligent hardware and firmware SPD functionalities and services; the Network layer is responsible for the secure, trusted, dependable and efficient data transfer based on self-configuration, self-management, self-supervision and self-recovery; the Middleware layer assures secure and efficient resource management and inter-operation among heterogeneous Embedded Systems' (ES) networks; the Overlay layer guarantees that different SPD modules belonging to the node, network and middleware layers can be *composed* in a proper way in order to solve any SPD issue globally. The output of each layer is available at the upper level which will take advantage of SPD features developed at a lower level empowering SPD features of the whole pSHIELD architecture in a transparent but manageable way.

At the Node level there may be distinguished three different kinds of Intelligent ES Nodes: Nano Node, Micro/Personal Node and Power Node. These three types of nodes, which can be considered as three node levels of increasing complexity, represent the basic components of the lower part of the SPD pervasive system and cover the possible requirements of several market areas: from the field data acquisition to transportation, personal space, home environment and to public infrastructures, etc.

Figure 1 provides a conceptual model of a pSHIELD Node Layer. This generic SPD Node architecture is composed of several functional blocks, where each block can implement features of various complexity. These nodes can be built using miscellaneous hardware architectures, they can also provide diverse functionalities and capabilities and assure different SPD compliance levels, depending on the type of a node and on the application field. For example, a typical Nano Node does not include capabilities such as Security and Privacy, Power Management and Reconfiguration.

The pSHIELD SPD Node Layer has two interfaces: one providing the pSHIELD Node Capabilities (pS-NC) to the pSHIELD Middleware Layer offering, for example, the necessary means for composing different nodes in an SPD system; and another interface with legacy, technology-dependent Node Capabilities (NC). The Legacy Node Capabilities are the capabilities already available for any embedded device provided by the Node Legacy Device Components such as CPU, I/O interfaces, memory, battery, etc. These capabilities are extended with SPD functionalities by the Node pSHIELD Specific Components which provide innovative SPD functionalities, such as the checkpoint-recovery, status and metrics. The translation between the technology-independent commands, configurations and decisions coming from the pS-NC interface into the technology-dependent ones is assured by the pSHIELD Node Adapter.

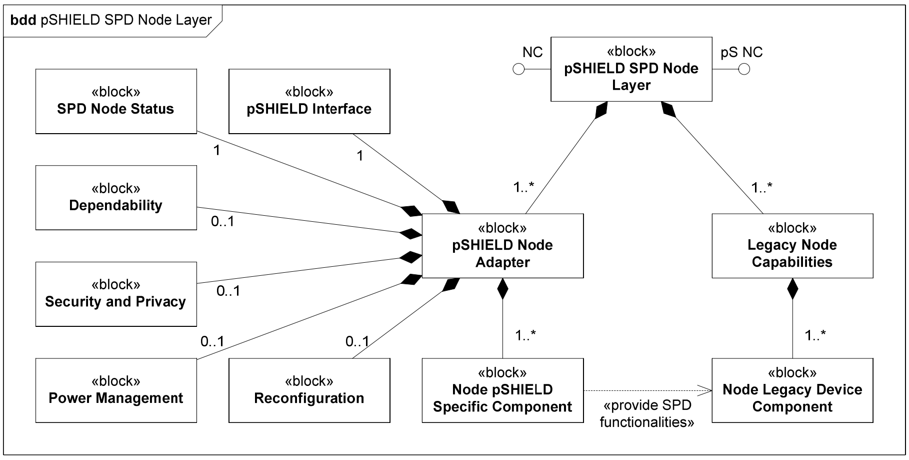

Fig. 1. pSHIELD SPD Node Layer Conceptual Architecture

Then, some innovative SPD components have been grouped into proper modules, such as: the pSHIELD Interface, which provides a proper interface for the pSHIELD Network; the SPD Node Status responsible for collecting the status of each individual component and providing SPD-relevant parameters and measurements to the Middleware Layer, and also responsible for checking the system health status for self-recovery, self-reconfiguration and self-adaptation; Reconfiguration, which performs the module or system reconfiguration by demand of the system SPD Node Status or the Middleware; Dependability responsible both for applying self-dependability at a node layer by detecting problems related to the system health status and for starting recovery; Security and Privacy, which enforces the system security and privacy at a node level by providing hardware or software encryption, decryption, key generation, firmware protection, etc.; and Power Management for managing power sources, and providing protection against blackouts, etc. The rationale behind the choice of these modules comes from the pSHIELD requirements, where a node should be built with extended dependability, security, privacy, composability, self-reconfiguration, self-adaptation and power management. Further details are available in the public deliverables of the pSHIELD project [3].

3 Power Node Demonstrator

Some of the pSHIELD Node capabilities were demonstrated by building a prototype for a test scenario. It consisted in the use of the FSK modulation to transmit the data between intrusion detection sensors placed in different cars of a freight train and an SPD Power Node, which in turn processes the signals and sends information to a Control Center through the pSHIELD network.

The intrusion detection systems are embedded devices which include a remote proximity sensor and a data encryptor. The remote proximity sensor is continuously measuring the distance to a nearby object. The encrypted data is then modulated, using the FSK modulation, and transmitted to the Power Node. Each device modulates the signal with a different carrier, so that the Power Node is able to receive signals from different sources, ensuring the possibility to connect the redundant sensors.

The Power Node receives the signals, demodulates them, decrypts, processes the data and provides it to a Control Center (Middleware layer) through the pSHIELD Network. The Control Center is a remote device (a personal computer, tablet or mobile phone) equipped with a web browser, able to visualize data and act upon it.

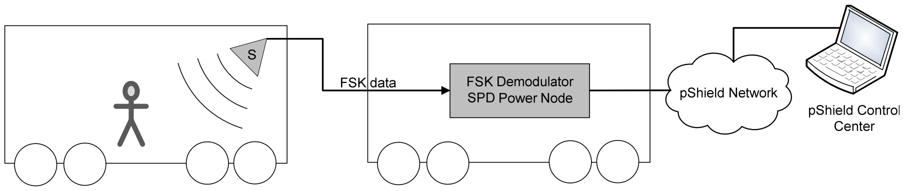

Fig. 2. Power Node demonstrator context

Figure 2 presents the demonstrator context: the SPD Power Node is located in a central car of the freight train. It receives the FSK modulated and encrypted data from other cars and delivers the plain information to the Control Center through the pSHIELD network. In our demonstrator, however, we have used a single sensor with two distinct carriers emulating sensor redundancy.

Based on the pSHIELD architecture framework (Fig. 1) and the demonstrator context (Fig. 2), a system has been developed, as presented in Figure 3. It consists of two different devices: the Intrusion detector and the FSK Demodulator SPD Power Node. The first one receives the data from an intrusion data generator and is connected to a push button, which makes it possible to request it to switch between the two carriers that are used for the FSK modulation. This system then sends the encrypted and FSK modulated data to the second system, the FSK Demodulator SPD Power Node. This system is also connected to a push button, which allows an injection of an internal fault into the node. Finally, the FSK Demodulator SPD Power Node is connected through the Ethernet to the pSHIELD Network, from where a Control Center can receive data and control this node.

The Intrusion detector is implemented on an EP3C120F780 Cyclone III Altera FPGA board. It is composed of three basic blocks corresponding to:

- a proximity sensor, consisting of an intrusion data generator which is based on a data file with emulated distances to the nearest object;
- a data encryptor, encrypting the sensor data, based on a blowfish algorithm with a 64 bit length fixed key;
- an FSK modulator, consisting of a hardware module (IP Core programmed on the FPGA), and using one of the two predefined carriers: 1 kHz and 2 kHz. If the carrier is 1 kHz, then the “Space” frequency is 968 Hz and the “Mark” frequency is 1031 Hz. If the carrier is 2 kHz, the “Space” frequency is 1937 Hz and the “Mark” frequency is 2062 Hz.

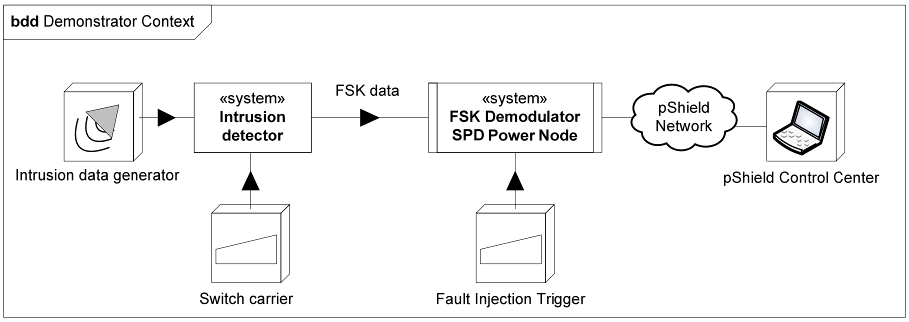

Fig. 3. Block diagram of the demonstrator context

The SPD Power Node is based on a Xilinx ML507 Evaluation Platform with a Virtex-5 FPGA. The modules composing this Power Node correspond to the pSHIELD SPD blocks depicted in Figure 1. These modules, with the exception of the Power Management, are the following:

- **Node Legacy Device Component**, which in the demonstrator is a legacy FSK demodulator module, implemented as an IP Core of a digital demodulator working with a clock of 32 kHz and demodulating 12 bits modulated data into 8 bits demodulated one.
- **Node pSHIELD Specific Component**, which is an SPD specific demodulator, providing the legacy demodulator with SPD capabilities, such as metrics and discovery. The system has several metrics values (dependability level, number of failures occurred, number of successful recoveries occurred, etc.) and it answers over the IP protocol to any discovery request incoming from the network layer. It is able to communicate the class it belongs to, the subclass specific features, the kind of demodulation, the carrier, the sampling rate and other information useful to identify the node.
- **Dependability** module, containing error detection and recovery. The system can recognize a fault condition (with a hardware based detection subsystem) and use a plausibility evaluation subsystem. If a fault is recognized, the system tries to re-

store the damaged feature by reconfiguring the appropriate part of the FPGA using for that the partial reconfiguration feature (see below, the Reconfiguration).

- **Security and Privacy** module, performing data decryption using a 64 bit fixed key blowfish algorithm. It is not the most flexible solution but it represents a very good compromise between robustness, liability and resources consumption.
- **Reconfiguration**, using the dynamic partial reconfiguration [4] of FPGA to instantiate a new demodulation core, with a different carrier frequency. The partial reconfiguration is also used for the dynamic adjustment of the system. If the modulator switches for any reason from one carrier frequency to another, the system automatically recognizes this fact and adjusts itself by reconfiguring the part of an FPGA containing demodulator logic with a new partial bitstream that implements the new required frequency demodulator.
- **pSHIELD Interface**, in this case it consists of a web server providing a web page through HTTP, with embedded XML information regarding the node identification, status, metrics, capabilities and function responses (the distance to the nearest object and alarms).
- **Fault Injector Trigger** is represented by a simple push button. When an external agent presses the button, the demodulator stops its proper operations. Then the demodulator specific component recognizes this faulty condition and triggers recovery by writing a new copy of the bitstream on the FPGA.

4 Use Case Scenarios

Several scenarios have been designed in order to demonstrate these SPD Power Node capabilities. Every scenario validates one or more innovative capabilities of the proposed node architecture, as presented in previous sections. These use case scenarios cover the demonstration of all the SPD blocks (see Fig. 1), except for the Power Management.

1. **Node Discovery and Legacy Component Integration** - This first scenario demonstrates the basic functions of the SPD Power Node and the Control Center (Fig. 2). It also demonstrates how a node can provide discovery information used for composability and how a legacy device was integrated in the SPD Power Node context: (a) The SPD Power Node runs a web server and thus provides the Control Center with a web page containing the information about the node identification, capabilities and status of the device. (b) The Control Center accesses this web page through an HTTP protocol by means of a web browser. (c) The Control Center displays the SPD Node identification, status and capabilities, including those related to the FSK Demodulator (a legacy device component).
2. **Metrics and High Performance** - The next scenario demonstrates the ability of the SPD Power Node to demodulate and decrypt the received data in real-time. (a) The intrusion detecting sensor in the first coach (Fig. 2) provides the generated data simulating a distance to an object. This data is encrypted, modulated and sent to the SPD Power Node. (b) The SPD Power Node demodulates the signal, decrypts it and stores in a local database (requires high performance). (c) Metrics data

is continuously collected and stored in a local database of the SPD Power Node. (d) The Control Center requests and displays SPD Power Node metrics, including distance to the intruding object; the information is continuously updated.

3. **Self-reconfiguration** - The SPD Power Node demonstrates its ability for self-reconfiguration to adapt to environmental changes. (a) The modulator in the intrusion detecting sensor switches to a different carrier. (b) The SPD Power Node detects a demodulation error and the demodulator is automatically reconfigured to the new carrier by a partial reconfiguration of the FPGA. (c) In the Control Center, the displayed sensor data is still valid. The metrics reveal that a self-reconfiguration has been performed. (d) The Control Center operator then may request another reconfiguration to the other carrier. The SPD Power Node reconfigures to the other configuration and then goes back to the previous one, as it does not match the carrier of the modulated signal. These switches can be noted from the changes in status and metrics readings.
4. **Dependability** - The SPD Power Node device autonomously recovers from a failure. (a) A fault is injected into the demodulator by pressing a pushbutton of a fault-injector prepared for the demonstrator. (b) An error is detected and recovered through the software and hardware (FPGA reconfiguration) recovery. (c) The correct data is still presented to the Control Center. The metrics reveal that an error has occurred and the recovery was successful.
5. **Security** - This last scenario demonstrates how encryption is used for a secure connection between the sensor devices and the SPD Power Node. (a) The encryptor in the intrusion detecting sensor switches to a different encryption key. (b) The SPD Power Node detects a decryption error. (c) The Control Center displays invalid sensor data. The metrics reveal that an error occurred.

All the scenarios have been successfully executed.

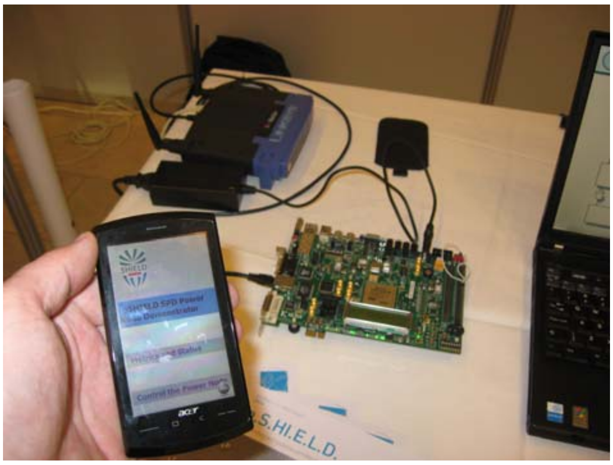

Fig. 4. pSHIELD SPD Node demonstrator

Figure 4 partially shows the demonstrator setup: the Xilinx ML507 board (the FSK Demodulator SPD Power Node), a network router and a mobile phone acting as the Control Center and presenting some data received from the SPD Node.

5 Conclusion

Security and dependability are the emerging topics in the design of embedded systems [5], and as such, they arouse both industry and researchers' interest. In this paper we presented an embedded node prototype with the integrated security, privacy and dependability (SPD) technologies which could be incorporated into an embedded network of SPD nodes, commanded by a control center.

This SPD node has been validated in an application scenario, which successfully demonstrated the legacy component integration, dependability, security, self-reconfiguration and the node-level composability.

The aim of the pSHIELD was to define an architecture framework for the development of the standardized nodes with built-in SPD capabilities, seamlessly composable in a network. The setup of an application with such nodes would be easier and faster; moreover, it would lower production costs and prolong active lifetime of developed systems. The demonstrator presented in this paper constitutes a step forward to validate the pSHIELD concept.

Acknowledgements. The authors acknowledge the support of the Critical Step project in their collaboration concerning the work presented in this paper.

References

1. ARTEMIS Joint Undertaking, the public private partnership for R&D in embedded systems, `http://www.artemis-ju.eu/`
2. pSHIELD project co-funded by the ARTEMIS Joint Undertaking (GA no.: 100204). Research of Security, Privacy and Dependability in context of Embedded Systems. `http://www.pshield.eu/`
3. pSHIELD project deliverables D2.3.2, D3.3, D5.3, accessed at `http://pshield.unik.no/wiki/PublicDeliverables`
4. Rana, V., Santambrogio, M., and Sciuto, D.: Dynamic Reconfigurability in Embedded System Design. In: IEEE International Symposium on Circuits and Systems ISCAS'2007. New Orleans (2007)
5. Schoitsch, E.: Design for Safety and Security of Complex Embedded Systems: A Unified Approach. In: Kowalik J.S., Gorski J., Sachenko A. (eds.), Cyberspace Security and Defense: Research Issues, Vol. 196 of NATO Science Series II - Mathematics, Physics and Chemistry, pp. 161-174 (2005)