ERCIM/EWICS/Cyber-physical Systems Workshop
SAFECOMP 2011, Naples, Italy, 22. September 2011

SPD Power Node ES solution in pSHIELD framework

Przemysław Osocha
e-mail: posocha.ext@sesm.it
SESM s.c.a.r.l.
Italy

João Carlos Cunha
e-mail: jcunha@isec.pt
Polytechnic Institute of Coimbra / CISUC
Portugal

Abstract

Cost reduction of embedded systems design and development is on top of ARTEMIS targets for the consolidation of European industry world leadership in embedded computing technologies. The pSHIELD consortium proposed a framework addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ES) as “built in” rather than as “add-on” functionalities, allowing a seamless composition of SPD technologies.
In this context, the pSHIELD project, co-funded by ARTEMIS-JU initiative, aims at demonstrating SPD composability by applying both existing and new SPD technologies on a SHIELD integrated system. SPD composability is supported by a layered architecture composed of four levels: node, network, middleware and overlay. For each level, the state of the art in SPD of single technologies and solutions will be improved and integrated, and enhanced with composable functionality, in order to fit in the pSHIELD architectural framework.
This paper presents the study underway regarding the definition of the node level architectural framework, and the design and construction of a SPD Node ES prototype. The demonstrator scenario consists of a FM demodulation of an encrypted signal, exhibiting node-level composability, dependability, security, self-reconfiguration and legacy component integration. The next step will be the integration of all the four layers into a full pSHIELD demonstrator.

1 Introduction

The pSHIELD project [1], co-funded by ARTEMIS JOINT UNDERTAKING initiative [2], aims at being a pioneer investigation addressing Security, Privacy and Dependability (SPD) in the context of Embedded Systems (ES) as “built in” rather than as “add-on” functionalities. Within this strategy, pSHIELD is proposing and perceiving the first step toward SPD certification for future embedded systems.

The project intends to have a great impact on the ES market regarding security, privacy and dependability, by addressing reusability of previous designed solutions, interoperability of advanced SPD technologies and the standardized SPD certifiability. To help safeguard society, pSHIELD will guarantee the privacy and security of embedded systems by making these “built in” features of future designs. Monitoring of hazardous materials being transported by train will be used to validate the results.

The goals of this project are achieved through a pSHIELD layered architecture, composed of four layers: Node, Network, Middleware and Overlay. 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 all pSHIELD architecture in a transparent but manageable way.

This paper presents the work under development towards the definition of a Secure-Private-Dependable Power Node Embedded System framework, as a part of the pSHIELD architecture. A demonstration scenario has been set-up consisting on a FM demodulation of an encrypted signal, allowing the exhibition of node-level composability, dependability, security, self-reconfiguration, and legacy component integration.

2 pSHIELD Composability

The pSHIELD multi-layered approach considers the partition of a given Embedded System into three technology-dependent horizontal layers: the node layer (meaning the hardware functionalities), the network layer (meaning the communication functionalities) and the middleware layer (meaning the software functionalities). In addition, pSHIELD considers a fourth vertical layer called Overlay which includes all inter-layer functionalities, allowing the decoupling of each horizontal layer from the others, so that the specific SPD modules/functionalities can be more easily added, removed, updated and controlled.

The main added value provided by the pSHIELD framework is the possibility to compose different SPD functionalities or components, each offering a given SPD service through an interface which can be semantically described according to the provided SPD Metrics.

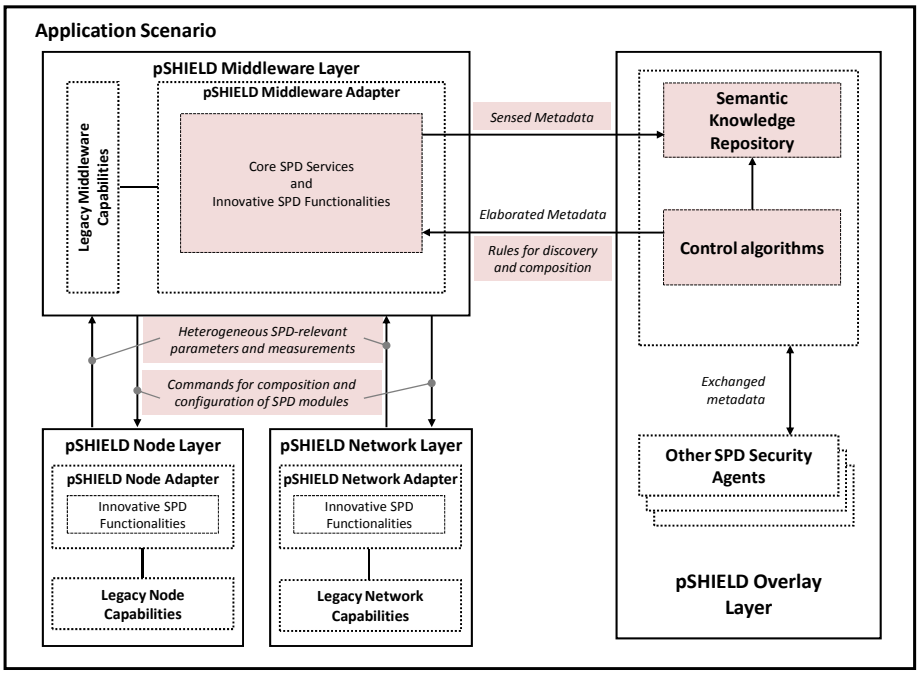

Figure 1 – pSHIELD composability functional View

Composition of SPD components entails the Sensing Functionalities needed to identify the most appropriate sensed metadata to describe the SPD components, a Control Algorithms which, on the basis of the sensed metadata, provide the rules for discovery, configuration and composition of the SPD components, and the Actuating Functionalities needed to actuate the above rules. Figure 1 highlights the key functionalities and interfaces involved in Composability.

3 pSHIELD SPD Node

A pSHIELD Node is an embedded system device equipped with several legacy Node Capabilities and with a pSHIELD Node Adapter. A pSHIELD Node is deployed as a hardware/software platform, encompassing intrinsic, innovative SPD functionalities, providing proper services to the other pSHIELD Network and Middleware Adapters to enable the pSHIELD Composability and consequently the desired system SPD.

There are three kinds of pSHIELD Nodes deploying each different configuration of Node Layer SPD functionalities of the pSHIELD framework, and comprising different types of complexity: Nano nodes, Micro/Personal nodes and Power nodes. Nano nodes are typically small ES with limited hardware and software resources, such as wireless sensors. Micro/Personal nodes are richer in terms of hardware and software resources, network access capabilities, mobility, interfaces, sensing capabilities, etc. Power nodes offer high performance computing in one self-contained board offering data storage, networking, memory and (multi-)processing.

While the three pSHIELD Node types cover a variety of different ESDs, offering different functionalities and SPD capabilities, they share the same conceptual model, enabling the pSHIELD seamless Composability.

The formal conceptual model of a generic pSHIELD SPD Node Layer is presented in Figure 2.

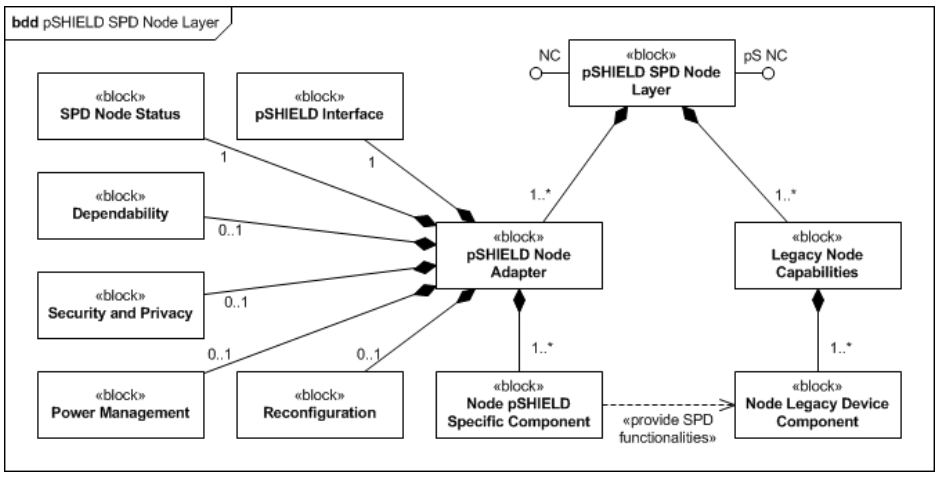

Figure 2 – pSHIELD SPD Node Layer Conceptual Architecture

3.1 Node Layer Interface

Besides providing the access to legacy, technology-dependent, Node Capabilities (NC) from third-party or of-the-shelf device components, the pSHIELD SPD Node Layer has a specific pSHIELD Node Capabilities interface (pS-NC) to the pSHIELD Network and pSHIELD Middleware Layers, allowing SPD composability, Node pSHIELD-specific functionalities, or access to legacy Node capabilities.

3.2 Legacy Capabilities

The pSHIELD SPD Node includes Legacy Node Capabilities, which consist of one or more Legacy Device Components, such as CPU, I/O Interfaces, Memory, Battery, etc. A pSHIELD Node Adapter enhance these legacy capabilities by providing, through the pS-NC interface, all the needed information to the pSHIELD Middleware adapter to enable the SPD composability of the Node layer legacy and Node pSHIELD-specific functionalities. Moreover, the pSHIELD Node Adapter translates the technology independent commands, configurations and decisions coming from the pS-NC interface into technology dependent ones and enforce them also to the legacy Node functionalities through the NC interface.

3.3 Innovative SPD

Depending on the specific implementation of the pSHIELD Node, the pSHIELD Node Adapter (see Figure 2) may include a set of components providing Innovative SPD capabilities. In brief, the main components of a generic pSHIELD Node Adapter are:

- SPD Node Status, responsible for collecting the status of each individual component, and providing SPD-relevant parameters and measurements to the Middleware Layer. It also checks on system health status for self-recovery, self-reconfiguration and self-adaptation.
- Reconfiguration, which performs module or system reconfiguration by demand of the system SPD Node Status or the Middleware.
- Dependability, responsible for applying self-dependability at node layer, by detecting problems related to system health status, and starting recovery. It is also responsible for collecting checkpoints from the remaining pSHIELD Node Adapter modules, and retrieving this information during system recovery.
- Security and Privacy, enforcing system security and privacy at node level, by providing hardware or software encryption, decryption, key generation, firmware protection, etc.
- Power Management, for managing power sources, providing protection against blackouts, etc.
- Node pSHIELD Specific Components are the innovative SPD functionalities provided to each of the Node Legacy Device Components, such as status and metrics, checkpoint-recovery, etc.

Depending on the type of node, application, technology, etc. each of these modules may be implemented with different pSHIELD SPD functionalities or not implemented at all.

4 pSHIELD Power Node Demonstrator

In order to demonstrate the capabilities of the proposed pSHIELD SPD Node Layer Architecture, a case study is being implemented.

The scenario consists on the use of FM modulation to transmit data between intrusion sensors placed in different cars of a freight train, into an SPD Power Node. The sensors are equipped with a FM modulator and a data encryptor, and each transmits using different carriers. The Power Node receives the signals, demodulates them, decrypts, processes the data and sends to a control center through the pSHIELD Network.

4.1 Node Context

The use case scenario is depicted in Figure 3. It consists of the following components:

- A FM signal generator, implemented on an Altera FPGA board, containing a proximity sensor for gathering information related to intrusions, a data encryptor for encrypting the acquired data, and a FM modulator, modulating the encrypted data into a FM signal.
- A parallel 8 bit wide data bus with the synchronization clock line, connecting the signal generator and the SPD Node.
- A SPD Power Node, built within a Xilinx Virtex-5 FPGA development board. This node has a FM demodulator, a data decryptor, and a web server, providing control center with the node identification, metrics and received data.

- A fault-injector, activated by a pushbutton, able to inject a fault into this FPGA
- A Control Center, which is a PC or mobile device, with a web browser, emulating the upper levels of the pSHIELD layered architecture.
- An Internet link between the SPD Node and the Control Center.

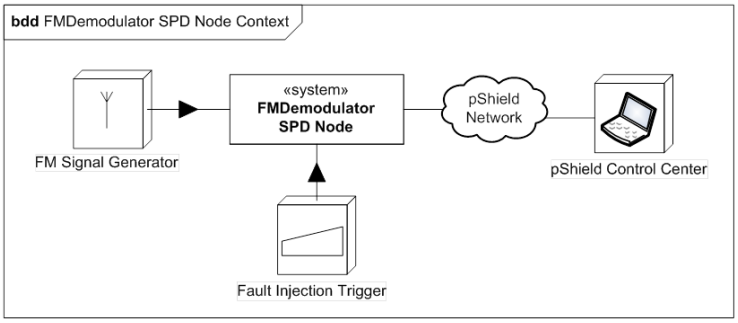

Figure 3 – FM Demodulator demonstration context

It is worth mentioning that the choice of this board for the SPD Node was, besides its capabilities for prototype designing, the fact that is supports dynamic partial reconfiguration [3]. This functionality is used to reprogram the demodulator, running in the FPGA.

4.2 SPD Node Capabilities

The SPD pSHIELD Node capabilities that will be demonstrated through this use-case scenario are basically the following:

- Dependability, by detecting errors in the demodulator, and tolerating them, through FPGA partial reconfiguration. After a fault being injected in the FPGA, affecting the demodulator, an error is detected and the FPGA is partially reprogrammed.
- Security, by receiving encrypted data and being able to decrypt it.
- Self-Reconfiguration, by detecting when a different carrier is being used in the FM signal, and reconfiguring the FPGA for adapting to a new carrier. This situation is forced by switching in run-time the carrier that is being used by the modulator to produce the FM signal.
- Metrics, by collecting and providing data such as the number of messages received, errors detected, etc.
- Composability, by providing discovery and composability information, such as the identification of the modules and its characteristics, that build-up the SPD Node.
- High performance, by demodulating and decrypting in real-time all the received data
- Legacy component integration in pSHIELD, by providing SPD functionalities to a legacy FM Demodulator, such as the collection of Metrics and the provision of composability information.

4.3 Metrics

The metrics collected and provided by the SPD node allows the overlay to decide on system composition. The following metrics are expected to be collected:

- SPD Node identification and status
- FM signal generators identification and status
- Demodulator identification and status, including carrier frequency
- Decryptor identification and status
- Received data samples from the signal generator, with statistics:
    - Sample ID, timestamp
    - Number of valid and invalid samples
- Decryption errors (could be intrusion attempts in the connection between the FM signal generator and the SPD node)
- Demodulation errors
- Self-reconfiguration (software, partial FPGA reconfiguration, or full FPGA reconfiguration)
- Error recovery (software, partial FPGA reconfiguration, or full FPGA reconfiguration)

5 Conclusions

This paper presented the first insight into the pSHIELD SPD Node Layer framework, developed in the context of the pSHIELD project. A SPD Node Layer Conceptual Architecture has been presented and discussed. A Power Node has been implemented according to this architecture, being able to demonstrate node-level composability, dependability, security, self-reconfiguration and legacy component integration.

This is an undergoing work, so further developments and results are anticipated. In particular, the integration with the other pSHIELD layers will result in a full pSHIELD demonstrator.

The results of this project may be the key factor in empowering next generation industrial processes and markets in Europe. As a consequence, the design of an innovative SPD-based framework will impact European competitiveness in domains as automotive, defense, health, industry and energy.

6 References

[1] pSHIELD: pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions (http://www.pshield.eu/)

[2] ARTEMIS Joint Undertaking (http://www.artemis-ju.eu/)

[3] Rana, V., Santambrogio, M., and Sciuto, D., 2007. Dynamic Reconfigurability in Embedded System Design. IEEE International Symposium on Circuits and Systems (New Orleans, LA, May 2007). ISCAS'2007.