ARTEMIS JOINT UNDERTAKING

The public private partnership for R&D in the field of Artemis

ARTEMIS

SHIELD

PILOT

WP3: SPD Node

pSHIELD Final Review, ARTEMIS JU

14 February 2012, Brussels

Supplementary Presentations

Major contributions from:

AS, ATHENA, CS, CWIN, ETH, MAS, SESM, THYIA

ARTEMIS Call 2009 – SP6100204

SESM A Finmeccanica Company

Thyia Technologies

SAPIENZA Università di Roma

Hellenic Aerospace Industry

EuroTecH The complete embedded PC solution

MOVATION

Critical software

DIBE

SELEX ELSAG A Finmeccanica Company

I.S.I. Industrial Systems Institute

MONDRAGON UNIBERTSITATEA

AnsaldoSTS A Finmeccanica Company

tecnalia Inspiring Business

CWI

Tecnologie nelle Reti e nei Sistemi T.R.S. SpA

AGENDA

- WP3 Status Overview (SESM)
- Power Supply Sources (Acorde Seguridad)
- The Controlled Randomness Protocol (ATHENA)
- Hardware and software crypto technologies (Critical Software)
- Rugged High Performance Computing Node (Eurotech)
- SPD Node Layer Conceptual Model (SESM)
- Nano and power nodes integration (Movation AS, CWIN)

WP3 Status

SESM

WP3 Status – Subject and Objectives

Subject:

- Basic components of the SPD Pervasive System
- Intelligent ES Nodes of increasing complexity:
  - nano node,
  - micro/personal node,
  - power node.

Objectives:

- Provide SPD intrinsic capabilities at node layer
- Create an Intelligent ES HW/SW Platform

WP3 Status – Tasks

- **WP 3 – SPD Node**
  - ✓ WP leader: **SESM**
- **Task 3.1 - Nano, Micro/Personal node**
  - ✓ Task leader: **THYIA**
  - ✓ Task partners: AS, CS, CWIN, MAS
- **Task 3.2 - Power node**
  - ✓ Task leader: **ETH**
  - ✓ Task partners: SESM, AS, CWIN
- **Task 3.3 - Dependable self-x and cryptographic technologies**
  - ✓ Task leader: **AS**
  - ✓ Task partners: CS, ATHENA, THYIA

WP3 Status – Deliverables

Internal

- **D3.1 - SPD node technologies prototypes**
  - ✓ Output of WP3 (Tasks: 3.1, 3.2 and 3.3)
  - ✓ **SESM**, AS, ATHENA, CS, CWIN, ETH, MAS, THYIA, (ISD)

Public

- **D3.2 - SPD nano, micro/personal node technologies prototype report**
  - ✓ Output of Tasks: 3.1
  - ✓ **THYIA**, AS, CS, CWIN, MAS, (ISD)

- **D3.3 - SPD power node technologies prototype report**
  - ✓ Output of 3.2
  - ✓ **ETH**, SESM, AS, CWIN

- **D3.4 - SPD self-x and cryptographic technologies prototype report**
  - ✓ Output of Tasks 3.3
  - ✓ **AS**, CS, ATHENA, THYIA

WP3 Status – Meetings and conferences

- **Frequent PhCs assure collaboration and information exchange**

- WP3 Phone Conferences and Meetings
  - 2010.12.14 PhC WP3
  - 2011.02.25 PhC WP3
  - 2011.03.21-22 Pre-Review & MidTerm Review Meeting in Brussels
  - 2011.04.18 PhC WP3
  - 2011.05.24 PhC WP3
  - 2011.06.21 PhC WP3
  - 2011.07.12-13 Consortium Meeting in Rome
  - 2011.09.09 PhC WP3
  - 2011.09.29-30 Pre-review and 2nd Review Meeting in Oslo
  - 2011.10.13 PhC WP3
  - 2011.12.15 PhC WP3
  - 2012.02.13-14 Pre-Review & Final Review Meeting in Brussels

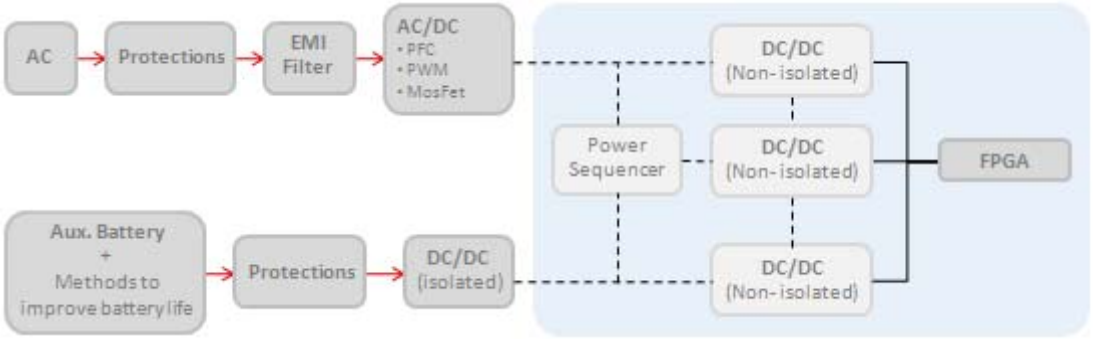
- Minutes of Meetings (MoMs) available pSHIELD Wiki and the repository

Power Supply Sources

Acorde Seguridad

Dependable power supply (AS)

- *The power supply design for an ES is one of the critical points in the design process, due to the requirements are more restrictive as time goes by.*



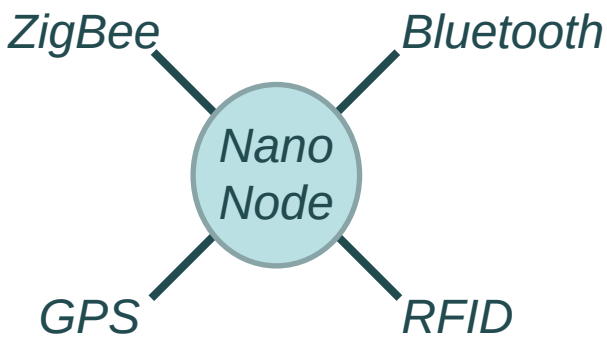
Power supply components - General design (power node)

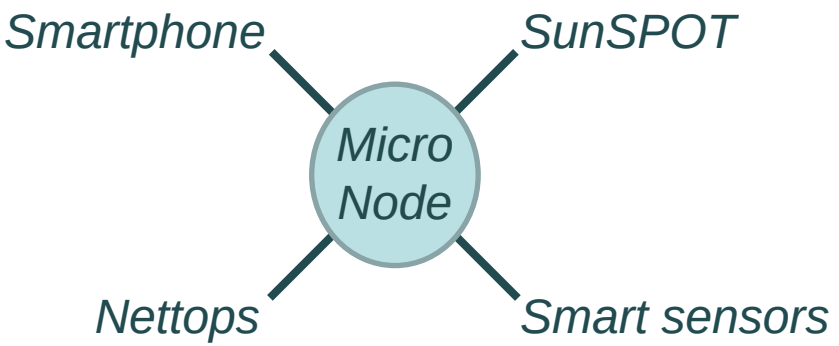
To protect the systems against external attacks, it is important to design the properly power supply protections. These will focus on three key points:

- *Study how to provide a continuous power supply source, without any cut in time or, at least, how to keep the system running during a period of time long enough to solve the problem with the main source or to send a warning to alert the person in charge.*
- *Design the appropriate protections to avoid system damages, including different operation modes to plug or unplug critical and non-critical sections of the nodes.*
- *Monitor the power consumption*

*Results are presented in **D3.1**, **D3.2, D3.3, D3.4***

Micro and Nano nodes



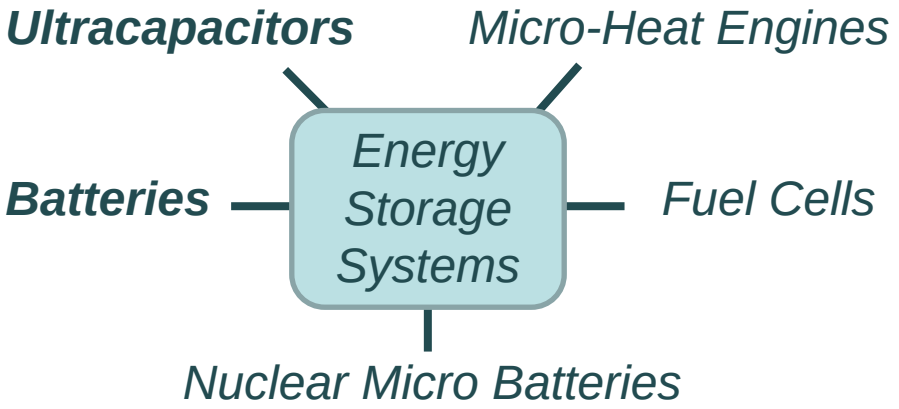


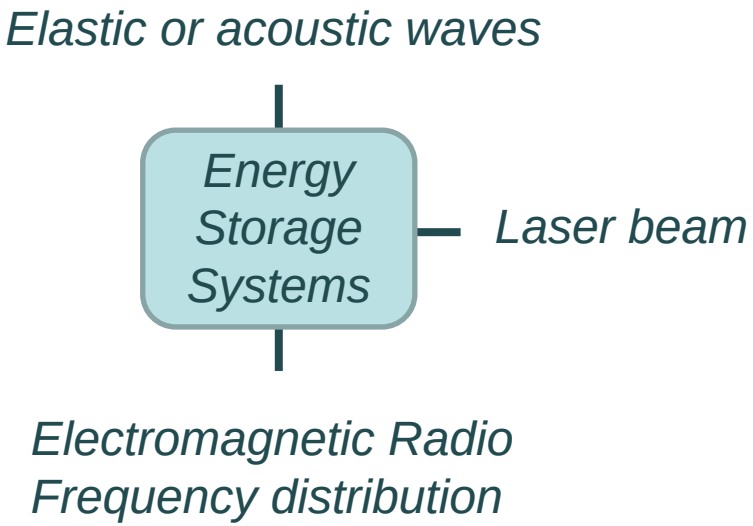
~150mW in full operating mode

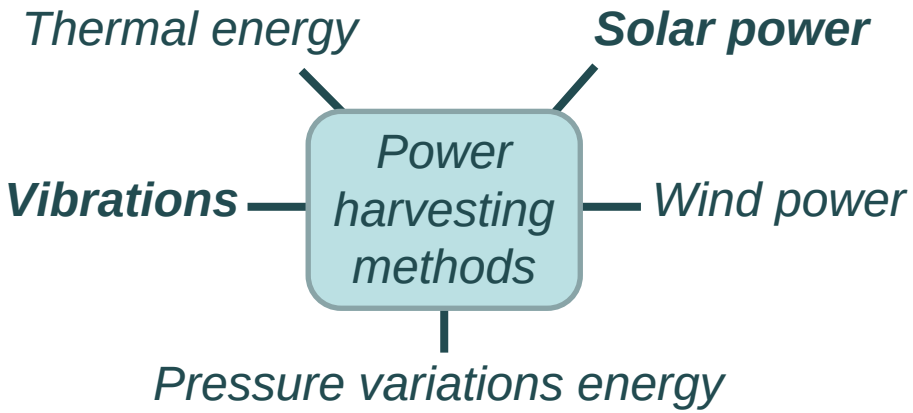
<1mW in sleep mode

Micro nodes are more complex than nano nodes so higher power consumption is expected (> 1W)

Power Supply Sources



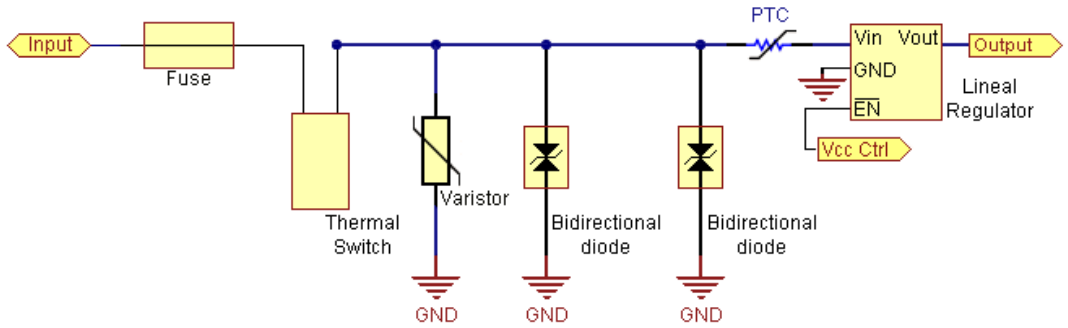




Nado Nodes: rechargeable battery combined with an ultracapacitor (hybrid battery). The ultracapacitor is useful during transmission or reception operations, where it is expected the maximum power consumption.

Micro nodes: rechargeable battery combined with a solar panel. If most of the time, these nodes are in low power consumption mode, a method based on harvesting power from vibrations could be implemented.

Power Supply Protections: Schematic (DC)



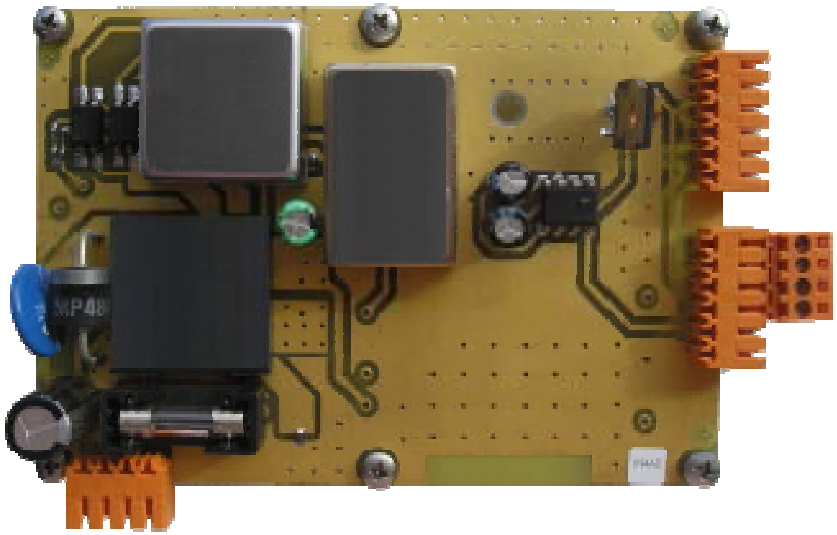
- ***Fuse****: protects against overloads or short circuits.*
- ***Thermal Switch****: opens its internal contact every time the temperature exceeded the limits*
- ***Varistor****: can absorb high transient energies and can suppress positive and negative transients.*
- ***Bidirectional Transient Voltage Suppression Diode****: provides high overvoltage protection.*
- ***Linear Regulator****: maintains a constant DC output voltage and continuously holds the output voltage at the design value.*
- ***Vcc Ctrl****: signal that lets the system plug/unplug the sub-systems connected to the output power*

Power Supply Protections: Protection circuit board (DC)

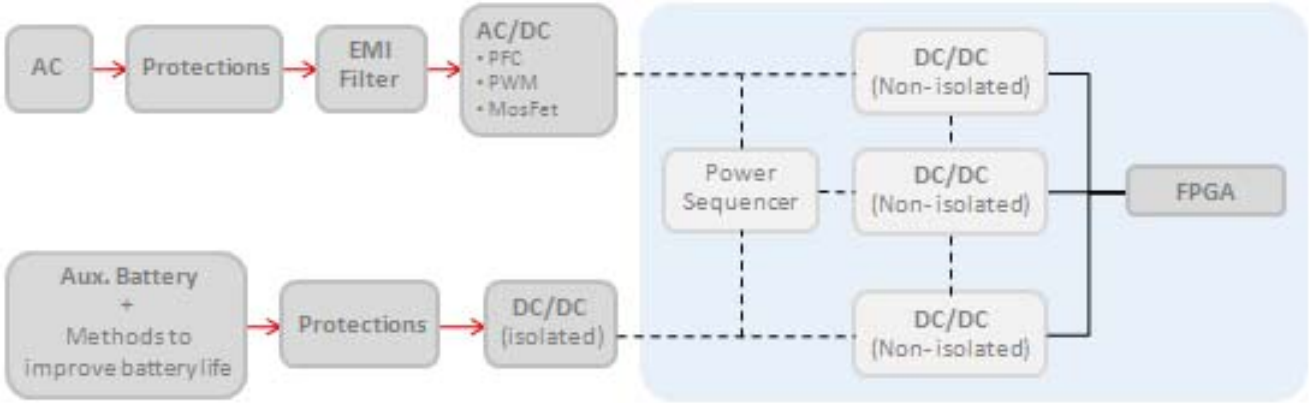
Protection board which could have up to five different sub-systems connected that can be independiently pluged/unpluged.

Includes the necessary protections to avoid damages into the circuit. To monitor power consumption, a current sense amplifier has been included.

Protection board which contains only the protections needed to avoid damages into the circuit.



Power supply components - General design (AC)



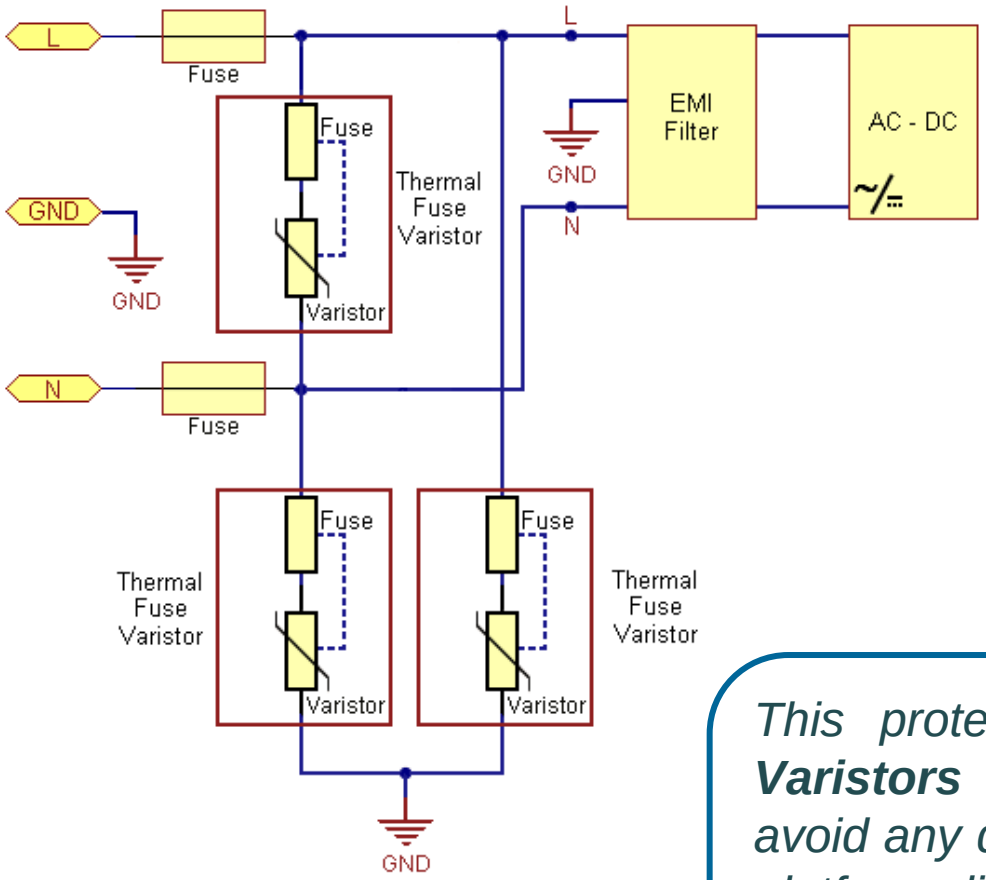
Both protection boards have been designed taking into account the normative EN/60950-1.

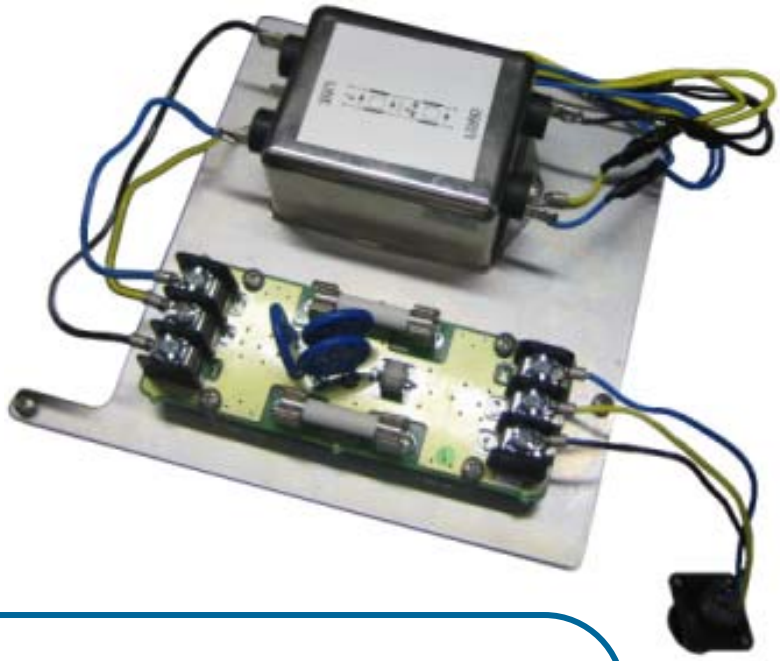
Both designs fulfil the specifications defined to achieve SPD features since they are able to protect power nodes against short circuits, overloads, over currents, over voltages and electrical noise.

The effect of parameters like leakage current, shock waves, harmonics, ESD or continuous over voltages, have been considered during test phase to check the protection boards.

EMI filter brings the electrical noise down to acceptable levels. It keeps any internally generated noise contained within the device and prevents any external AC line noise from entering the device

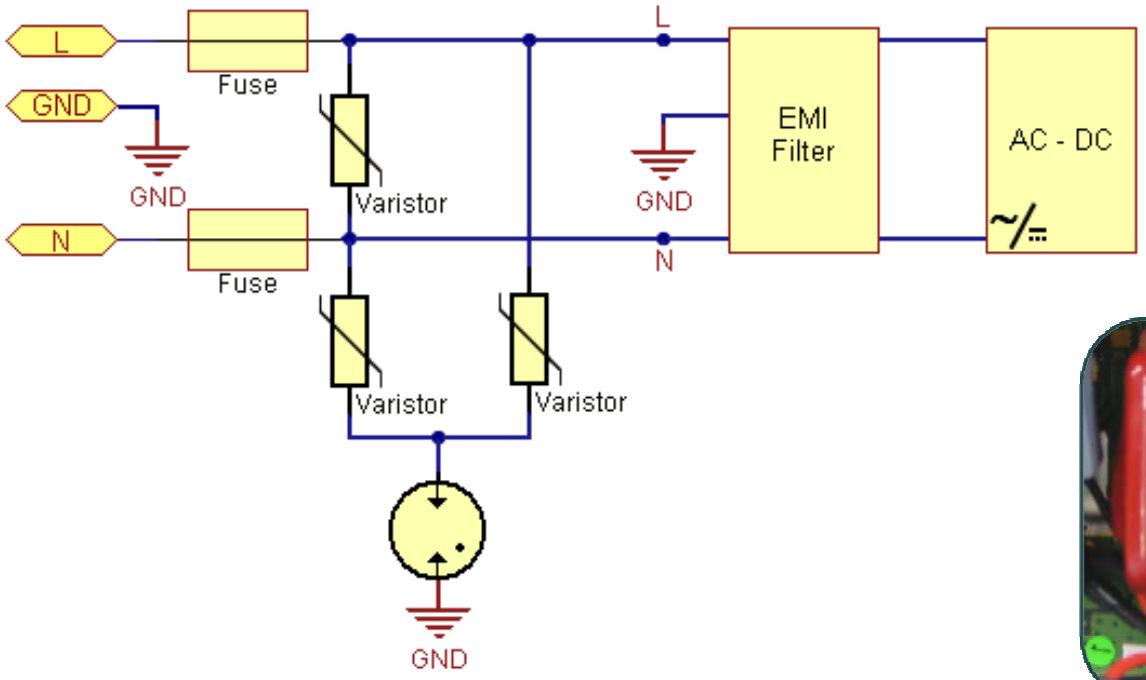
Protection Board prototype
Varistors and Gas Discharge (AC)

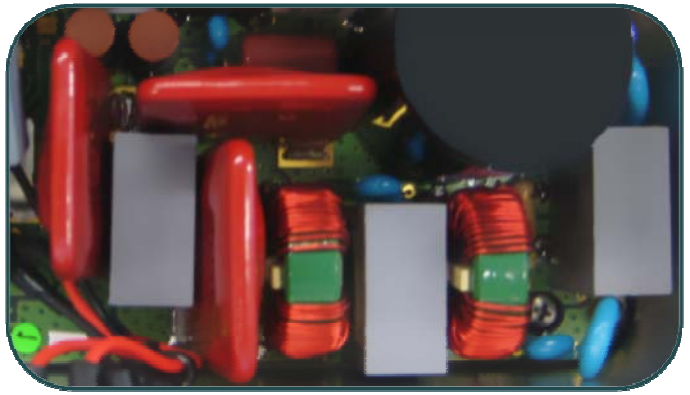




*This protection board is based on **Varistors with a Gas Discharge** to avoid any damage in the system. This platform disconnects the system from the AC power when the protection board cannot avoid damages against high voltage transients.*

Protection Board prototype
Thermal Fuse Varistors (AC)





Thermal Fuse Varistors *which protect the system against high voltage transients but, even if these devices break down, the system is able to continue working without any protection against these transients.*

AES – Hardware and Software Optimizations

SW optimizations

- ***Code adaptation***
- *Varying data type size*
- ***Function-inlining***
- *Loop Unrolling*
- ***Reducing Memory Moves***
- ***Using Pointers and eliminating Local Buffers***
- ***Using Global Variables***
- *On-the-fly-key generation*
- *MixColumns with 16-bit Memory Writes*

HW optimizations

- *Basic iterative*
- *Loop unrolling*
- *Pipelining*
- *Shared resources*

The original AES algorithm is too heavy so it can't be implemented in those platforms with limited resources.

AES – Implementation on wireless platform

Microcontroller		
Supply voltage range		1.8V to 3.6V
Power Consumption	Active Mode	330uA (2.2V@1MHz)
	Standby Mode	1.1uA
	Off Mode	0.2uA
16-bit RISC Architecture		
Frequency		8MHz
Flash		48KB
SRAM		10240B

Transceiver		
Frequency Band		387 – 464 MHz
16-bit RISC Architecture		
Frequency		8MHz
Flash		48KB
SRAM		10240B
Sensitivity		-116 dBm at 0.6kBaud
Current Consumption	TX	34mA@3.6V
	RX	17mA@3.6V
	Sleep mode	200nA

The proprietary platform has limited resources because of memory constrains so some SW optimizations were necessary to transmit protected data:

- *Reducction in stack usage*
- *Replacement of local buffers by pointers*
- *Use of global variables*
- *Code adaptation → AES-128*
- *Code modification → Memory movements reducction*

The Controlled Randomness Protocol

ATHENA

Key management in embedded systems

- The key management problem
  - Generation; distribution; storage; exchange; usage; destruction of cryptographic keys
- Control Channel
  - Public Key Cryptosystem
  - Symmetric Key Cryptosystem
- Data Channel
  - Symmetric Key Cryptosystem
- Tradeoff
  - Security vs. Resource consumption
  - Frequent vs. infrequent exchange of keys
- The Controlled Randomness Protocol (CRP)
  - Allows multiple keys to be valid simultaneously

The Protocol 1/3

- In each time frame (session)….
  - Multiple keys are valid
  - The sender chooses randomly one of them and encrypts the message
  - The receiver has the means to deduct which key has been used and decrypts the message
- CRP does not dictate how those keys are transferred
- CRP dictates how those keys are used and reused within the session

The Protocol 2/3

- Usage of Message authentication Codes
  - n encryption keys + n keys used for MAC
- Sender
  - Chooses a random index for the next set of keys (encryption / MAC)
  - Encrypts message under that encryption key
  - Produces the MAC of the resulting ciphertext using that MAC key
  - Sends the concatenation of the two results

The Protocol 3/3

- Receiver
  - Computes the MAC of the ciphertext for every possible MAC key and compares the result with the sent MAC
    - At most n MAC computations
  - Decrypts the ciphertext with the decryption key of the deducted index
    - 1 Decryption operation
- Implementation
  - AES is used as the symmetric algorithm
  - SHA-1 / SHA-256 / AES-CMAC is used as the keyed hash algorithms (MAC)

Advantages

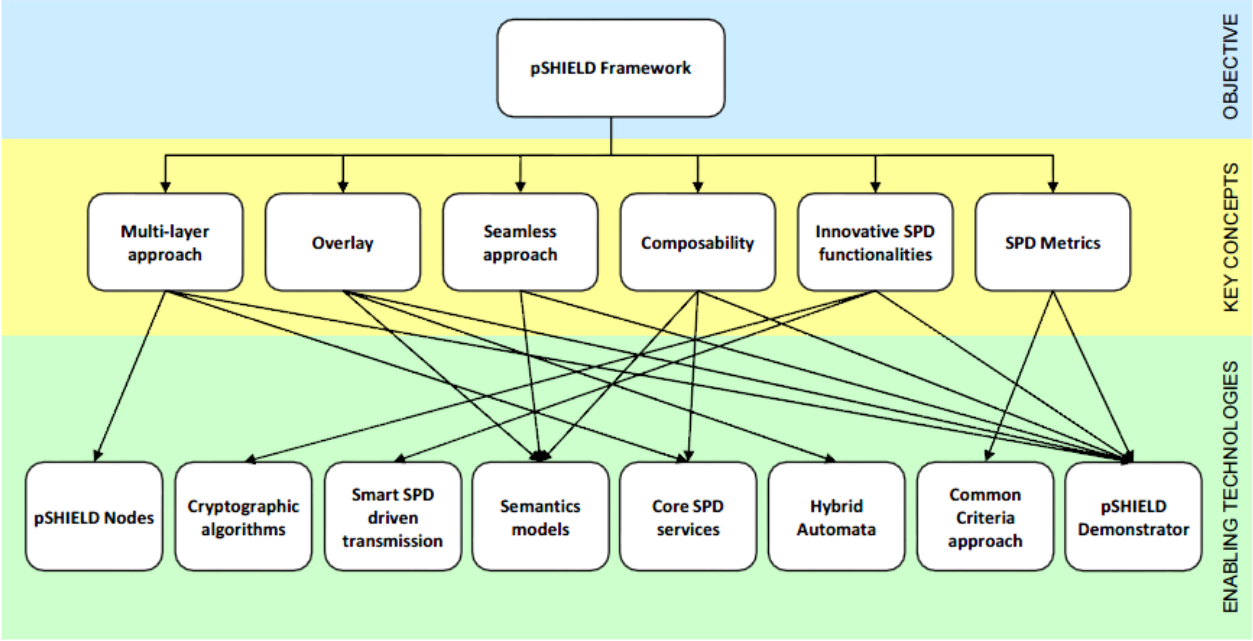
- Allows to extent the lifetime of each key well beyond the time of a conventional session
- Allows less frequent exchanges of messages in the control channel
- Complexity
  - Classical key management
    - $O(2^{2n/3})$: n = bits master key
  - Controlled Randomness
    - $O(l(2^{p}+l2^{n/2}))$: l = # of keys, p = bits MAC key
- The computational overhead can be lowered up to 1%
  - By performing the key detection operation every few packets

Hardware and software crypto technologies

Critical Software

Hardware and software crypto technologies (CS)
Cryptography for embedded devices

- Cryptography algorithms made a fundamental contribution for the provision of different systems security, inside the pSHIELD enabling technologies.



The main enabling technologies and their main relation

Results presented in **D3.1** and **D3.4**

Hardware and software crypto technologies
Cryptography for embedded devices

- Researching the state-of-the-art in the means of providing security in lightweight and networked embedded devices through an adequate cryptographic scheme

- Typical cryptographic schemes are essentially composed of a cyphering algorithm (whether symmetric or asymmetric), key management scheme and MACs (hashing functions)

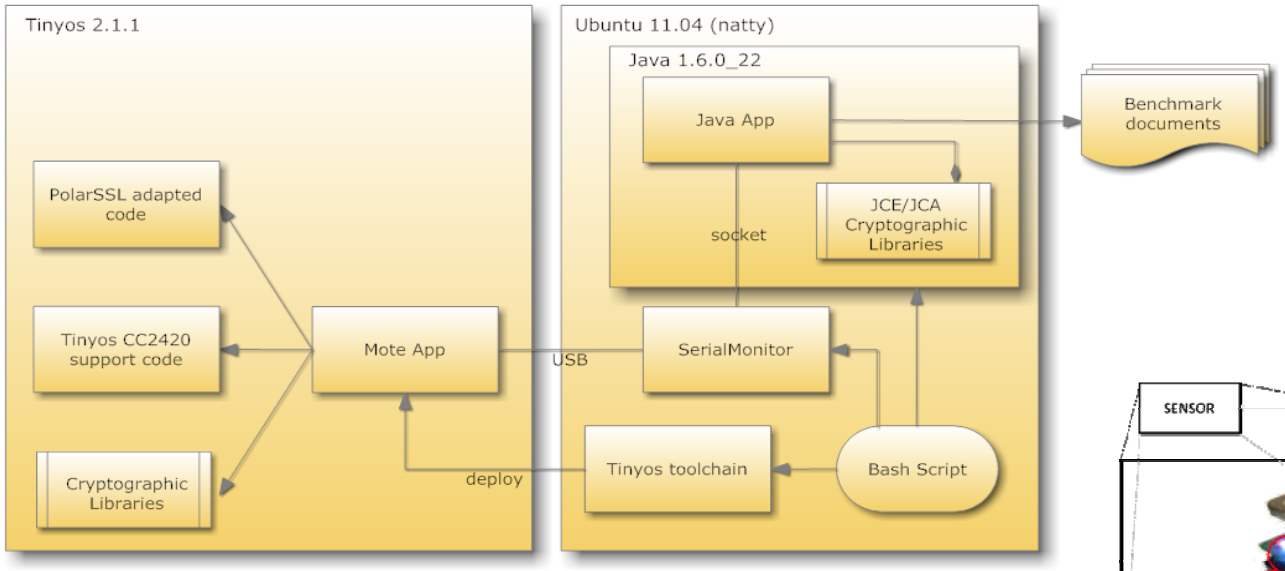
- Characteristics that may shape security schemes: resource constraints, mobility, heterogeneity, architecture, timeliness

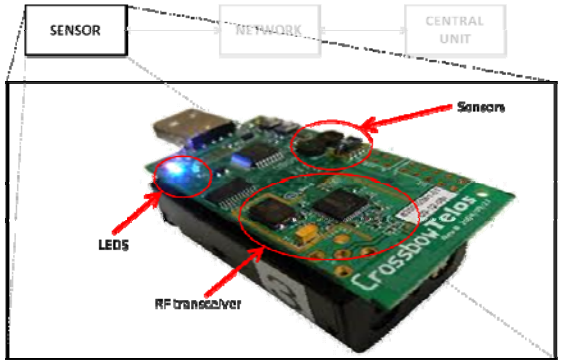
- Cryptographic schemes:
  - **WP3 - Symmetric and Asymmetric Cyphering Algorithms**
  - WP4 - Dependable key distribution mechanisms
- Asymmetric Algorithms
  - RSA, ECC and E-Gamal are the three most representative algorithms for well-known asymmetric cryptography approaches.
  - ECC emerges as a promising candidate for lightweight devices whether implemented in hardware or software, mainly due the small key size used while being able to maintain a high level of security.
- Symmetric Algorithms
  - The main reason for their continued use is the need for security in spite of constrained resources because symmetric ciphers are orders of magnitude more efficient than the asymmetric ones.
  - Analysis by international projects: Advanced Encryption Standard (AES), the European NESSIE and eSTREAM projects, and the Japanese government's CRYPTREC project

Hardware and software crypto technologies
Cryptography for embedded devices

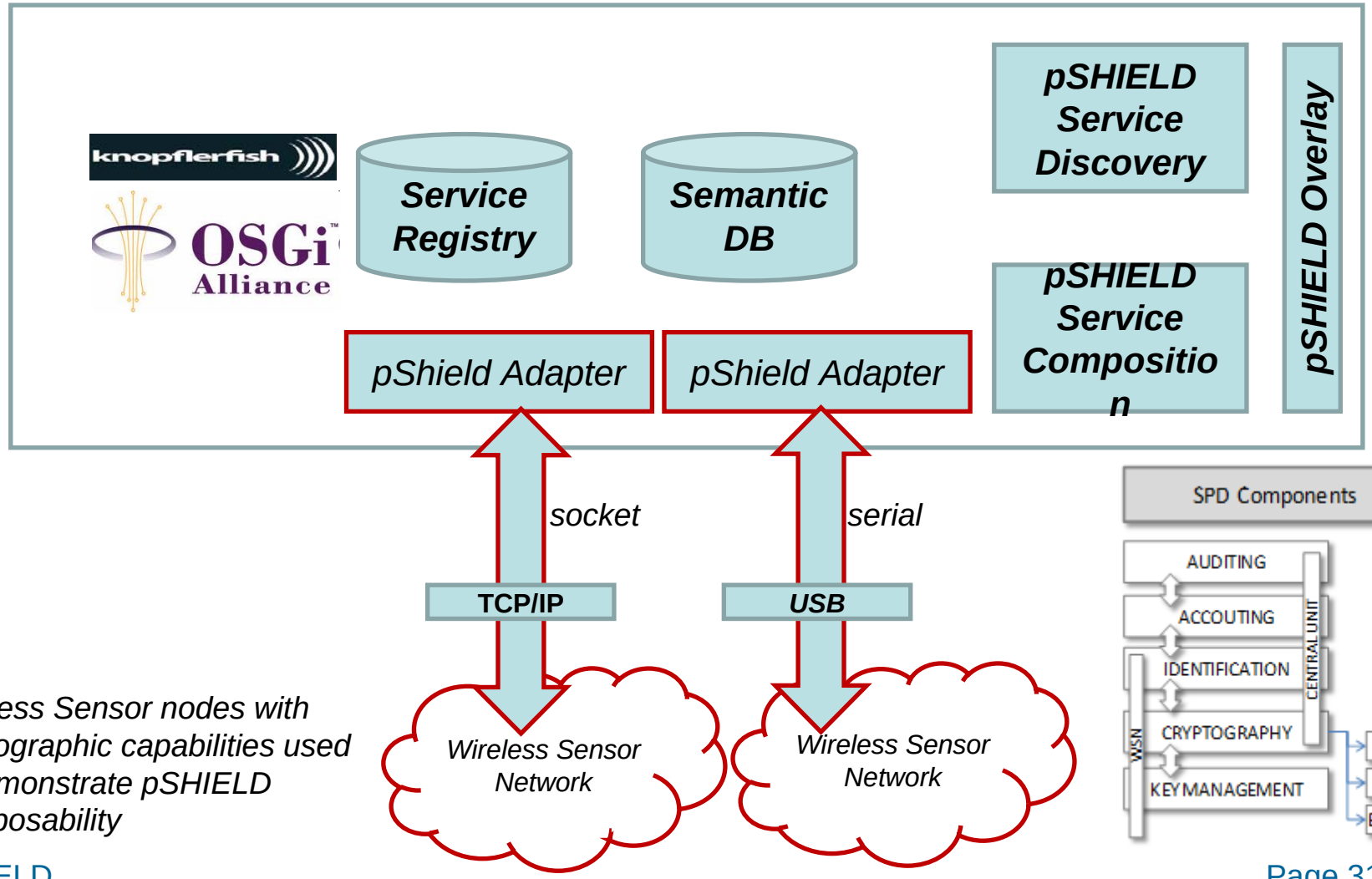
- Networked systems that include lightweight devices such as sensors require customized security schemes
- Asymmetric or symmetric cryptography cannot individually provide a complete security scheme when networked embedded systems are the target
- A hybrid security scheme is recommended where it should provide a compromise between the security sought and the constraints faced

- Test the cryptographic algorithms implementation on the hardware of a micro node (TelosB mote)





- Middleware prototype for the demonstration of **composability**



Wireless Sensor nodes with cryptographic capabilities used to demonstrate pSHIELD Composability

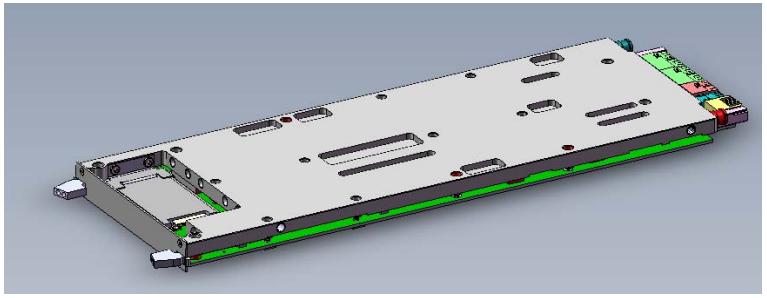
Rugged High Performance Computing Node

Eurotech

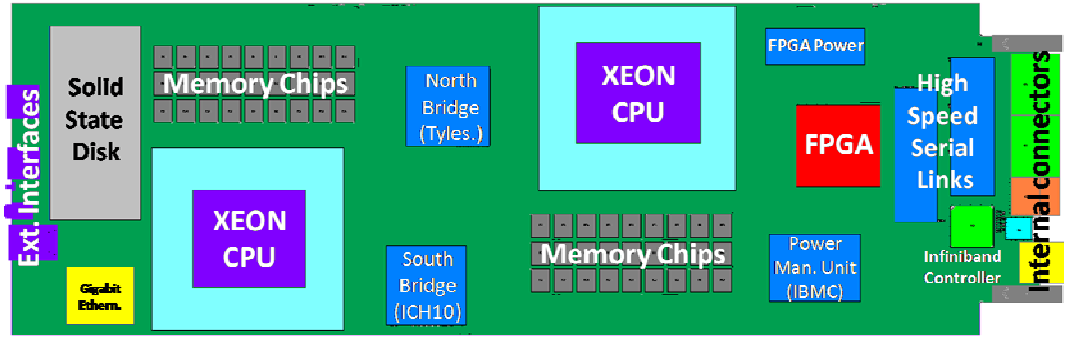
Rugged High Performance Computing Node (ETH)

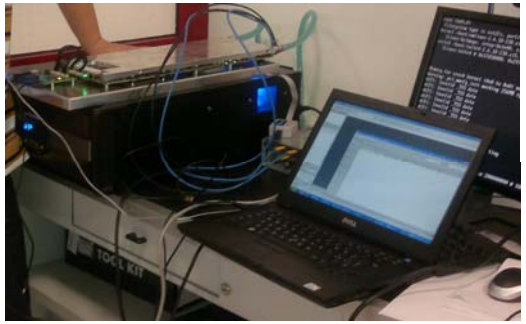
- The Power Node is a high performance embedded PC and the position of components is crucial to ensure the required performances (computing power, throughput, heat dissipation, etc.):
  - CPU positioning to maximize performance and parallelism;
  - Memory/CPU close coupling;
  - Connector positioning to ensure easy composability;
  - Distribution of components to optimize heat dissipation;
  - PCB power aware design;
  - First analysis of the cold-plate heating system.

Results described in **D2.3.1, D.3.1**, and future **D3.3**



•The Power Node is an Intel based platform with 2 Nehalem/Wesmare Xeon dual-processor.
•It is an open node of pShield and nShield platform because it contains an high speed FPGA (Altera Stratix IV) that allows the user to create its own customized hardware.





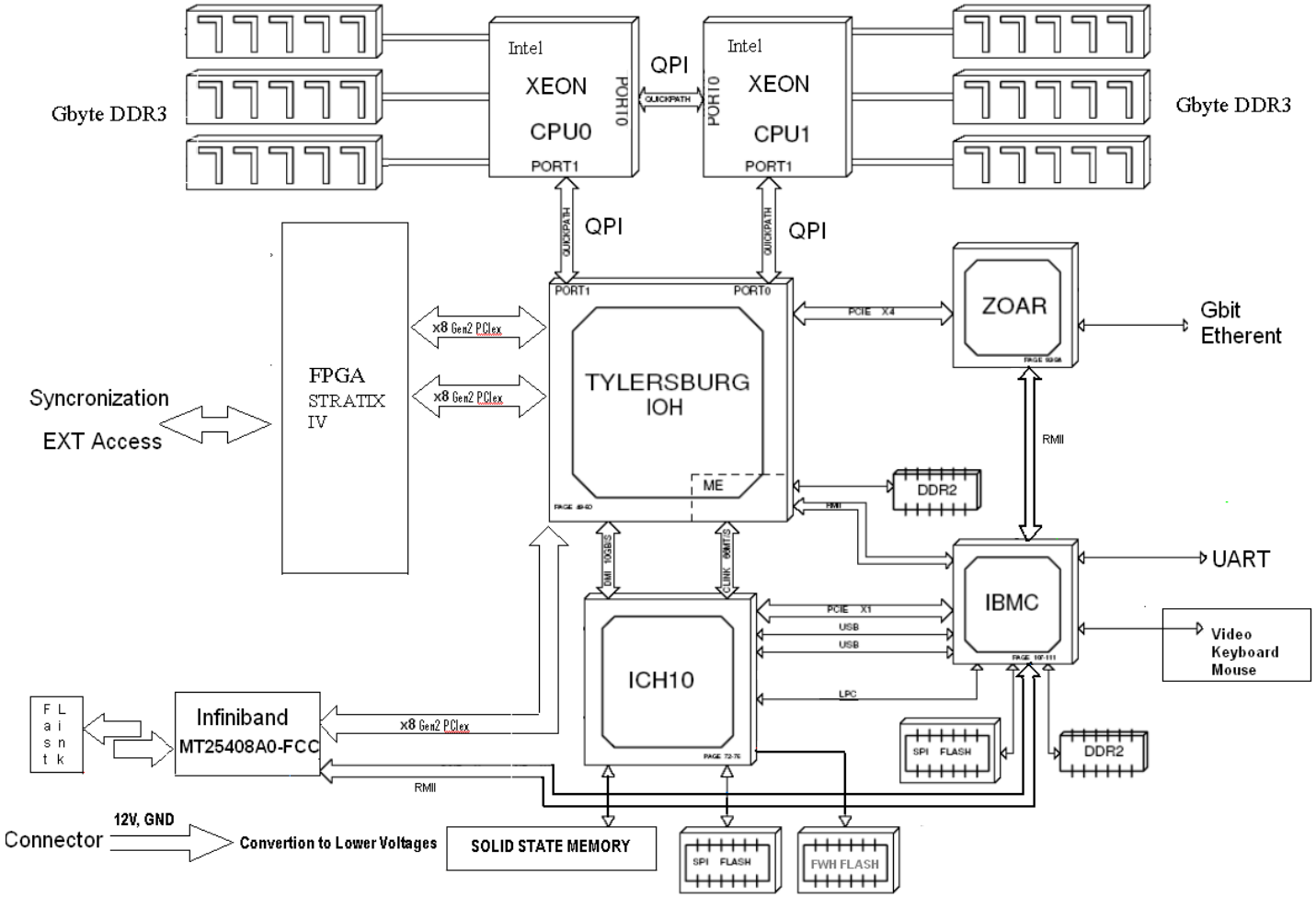
Power Node - Activities summary (ETH)

- Identification of Power Node requirements.
- Definition of Power Node system architecture.
- Board layout design.
- Software support.

Power Node – Hardware Architecture (ETH)

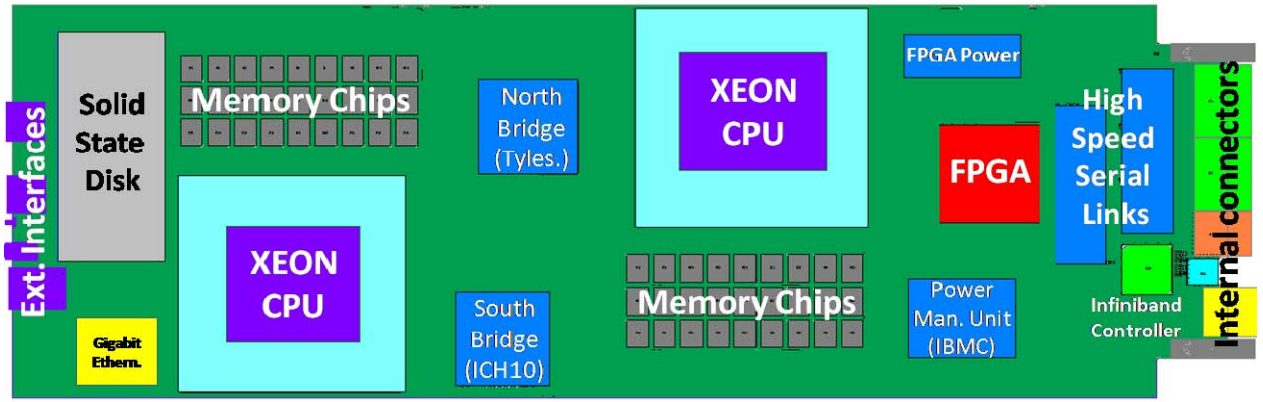
- The Power Node is an Intel based platform with 2 Nehalem/Wesmare Xeon dual-processor.
- The entire node is built around the Tylesburg chipset that represents a high performance hub for the cpus and the onboard peripherals.
- It is an open node of pShield and nShield platform because it contains an high speed FPGA (Altera Stratix IV) that allows the user to create its own customized hardware.
- Also the external interface has been designed to support an high bandwidth communications with an Infiniband chip connected through a x8 PCI 2.0 bus.

Power Node - Hardware Architecture (2) (ETH)



Power Node – Board design (ETH)

- The Power Node is a high performance embedded PC and the position of components is crucial to ensure the required performances (computing power, throughput, heat dissipation, etc.):
  - CPU positioning to maximize performance and parallelism;
  - Memory/CPU close coupling;
  - Connector positioning to ensure easy composability;
  - Distribution of components to optimize heat dissipation;
  - PCB power aware design;
  - First analysis of the cold-plate heating system.



Power Node – Software Support (ETH)

- Design and implementation of board firmware.
- Operating System selection:
  - Open source distribution, with strong preference to Linux OS (Red Hat, CentOs or Scientific Linux);
  - Drivers for Infiniband networking interface and for the IBMC Board Management Controller.

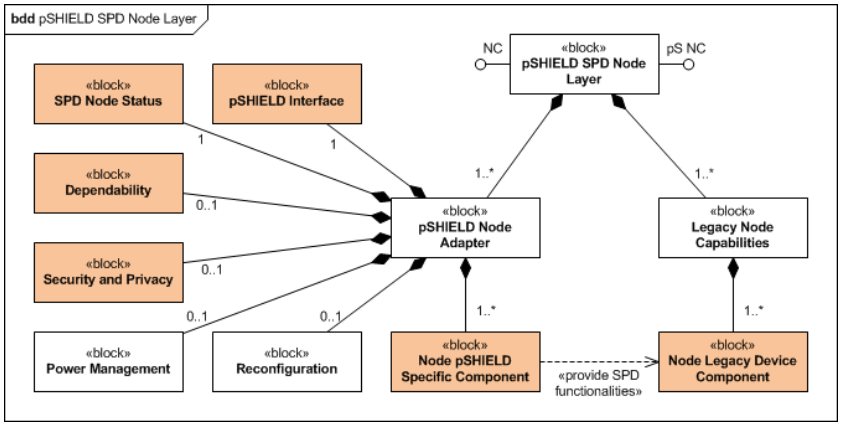
- Preliminary study of the power node SDK:
  - Compiler support (C, C++, Fortran);
  - Libraries: Scientific Computation Libraries from EPEL Repository, Intel Math Kernel Libraries, Intel Integrated Performance Primitives, Other Intel;
  - FPGA programming tools (from Altera).

SPD Node Layer Conceptual Model

SESM

pSHIELD SPD Node Layer Conceptual Model (SESM)

- Development of Node Requirements that follow TA. Results in **D2.1.1** and **D2.1.2,** chapter "Node Requirements and Specifications"
- Design of generic conceptual model of a pSHIELD node for all node types, which can be implemented in different architectures, providing different functionalities and different SPD compliance levels depending on the type of node and application field. Contributed to **D2.3.1** and **D2.3.2** (Node section).

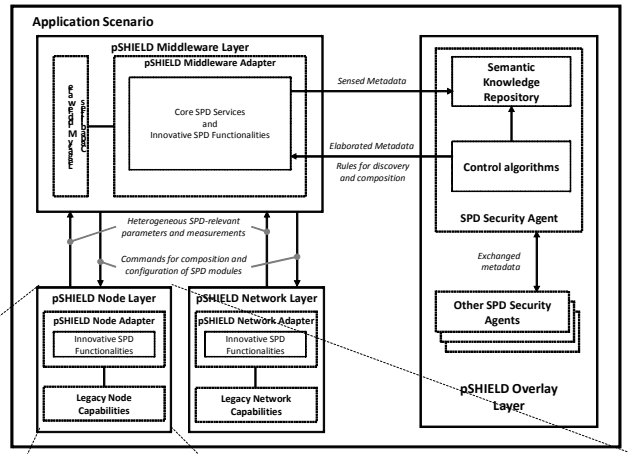


pSHIELD SPD Node Layer Conceptual Model

Running FPGA Power Node Prototype

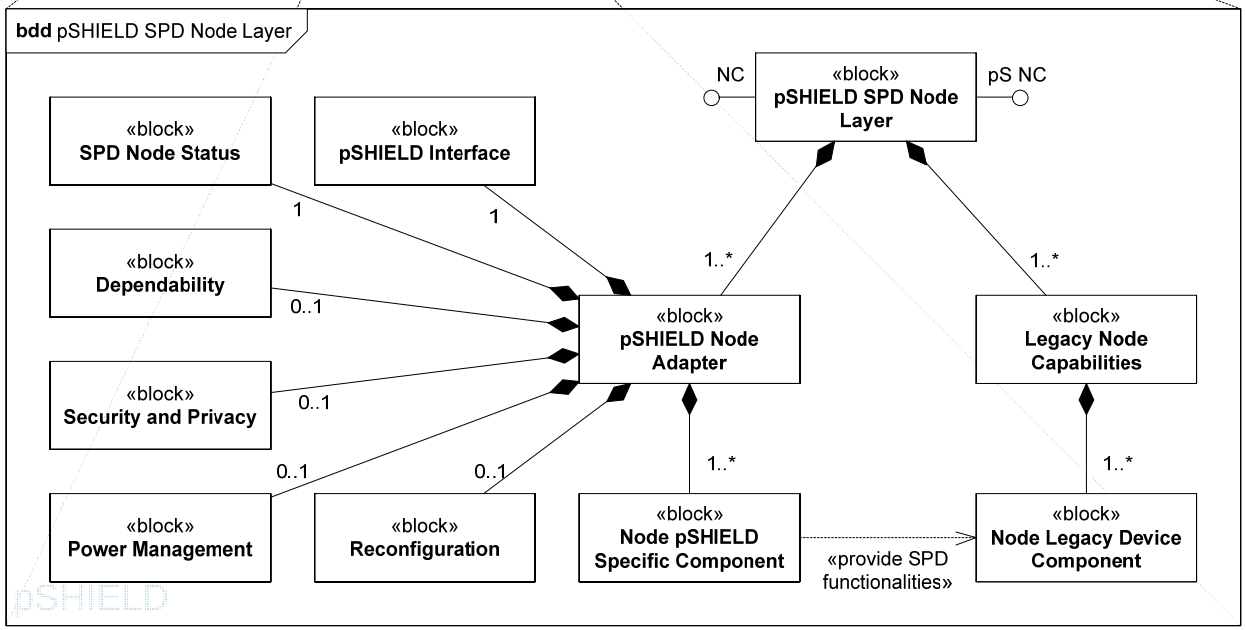
- The pSHIELD SPD FPGA Power Node prototype was developed. Results in **D3.1** and **D3.3**.
- Results of platform and demonstrator development, together with real world requirements are presented in **D6.1**, **D6.3** and **D6.4**.

pSHIELD SPD Node Layer Conceptual Model



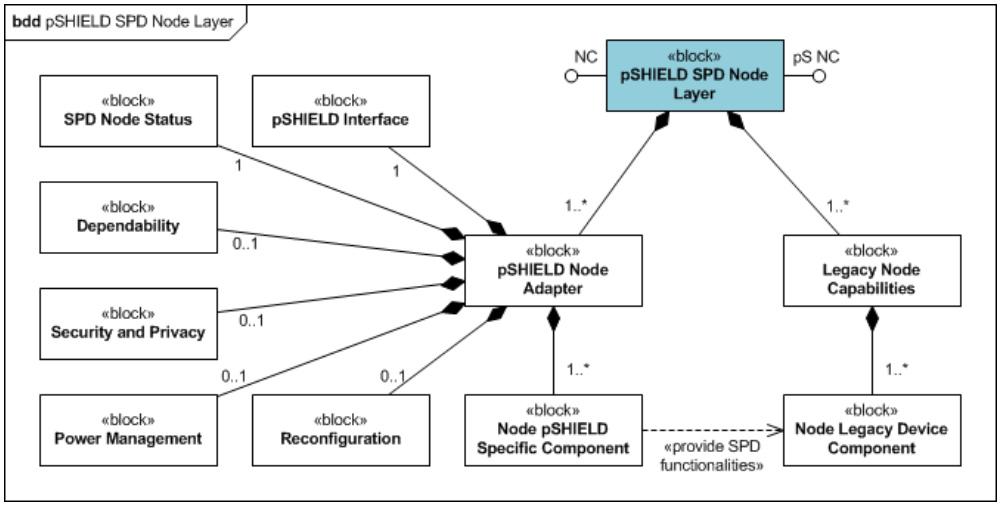
pSHIELD SPD Functional Component Architecture

and exploding:



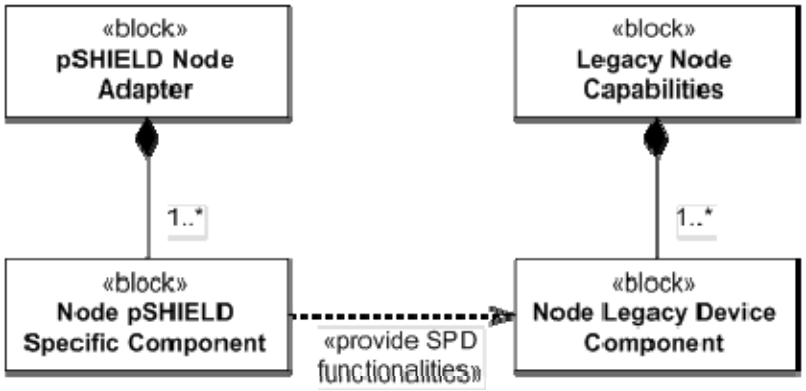
pSHIELD SPD Node Layer Conceptual Model

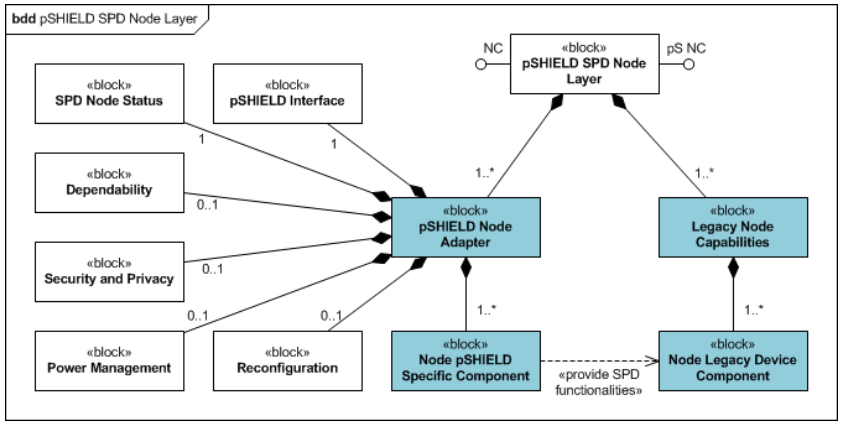
pSHIELD SPD Node Layer: Interfaces



- **pS-NC** - pSHIELD Node Capabilities interface with the Middleware Layer:
  - To enable the SPD composability
  - To provide Node pSHIELD-specific functionalities
  - To provide access to legacy Node capabilities
- **NC** - legacy, technology-dependent, Node Capabilities

pSHIELD SPD Node Layer: Legacy capabilities

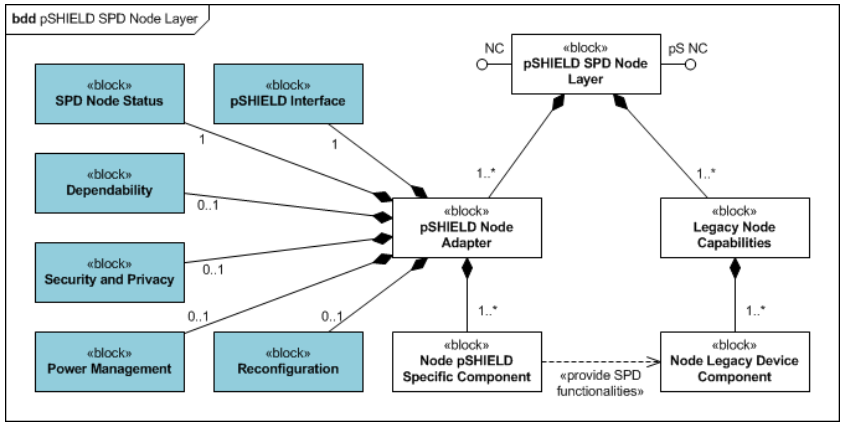




- **Legacy Node Capabilities** – consist of one or more **Legacy* Device Components**, such as CPU, I/O Interfaces, Memory, Battery, etc.
- **pSHIELD Node Adapter**, composed of **Specific Components** – the innovative SPD functionalities provided to each of the Legacy Device Components, such as status, metrics, or checkpoint-recovery

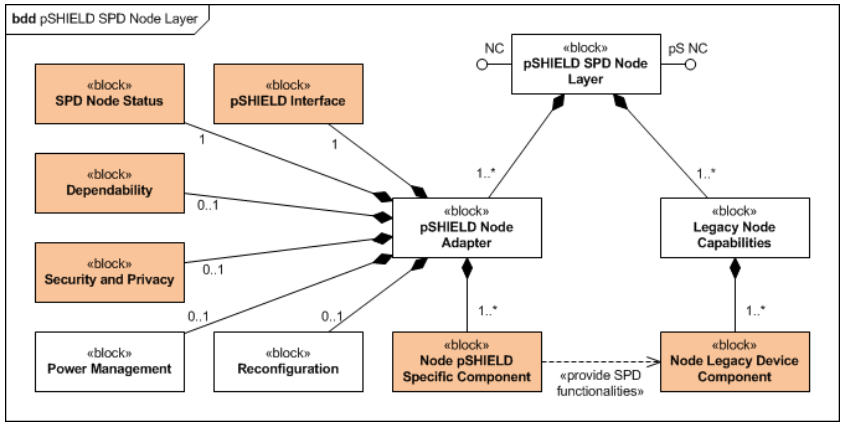
* By Legacy means any third-party or of-the-shelf device

pSHIELD SPD Node Layer: Innovative SPD



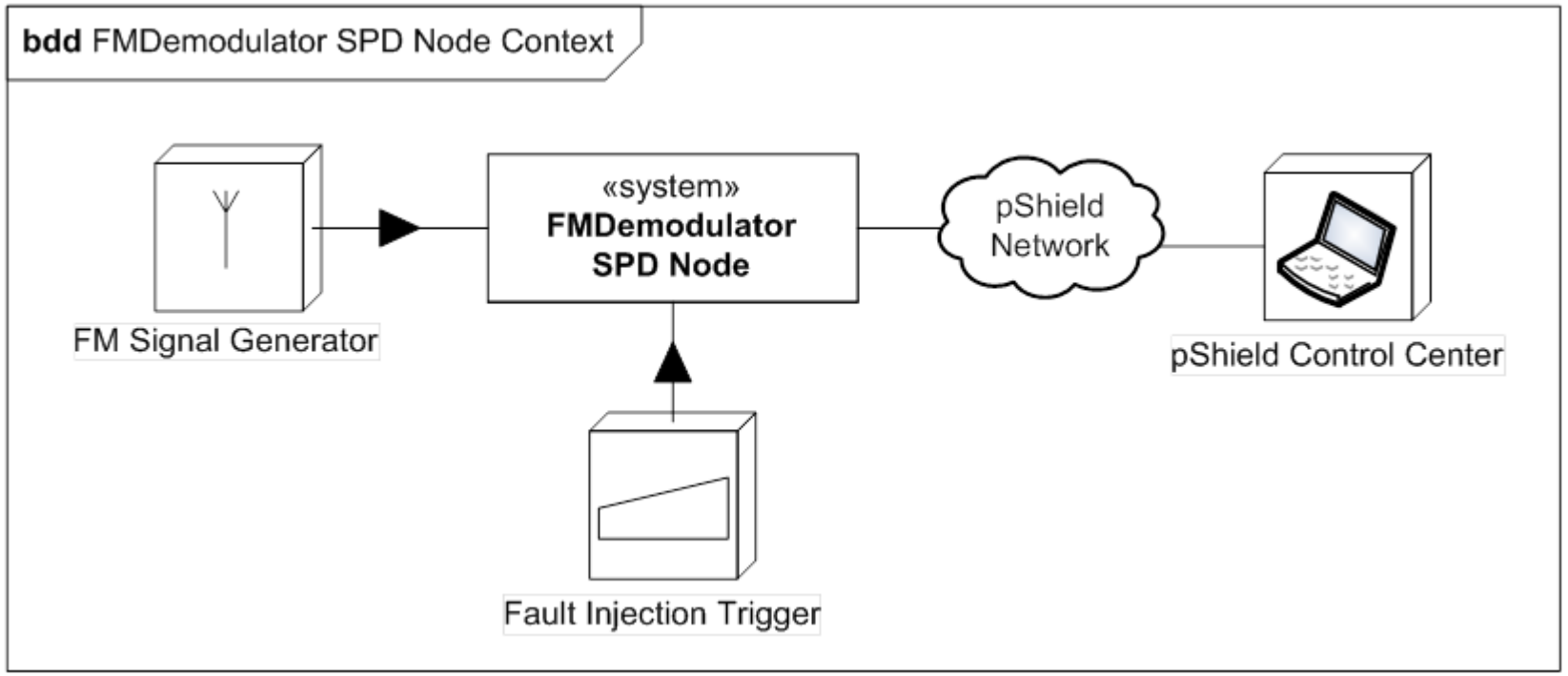
- **pSHIELD Interface** – physical interface to the pSHIELD Network.
- **SPD Node Status** – collection and disclosure of SPD-relevant parameters and measurements. Checks on system health status for self-recovery, self-reconfiguration and self-adaptation.
- **Reconfiguration** – module or system reconfiguration for recovery or new functionalities.
- **Dependability** – self-dependability at node layer: error detection and system recovery. Checkpointing service provider.
- **Security and Privacy** – hardware and software security and privacy service provider.
- **Power Management** – power sources management.

pSHIELD Power Node Demonstrator: FMDemodulator

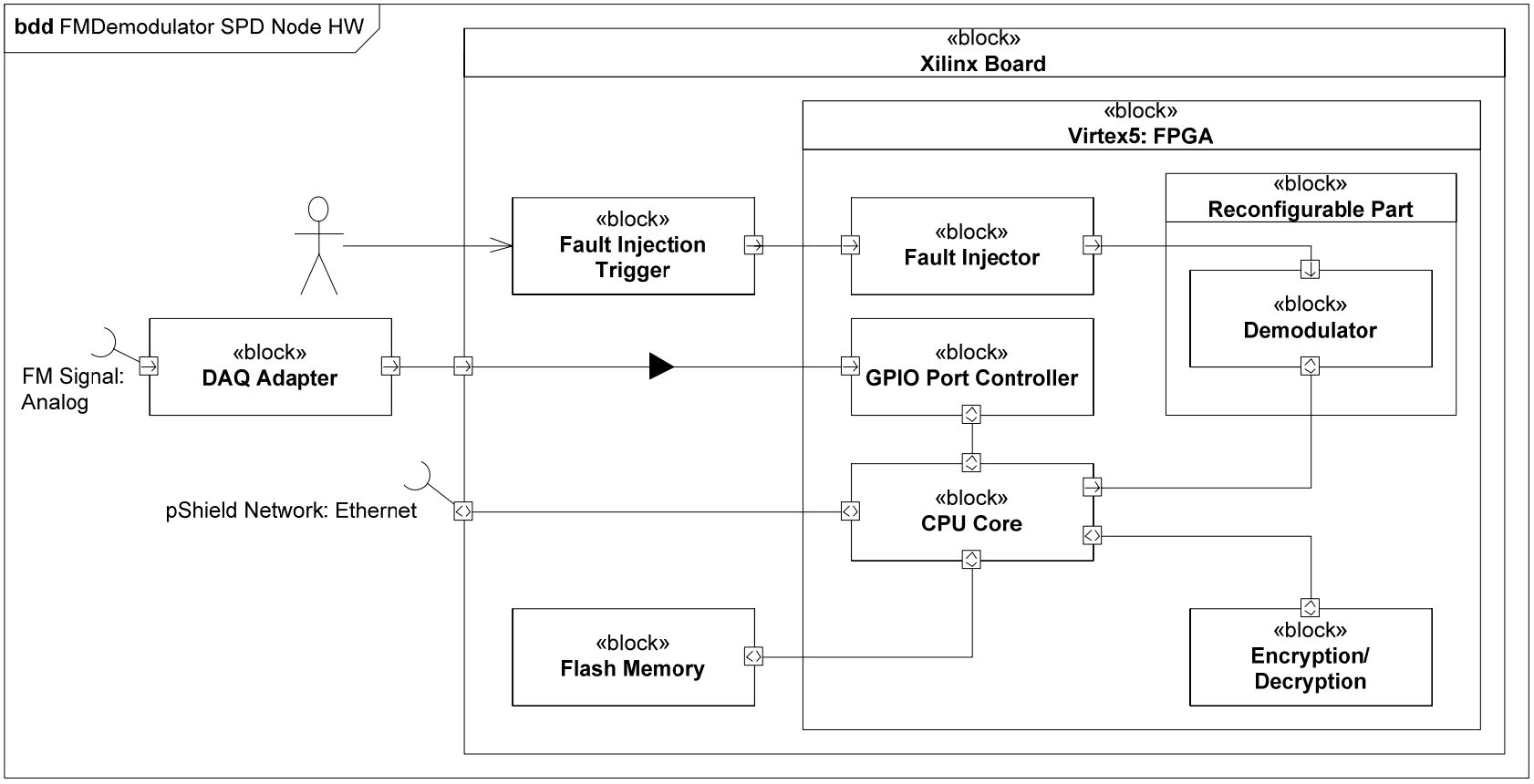


- Demonstration of:
  - Node Legacy Device with SPD functionalities:
    - pS-NC interface
    - SPD metrics
    - Self-recovery from hardware transient faults (through fault-injection)
    - Auto-reconfiguration
    - Data encryption
  - Provision of security and privacy services – hardware data encryption/decryption
- Node function
  - Dependable, secure and reconfigurable FM Demodulation

FMDemodulator: Node Context



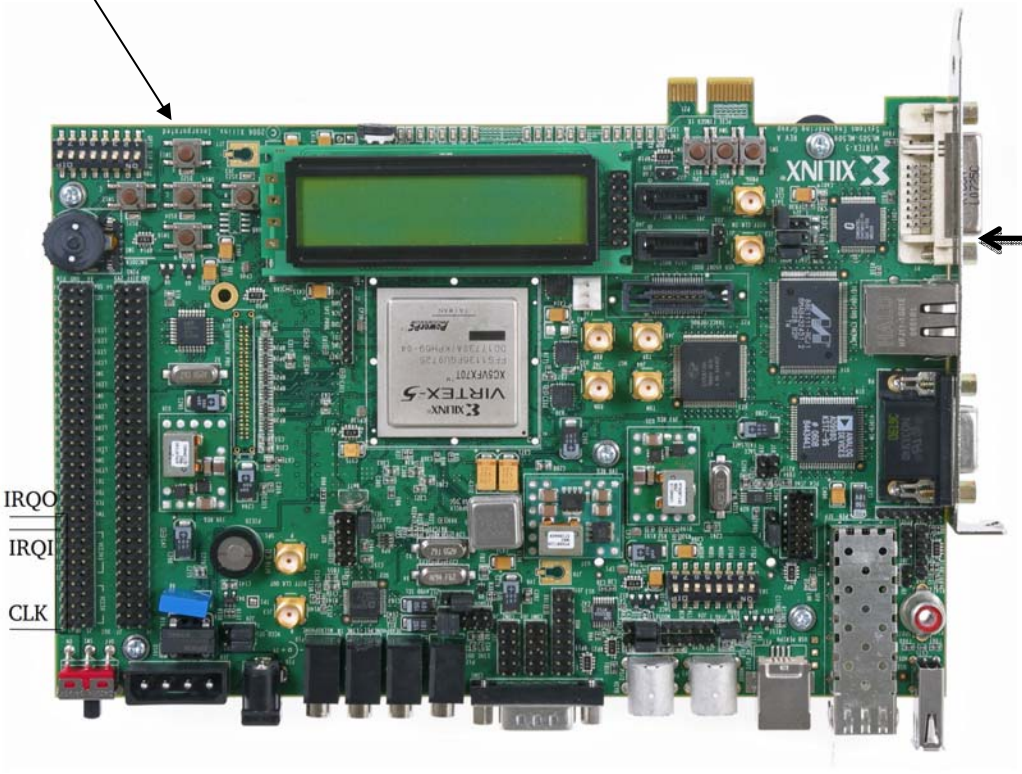
FMDemodulator: Hardware



FMDemodulator: Hardware

Fault injection trigger

Xilinx ML507 evaluation board

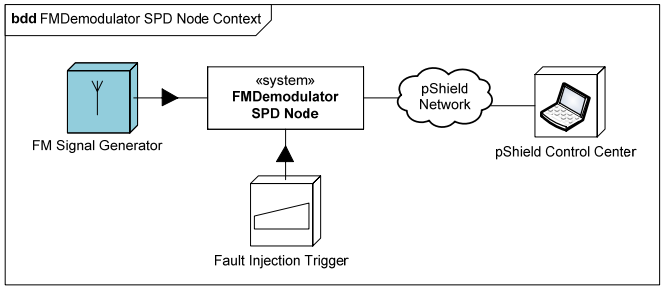


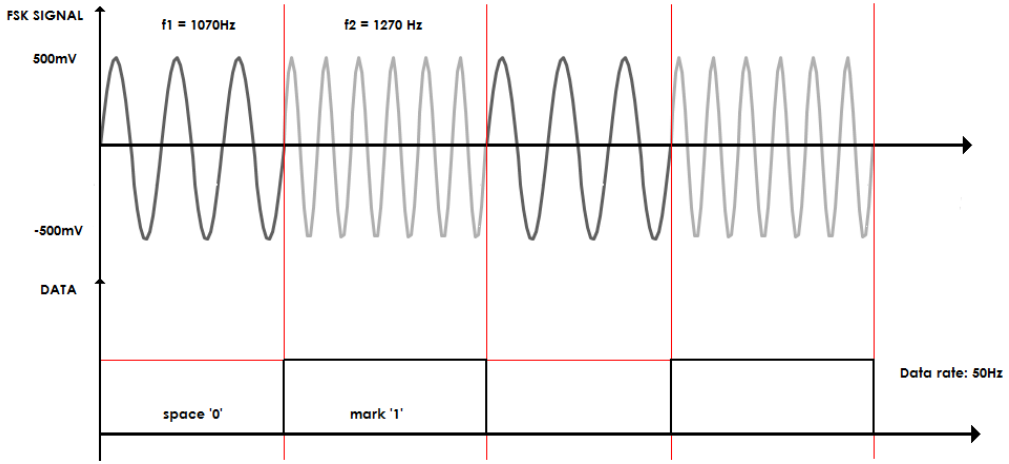
Ethernet (pShield Network)

FM signal

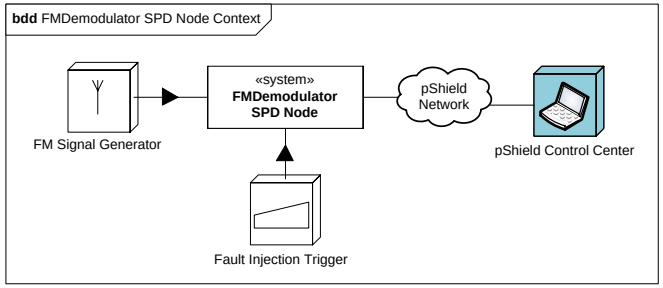
FM Signal Generator

- Implemented using specially developed board broadcasting signal.
  The signal features are contained in a wave file.
- Consists of a Audio Frequency-Shift Keying (A-FSK) modulated signal:
  - FSK Rate: 50 Hz
  - “Space” freq.: 1070 Hz
  - “Mark” freq.: 1270 Hz
  - Amplitude: 1 Vpp



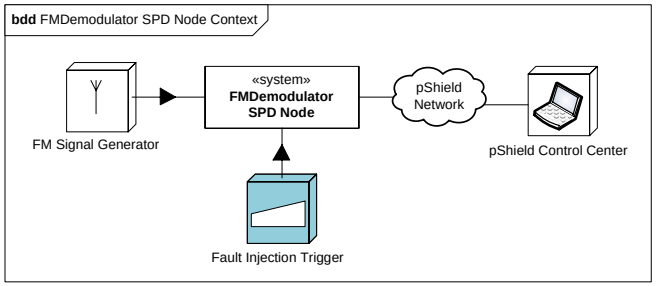


pSHIELD Control Center



- A remote PC, connected to the pSHIELD network via ethernet.
- A server/client application running on the PC allows a remote user to:
  - receive and store the data samples sent by FMDemodulator;
  - receive and analyze the metrics of the system
  - send the commands (reconfigure/recover) to the system

Fault Injector

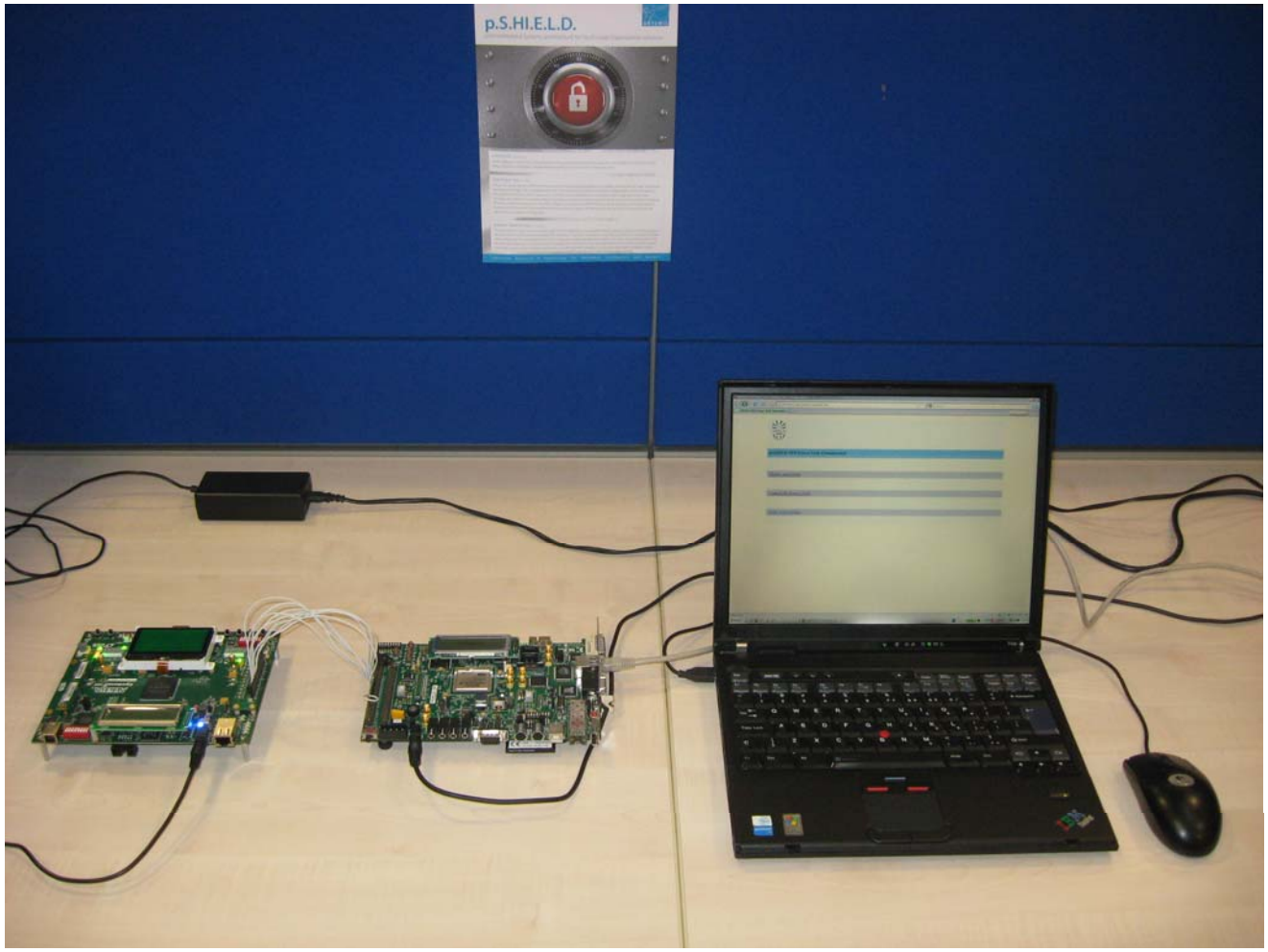


- The Fault Injector emulates a hardware fault, by changing a register cell that corresponds to a parameter of the processing algorithm.
- The result of the fault should be a fatal error of the FM Demodulation application.
- The fault is triggered by pushing a button.

FMDemodulator Metrics

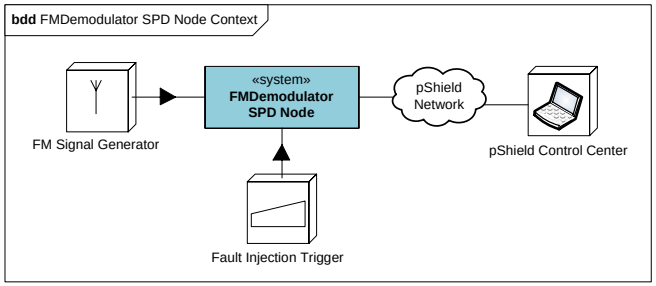
Device:	*SESM pSHIELD SPD Power Node Demodulator*
Function	
Name:	*FMDemodulation*
Inputs:	*Analog Audio FSK signal (Data Rate: 50 Hz; Mark:1020 Hz; Space: 1070 Hz; Amplitude: 1Vpp)*
Outputs:	*Digital demodulated signal (Data Resolution: 8 bit)*
SPD Status	
SPD Level:	*0-3(TBD)*
Status:	*Halted / Initialized / Running-full / Running-degradated / Error*
Description	
In Port:	*DAQ Adapter IN*
Out Port:	*TCP/IP Port 80*
Key Length:	64 bit
Key Length range:	32 to 448 bit
Data encrypted length	64 bit
Measurements	
Demodulated frames:	*20*
Demodulation errors:	*2*
Function recovery:	*0*
Device recovery failures:	*1*
Encrypted Bytes	*1000*

FPGA Power node prototype



Running FPGA Power node prototype

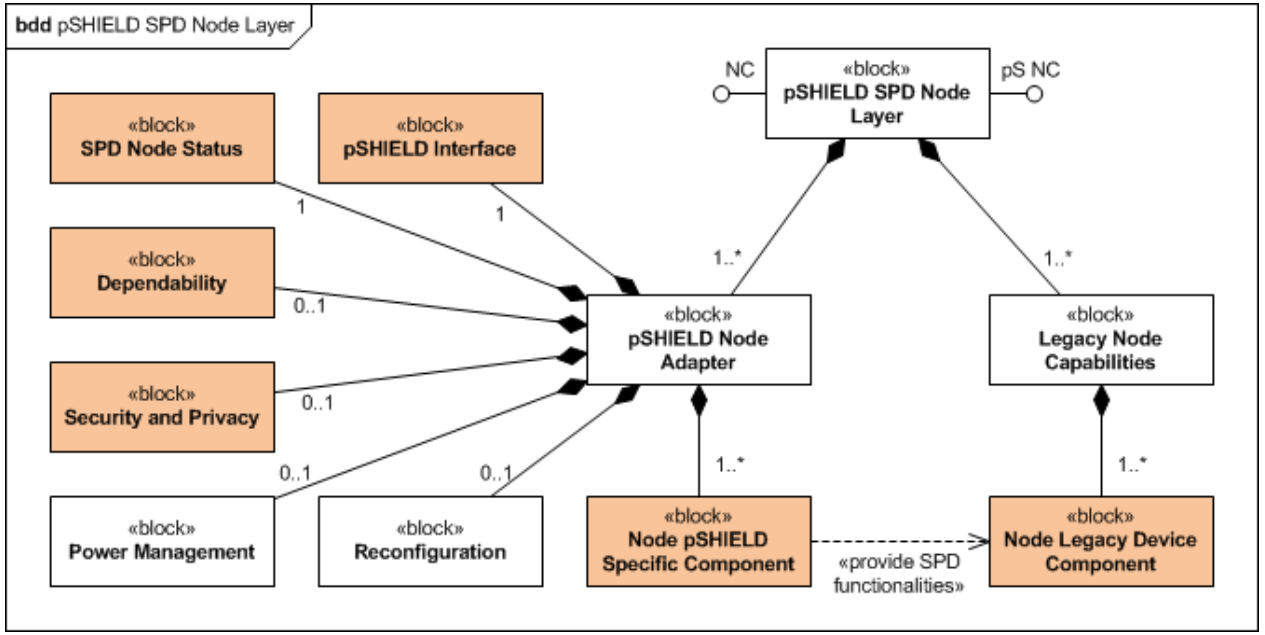
FMDemodulator SPD Node Function



- Dependable, secure and reconfigurable FM Demodulation functions:
  1. **FM signal demodulation**
     - Demodulates incoming FM Signal
     - Processes & analyzes the characteristics of the sampled signal
     - Provides all the valid samples to the pShield Network
  2. **Dependability**
     - Rejects the invalid samples
     - Recovers from device failure: FPGA reprogramming
  3. **Metrics**
     - Collects performance results
     - Collects dependability and security measurements
  4. **Security**
     - Encrypts demodulated data
  5. **Reconfiguration**
     - Self-adaptation for improved performance: FPGA partial reconfiguration (only demodulation module)

Power Node Prototype - Conclusions

- Developed Node Layer represents the base components of the pSHIELD SPD pervasive system
- Development of SPD Node Layer framework should result in standardization and certificability of future European ESs solution

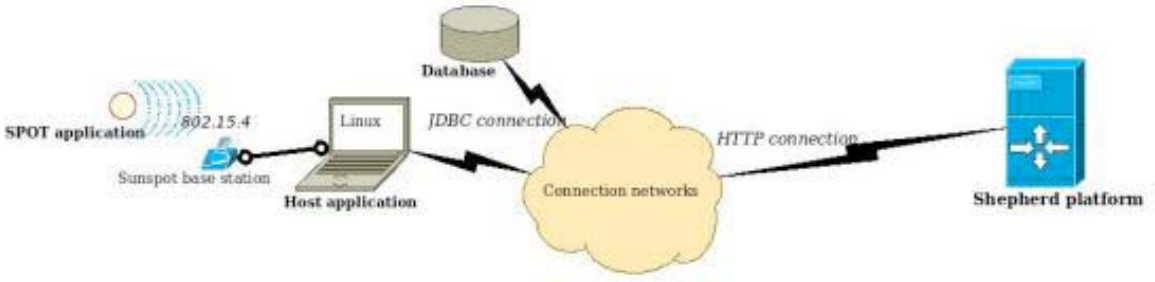


- In developed of pSHIELD SPD Node Layer Framework architecture:
  - Several blocks (filled pink in diagram) were already tested by implementation in prototype
  - Some blocks will by implemented during future works in company or by partners

Nano and power nodes integration

CWIN, Movation AS

Nano and power nodes integration (CWIN, MAS)



System overview, communication between Sun SPOT sensors and its base station, and between the ES and the Shepherd Platform.

Integration aspects of micro, power and possibly personal node with the demonstrator.

- Micro Node – Sun SPOT Sensor Platform
- Power Node – VIA Embedded Board
- *Integration with Telenor Shepherd® Platform*
- *Connectivity with Shepherd® Platform*

*Results are presented in **D3.1**, **D3.2** and **D3.3.***

ARTEMIS JOINT UNDERTAKING

The public private partnership for R&D in the field of Artemis

SHIELD

PILOT

WP3 Status

Leader : SESM

ARTEMIS Call 2009 – SP6100204

SESM A Finmeccanica Company · Thyia Technologies · Sapienza Università di Roma · Hellenic Aerospace Industry · EuroTech · Movation · Critical Software · DIBE · Selex Elsag A Finmeccanica Company · I.S.I. Industrial Systems Institute · Mondragon Unibertsitatea · AnsaldoSTS A Finmeccanica Company · tecnalia Inspiring Business · CWI · Tecnologie nelle Reti e nei Sistemi T.R.S. SpA