Project no: 269317

nSHIELD

new embedded Systems arcHItecturE for multi-Layer Dependable solutions

Instrument type: Collaborative Project, JTI-CP-ARTEMIS

Priority name: Embedded Systems

nSHIELD Acronyms document

Due date of deliverable: -

Actual submission date: M13

Start date of project: 01/09/2011 Duration: 36 months

Organisation name of lead contractor for this deliverable:

Selex ES, SES

Revision [Issue 10]

Document Authors and Approvals

Authors		Date	Signature
Name	**Company**		
Lorena de Celis	ACORDE	25/09/2012	
Elisabetta Campaiola	SES	28/09/2012	
Reviewed by			
Name	**Company**		
Approved by			
Name	**Company**		

Applicable Documents		
ID	**Document**	**Description**
[01]	TA	nSHIELD Technical Annex

Modification History		
Issue	**Date**	**Description**
Issue 1	29.02.2012	Initial version. Added D2.1 list of terms
Issue 2	31.04.2012	Added D3.1 list of terms
Issue 3	03.08.2012	Added D2.3 list of terms
Issue 4	28.09.2012	Added D2.5
Issue 5	29.09.2012	Added D2.4
Issue 6	29.09.2012	Added D5.1 list of terms
Issue 7	29.09.2012	Added D4.1 list of terms
Issue 8	25.04.2013	Added D3.2 and D3.3 list of items
Issue 9	28.06.2013	Added D1.2 list of terms
Issue 10	30.09.2013	Added D4.2 and D4.3 list of terms
Issue 11	09.10.2013	Added D6.2 list of terms

Contents

This Page is intentionally left blank

1 Introduction

This document contains all the acronyms used in nSHIELD Deliverables. As a consequence every deliverable doesn't need to have his own acronym list but has only to make reference to this global list. The reason for adopting such a strategy is that of avoiding duplication of the same definition in several documents as well as preventing misunderstanding that could derive from describing the same acronym in different ways. Furthermore this approach will be useful for maintenance purposes because the addition of a new acronym will only affect this document.

Acronym	Meaning
µC	Microcontroller
2D	Two Dimensional
3D	Three Dimensional
6LoWPAN	IPv6 over Low power Wireless Personal Area Networks
A/C	AirCraft
AAA	Authentication Authorization Accounting
AAGR	Average Annual Growth Rate
AC	Access Control
AC	Alternating Current
ACF	Auto-Correlation Function
ACL	Agent Communication Language
ACM	Association for Computing Machinery
ACM	Assurance Configuration Management
ADAS	Advanced Driver Assistance Systems
ADC	Analog to Digital Conversion
ADO	Assurance Delivery and Operation
ADR	European Agreement concerning the international carriage of Dangerous goods by Road
ADSP	Attack-tolerant Distributed Sensing Protocol
AES	Advanced Encryption Standard
AFDX	Avionics Full-Duplex Switched Ethernet
AFR	Automatic Firmware Recovery
AGD	Assurance Guidance Documents
AIFB	Institute of Applied Informatics and Formal Description Methods
AMLCD	Active-Matrix Liquid Crystal Display
AMMC	Aircraft & Mission Management Computers
ANSI	American National Standards Institute
AODV	Ad Hoc On-Demand Distance Vector Routing Protocol

APCA	ARTEMIS Project consortium Agreement
API	Application Program Interface
ARINC	Aeronautical Radio, Incorporated
ARP	Audit Automatic Response
ASAP	Advanced Service in AirPort
ASICs	Application-Specific Integrated Circuits
AT3	Agent Toll III
ATx	ARTEMIS Target x
AUML	Agent Unified Modeling Language
AVA	Assurance Vulnerability Assessment
AVANTSSAR	Automated VAlidatioN of Trust and Security of Service-oriented ARchitectures
AWT	Adaptive Weighted Threshold
BANs	Body Area Networks
BER	Bit Error Rate
BF	Beacon Falsification
BGA	Ball Grid Array
BH	Black-Hole
BPEL4SWS	Business Process Execution Language for Semantic Web Services
BPMN	Business Process Modeling Notation
BS	Base Station
BSNs	Body Sensor Networks
BSP	Board Support Package
C	Catastrophic
C&C	Command and Control
C/R	Control/Reaction
CAM	Cryptographic Attack Metrics
CAN bus	Controller Area Network bus
CBC-X	Cipher Block Chaining X
CBEFF	Common Biometric Exchange Formats Framework
CBR	Case-Based Reasoning
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosives
CC	Common Criteria
CCC	Common Control Channel
CDC	Connected Device Configuration
CDMA	Code Division Multiple Access
CE	Code Execution

CE	Central Entity
CEN	Cognitive Enabled Node
CHOP	Configuring, Healing, Organizing, Protection
CIA	Confidentiality Integrity Authenticity
CIAA	Confidentiality Integrity Authenticity Availability
CISC	Complex Instruction Set Computer
CLDC	Connected Limited Device Configuration
CMPNs	Cognitive Micro Personal Nodes
CNs	Cognitive Networks
CoAP	Constrained Application Protocol
CODEC	Coder-Decoder
CORBA	Common Object Request Broker
COTS	Commercial Off-the-Shelf
CPDF	Conditional Probability Density Function
CPLDs	Complex Programmable Logic Devices
CPSR	Current Program Status Register
CPU	Computer Processing Unit
CR	Cognitive Radio
CRC	Cyclic Redundancy Check
CRN	Cognitive Radio Network
CRP	Controlled Randomness Protocol
CSAV	Composition Security Assurance Value
CWSN	Cluster Wireless Sensor Networks
DAA	Direct Anonymous Attestation
DAC	Digital to Analog Conversion
DAS	Dependable Avionic Systems
DC	Direct Current
DCOM	Distributed Component Object Model
DDC	Digital Down-Conversion
DDC	Dependable Distributed Computation
DDoS	Distributed Denial-of-Service
DDS	Data Distribution System
DEMA	Differential ElectroMagnetic Analysis
DES	Data Encryption Standard
DF	Data Freshness
DFA	Differential Frequency Analysis

DM	Device Management
DM	Dependability metric
DM	Dynamic Metric
DMA	Direct Memory Access
DNS	Domain Name System
DODAF	Department of Defense Architecture Framework
DoS	Denial of Service
DoW	Description of Work
DPA	Differential Power Analysis
DPM	Deterministic Packet Marking
DPWS	Devices Profile for Web Services
DPWS4J	Devices Profile for Web Services for Java
DRBTS	Distributed Reputation and trust-based Beacon Trust System
DRE	Distributed Real-time and Embedded
DSP	Digital Signal Processor
DSSACF	Delta Sub-band Signals Auto-Correlation Function
DUC	Digital Up-Conversion
DWT	Discrete Wavelet Transform
E&O	Errors and Omissions
EAP	Extensible Access Protocol
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EDU	Electrical Distribution Unit
EFRS	Embedded Face Recognition System
EM	Electro Magnetic
EMC	Electro Magnetic Compatibility
EMI	ElectroMagnetic Interference
EQSW	EQuipment SoftWare
ES	Embedded System
ESD	Embedded System Device
ESs	Embedded Systems
FANS	Future Air Navigation System
FAR	False Accept Rate
FAU	Functionality AUdit
FC	Fusion Center

FCC	Federal Communications Commission
FCO	Functionality COmmunication
FCS	Functionality Cryptographic Support
FDP	Functionality user Data Protection
FEC	Front End Clippling
FERET	FacE Recognition Technology
f-ESD	Full communication capabilities Embedded System Device
FIA	Functionality Identification and Authentication
FIPS	Federal Information Processing Standards
FIQ	Fast interrupt request
FMS	Flight Management System
FMT	Functionality security ManagemenT
FP7	Seventh Framework Programme
FPGA	Field-Programmable Gate Array
FPR	Functionality PRivacy
FPT	Functionality Protection of TSF
FRP	Face Recognition Project
FRU	Functionality Resource Utilization
FRVT	Face Recognition Vendor Test
FSSD	Flexible and Secure Service Discovery
FTA	Functionality TOE Access
FTP	Functionality Trusted Path
FUA	Faults with Unauthorized Access
FW	Firewall
GA	General Assembly
GPIO	General Propose Input Output
GPP	General Purpose Processor
GPS	Global Positioning System
GPSR	Greedy Perimeter Stateless Routing
GSM	Global System for Mobile communication
GSM-R	Global System for Mobile communication Railway
GW	GateWay
H	High
HA	Hardware Accelerators
HAL	Hardware Abstraction Layer
HCInt	High Computational Intensity Test

HECC	Hyper Elliptic Curve Cryptography
HH	Handheld
HHN	Hybrid Heterogeneous Network
HIDS	Host Intrusion Detection System
HLR	High Level Requirements
HMAC	Hash Based Message Authentic Code
HMF	Human-Made Faults
HTTP	HyperText Transfer Protocol
HW	Hardware
I/O	Input/Output
ICAO	International Civil Aviation Organization
ICMP	lnternet Control Message Protocol
ICT	Information and Communication Technology
ID	Identity
IDE	Intrusion Detection Event
IDS	Intrusion Detection Systems/Schemes
IEC	International Electro-technical Commission
IEEE	Institute of Electrical and Electronics Engineers
I-ES Node	Intelligent Embedded System Node
IETF	Internet Engineering Task Force
IF	Intermediate Frequency
IFP	Integer Factorization Problem
IKE	Internet Key Exchange
IMA	Integrated Modular Avionic
INCITS	InterNational Committee for Information Technology Standards
IO	Input Output
IoT	Internet of Things
IP	Intellectual Property
IP	Internet Protocol
IPR	Intellectual Property Rights
IPSec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPx	Industrial Priority x
IRQ	Interrupt ReQuest
IRS	Inertial Reference Systems

ISO	International Organization for Standardization
IT	Information Technology
ITH	Internet of Things and Human
J2ME	Java 2 Platform Micro Edition
J2SE	Java 2 Platform Standard Edition
JCP	Java Community Process
JINI	Java Intelligent Network Infrastructure
JMEDS	Java Multi Edition DPWS Stack
JU	Joint Undertaking
JVM	Java Virtual Machine
KL	Karhunen-Loève
L	Low
LAN	Local Area Network
LBSN	Location Based Social Networking
LBSs	Location Based Services
LCSE	Life Cycle Support Element
LDA	Linear Discriminant Analysis
LDPKI	Locally Distributed Public Key Infrastructure
LDs	Legacy Devices
L-ESD	Legacy Embedded System Device
LOS	Line Of Sight
LPC	Low Pin Count, TPM bus interface
LRUs	Line-Replaceable Units
LSB	Least Significant Bit
LSPDN	Legacy SPD Node
LSSL	Light Secure Socket Layer
M	Medium
M2B	Most To Business
MAC	Medium Access Control
MAC	Message Authentication Code
MANET	Mobile Ad Hoc Network
MAS	Multi Agent System
MCMR	Multi-Channel Multi-Radio
MCU	Multipoint Control Unit
MDSSACF	Mean-Delta Sub-band Signals Auto-Correlation Function
MEMS	Micro ElectroMechanical Systems

MF	Master File
MIDP	Mobile Information Device Profile
MMC	Multimedia Cards
MMS	Multi-dimensional Metric Space
MMU	Memory Management Unit
MNTs	Micro and Nano Technologies
MODAF	Ministry of Defence Architecture Framework
MOM	Message Oriented Middleware
MOSA	Modular Open System Approach
MP	Multi Prerequisite
MPNs	Micro Personal Nodes
MRS	Main Requirements Specification
MS	Middleware Service
MSB	Most Significant Bit
MSC	Mid Speech Clipping
MSSACF	Mean Sub-band Signals Auto-Correlation Function
MTTF	Mean Time To Failure
MTTR	Mean Time To Repair
MwA	Middleware Adapter
NAC	Network Access Control
NC	Node Capability
ND	Network Delay
NDP	Neighbor Discovery Protocol
NDS	Noise Detected as Speech
n-ESD	No communication capabilities Embedded System Device
NFUA	Not Faults with Unauthorized Access
NHMF	NonHuman-Made Faults
NIDS	Network Intrusion Detection System
NIST	National Institute of Standards and Technology
NMA	Network Management Authority
NMP	Nano, Micro, Personal
NMPS	Nano, Micro, Personal Sensor
NMP-SPD	Nano, Micro, Personal Security Privacy Dependability
NoA	Node Adapter
NPHCT	Neyman-Pearson Composite Hypothesis Testing
NS	Network Service

nSA	nSHIELD System Architecture
nS-ESD	nSHIELD Embedded System Device
Ns-ESD GW	nSHIELD Embedded System Device GateWay
nSHIELD	new embedded Systems arcHItecturE for multi-Layer Dependable solutions
nS-MS	nSHIELD Middleware Service
nSNA	nSHIELD Node Adapter
nS-OS	nSHIELD Overlay Service
nS-P	nSHIELD Proxy
nSS	nSHIELD System
nS-SPD-ESD	nSHIELD SPD Embedded System Device
NSU	Navigation Sensor Unit
NTRU	Nth degree Truncated Polynomial Ring Cryptography
NW	Network
NwA	Network Adapter
OFA	Objective Function Attack
OGSA	Open Grid Service Architecture
OLSR	Optimized Link State Routing Protocol
OMaSE	Organization-based Multiagent System Engineering
OMG	Object Management Group
Open GL	Open Graphic Library
ORBs	Object Request Brokers
OS	Operating System
OSAV	Operational Security Assurance Value
OSGi	Open Services Gateway initiative
OSI	Open Systems Interconnection
OSP	Organisational Security Policy
OTA	Over-The-Air
OVP	Open Virtual Platforms
OWL-S	Ontology Web Language for Services
P2P	Peer-to-Peer
P3	Peer-to-Peer-to-Place
PA	Path Array
PACA	Passive and Active Combined Attacks
PACS	Physical Access Control System
PANA	Protocol for Carrying Authentication for Network Access
PB	Project Board

PB	Priority-Based
PBM	Policy Based Management
PC	Personal Computer
PCA	Principle Component Analysis
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
PCIX	Peripheral Component Interconnect eXtended
PDA	Personal Digital Assistant
PDF	Probability Density Function
PGD	Page Global Directory
PIM	Platform-Independent Model
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKG	Private Key Generator
PKI	Public Key Infrastructure
Pl-ESD	Proprietary logical communication capabilities Embedded System Device
PM	Project Manager
Pnodes	Persistence nodes
PNs	Power Nodes
PP	Protection Profile
pp-ESD	Proprietary physical communication capabilities Embedded System Device
PPM	Probabilistic Packet Marking
PPTMs	Public and Private Transportation Means
PRNG	Pseudo Random Number Generator
pSHIELD	pilot embedded Systems arcHItecturE for multi-Layer Dependable solutions
PSM	Platform-Specific Model
PTE	Page Table Entry
PU	Primary User
PUEA	Primary User Emulation Attack
QA	Quality Assurance
QC	Quality Control
QL	Queue Length
QMF	Quadrature Mirror Filters
QoS	Quality of Service
R&D	Research and Development
R&S	Requirements and Specifications

RAM	Random Access Memory
RBFC	Random Branch Function Call
R-CFG	Radio Configuration
REL	Rights Expression Language
REQ	Requirement
RF	Radio Frequency
RFI	Radio Frequency Interference
RFID	Radio Frequency IDentification
RFSN	Reputation-based Framework for Sensor Network
RGB	Red, Green and Blue
RISC	Reduced Instruction Set Computer
RIU	Remote Interface Unit
RM-ODP	Reference Model for Open Distributed Processing
RNG	Random Number Generator
ROC	Receiver Operator Characteristic
ROM	Read Only Memory
RPCs	Remote Procedure Calls
RR	Runtime Reconfiguration
RS	Railway Security
RSA	Rivest Shamir & Adleman
RSS	Received Signal Strength
RSSI	Received Signal Strength Indication
RT	Response Time
RTOS	Real Time Operating System
RTPS	Real Time Publish Subscribe
SA	Security Assurance
SAE	Speech Activity Envelope
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SAV	Security Assurance Value
SBLs	Street and Building Lights
SBW	Small Backoff-Window
SBW	Soldier Broadband Waveform
SC	Security Context
SCA	Side-Channel Attacks
SCENs	Sensor Cognitive Enabled Nodes

SD	Secure Digital
SDP	Service Discovery Protocol
SDR	Software Defined Radio
SDRM	Second Derivative Round Mean
SEMA	Simple ElectroMagnetic Analysis
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SHIELD	Systems arcHItecturE for multi-Layer Dependable
SJA	Smart Jamming Attack
SKC	Symmetric Key Cryptosystem
SLP	Service Location Protocol
SM	Static Metric
SM	Security Mechanism
SMART	Specific Measurable Attainable Repeatable and Time-dependent
SMN	Social Mobility and Networking
SMS	Security Management System
SNC	Sensing, Networking and Computation
SNMP	Simple Network Management Protocol
Snodes	Synchronization nodes
SNR	Signal/Noise Ratio
SOA	Service Oriented Architecture
SoA	State of Art
SOAP	Simple Object Access Protocol
SoC	System on Chip
SOCRADES	Service-Oriented Cross-layer Infrastructure for Distributed Smart Embedded Devices
SODA	Service-Oriented Device & Delivery Architecture
SoES	System of Embedded System
SOM	System-on-Module
SP6	Sub Programme 6
SPA	Simple Power Analysis
SPD	Security, Privacy and Dependability
SPDN	Security, Privacy and Dependability Node
SPDP	Secure Pervasive Discovery Protocol
SPDT	Security Privacy Dependability Trust
SPD-WSN	Security, Privacy and Dependability Wireless Sensor Network

SPU	Smart Power Unit
SQL	Structured Query Language
SR	Secure Routing
SRM	Secure Radio Middleware
SRS	System Requirements and Specification
SSACF	Sub-band Signals Auto-Correlation Function
SSDFA	Spectrum Sensing Data Falsification Attack
SSDP	Simple Service Discovery Protocol
SSL	Secure Socket Layer
STPD	Security Trust Privacy Dependability
STS	Security Token Service
SU	Secondary User
SVC	Supervisor Call
SVM	Support Vendor Machine
SW	Software
SWAVE	Secure Wideband Multi-role - Single-Channel
SWI	Software Interrupt
SWS	Semantic Web Services
SW-TPM	Software Trusted Platform Module
TA	Technical Annex
TAI	Total Attack Impact
TASI	Time Assignment Speech Interpolation system
TBD	To Be Defined
TC	Thread Count
TC	Trusted Computing
TC	Trust Chain
TCB	Trusted Code Base
TCEM	Trusted Composition Evaluation Model
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEO	Teager Energy Operator
TETRA	Terrestrial Trunked Radio
TLB	Translation Looks Aside Buffer
TLS	Transport Layer Security
TM	Technical Manager

TMC	Technical Management Committee
ToC	Table of Content
TOE	Target Of Evaluation
TOGAF	The Open Group Architecture Framework
TPM	Trusted Platform Module
TSF	TOE Security Functionality
TTP	Trusted Third Party
TV	Television
TX/RX	Transmission /Reception
U&PC	Ubiquitous and Pervasive Computing
UART	Universal Asynchronous Receiver-Transmitter
UAV	Unmanned Aerial Vehicle
UCN	Ubiquitous Computing Network
UDDI	Universal Description, Discovery and Integration
UDP	User Datagram Protocol
UHF	Ultra High Frequency
UM	Used Memory
UML	Unified Modeling Language
UMTS	Universal Mobile Telecommunications System
UPC	Ubiquitous and Pervasive Computing
UTP	Unshielded Twisted Pair
UWCN	Ubiquitous Wearable Computing Network
V&V	Validation & Verification
VAD	Voice Activity Detection
VAS	Voice Activity Shape
VD	Voice Detection
VFR	Voice/Facial Recognition
VGA	Video Graphics Array
VH	Very High
VHF	Very High Frequency
VL	Very Low
VM	Virtual Machines
VMM	Virtual Machine Monitor
VMS	Vehicle Management System
VoIP	Voice over IP
VPN	Virtual Private Network

VULOS	VHF/UHF Line Of Sight
W3C	World Wide Web Consortium
WAN	Wide Area Network
WBDL	Wide Band Data link
WCN	Wearable Computing Networks
WLAN	Wireless Local Area Network
WO	Wireless Operator
WPL	Work Package Leader
WPs	Work Packages
WPT	Wavelet Packet Transform
WPx	Work Package x
WS	Wireless Sensor
WS4D	Web Services for Devices
WSA	Web Services Architecture
WS-BPEL	Web Services Business Process Execution Language
WS-CDL	Web Services Choreography Description Language
WS-CF	Web Services Contract-First
WSCI	Web Services Choreography Interface
WSDL	Web Services Description Language
WSMO	Web Services Modeling Ontology
WSN	Wireless Sensor Network
WSPRT	Wald's Sequential Probability Ratio Test
WSS	Web Services Security
WT	Wait Time
WWSN	Worldwide Wireless Sensor Network
XML	Extensible Markup Language