



SHIELD

Status, achievements, impact

Budapest

11-12 September 2012



- **1 September 2011:** *Project started*
- **October 2011:** *Kick Off meeting*
- **October 2011:** *SHIELD first participation at the ITEA Co-Summit meeting in Helsinki*
- **October 2011:** *Wiki page and Website set up*
- **November 2011:** *Negotiation concluded*
- **December 2011:** *Josef Noll (Movation) signed the Joint Undertaking Grant Agreement.*
A "Final" Official Technical Annex is available in wiki.
Partners who have their National Grant Agreement signed: In order to receive the funds, A3 Form has to be signed in three copies.
- **February 2012:** *Reviewed the Amendments proposed from the Consortium. Josef Noll will present Amendments to JU Officer for approval in October 2012.*
- **31 December 2011:** *pSHIELD "officially" concluded on 14 February 2012*
- **Feb 2012:** *SESM moves 4 MM from the task #7.2 "Voice/Facial Recognition" to the task #7.3 "Dependable Avionic Systems".*
SESM will have 16MM on the 7.2 task.
- **April 2012:** *WP2 deliverables (THYIA - SE) discussions. Status D2,1 (completed) and D2,2 finalized but need to be reworked*
- **April 2012:** *The software used by the Commission to check the plagiarism ration of a document is Viper. Shall we use it?*
- **May 2012:** *ESIS left the project. Their effort is 16 MM (WP6-WP7).*
- **May 2012:** *Operational Manual (D8.4) and Standardisation (D8.3) need to be better addressed*
- **June 2012:** *D3.1, D4.1 completed.*
- **June 2012:** *First version D2.2 finalized. SE proposed a new version of the document and is leading the re-work.*
- **September 2012:** *Project review in preparation of the Annual Review (October 2012)*
- **October 2012:** *First Annual Review*

			WP1		WP2			WP3					WP4				WP5				WP6			WP7				WP8			
			T1.1	T1.2	T2.1	T2.2	T2.3	T3.1	T3.2	T3.3	T3.4	T3.5	T4.1	T4.2	T4.3	T4.4	T5.1	T5.2	T5.3	T5.4	T5.5	T6.1	T6.2	T6.3	T7.1	T7.2	T7.3	T7.4	T8.1	T8.2	T8.3
1	Movation AS	MAS	NO																			5	2		5			3		1	2
2	Ansaldo STS	ASTS	IT	2		5	4															3	3		16			1	1	1	
3	ACORDE Technologies, SA	AT	ES	9				8	7	7												13	6		2			2	2		
4	ATHENA	ATHENA	GR	3								3	5		10							9	9	3				2	2		
5	Selex Elsag	SE	IT	17	6	4	6	3	2	2	3	1	0	50	30	2	2	10	5	18	10				2	0	5	3	3	0	0
6	Fundación Tecnalia Research & Innovation	TECNALIA	ES	5													6	8						15		8		2	2	4	
7	ESIS Norge AS	ESIS	NO																			4					8			1	
8	Eurotech Security	ETH	IT	1		1	1		25													3			18			1			
9	Hellenic Aerospace Industry	HAI	GR	12	3	5	5	12				4			12	3	6		15	6		18	8	6	10		3	10	2		4
10	Indra Software Labs	ISL	ES	10											12	22				18		24						5	4	5	
11	Integrated Systems Development	ISD	GR	2							58											2	2	2	2	2	2				
12	Selex Galileo	SG	IT	30	10	5	5		5	5	6		5		5	5	5	5				10				30	5	5			
13	University of Mondragon	MGEP	ES	3											12	8	8					3						11			
14	Noom AS	NOOM	NO																			1					5				
15	Security Evaluation Analysis and Research Lab.	S-LAB	HU			5	5					6	6					14				5	12	12	6	6	6	6	5		
16	SESM - FINMECCANICA	SESM	IT								15																16				
17	Swedish Institute of Computer Science	SICS	SE			3		3	5	5	5	5																			
18	T2 DATA AB	T2D	SE			5		5			13	13																			
19	Telcred AB	TELC	SE								3		3												3						
20	THYIA Tehnologije	THYIA	SI	10	3	10	5	5	12	6		6	6	4	3		5	8	2	2	7	8	4		8		24	2	2	1	
21	Technical University of Crete	TUC	GR	4		3	4	3	7	7		8	15			6	8			10	8					4		5	5		
22	Università di Genova	UNIGE	IT								15	15		20	5												3	2			
23	Università di Udine	UNIUD	IT	3		1	1	1	12						12								6								
24	Sapienza - Università di Roma	UNIROMA1	IT	3											0		9	14		18		4									

Total			114	22	47	50	44	50	73	100	46	66	79	60	50	61	49	66	69	48	0	122	68	38	54	41	62	66	46	19	18
-------	--	--	-----	----	----	----	----	----	----	-----	----	----	----	----	----	----	----	----	----	----	---	-----	----	----	----	----	----	----	----	----	----

1628

ESIS left the project

SLAB effort/2 => from 28 to 14 in WP5

T5,4 and T5,5 are merged (T5,5 deleted)

UNIROMA moves 8MM from WP4 to WP5

TUC reallocated MM distribution. Total is the same. See Amendment 16

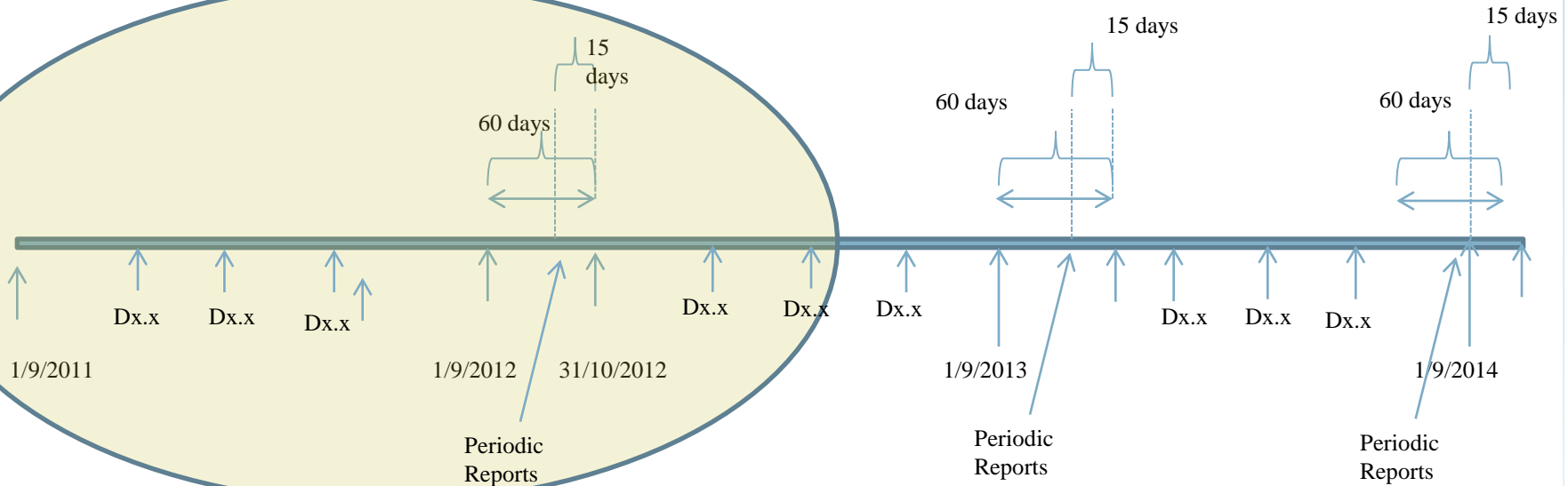
UNIUD reallocate WP2 effort as 1MM on T2,1, 1MM on T2,2, and 1 MM on T2,3

ACORDE requested to move all our MM from T3.3 to task T3.1

Telcred has 3 MM on 7,1 and 0 on 7,4

SESM moves 8 MM from 7.2 to 7.3 (7,2=0MM, 7,3=16MM)

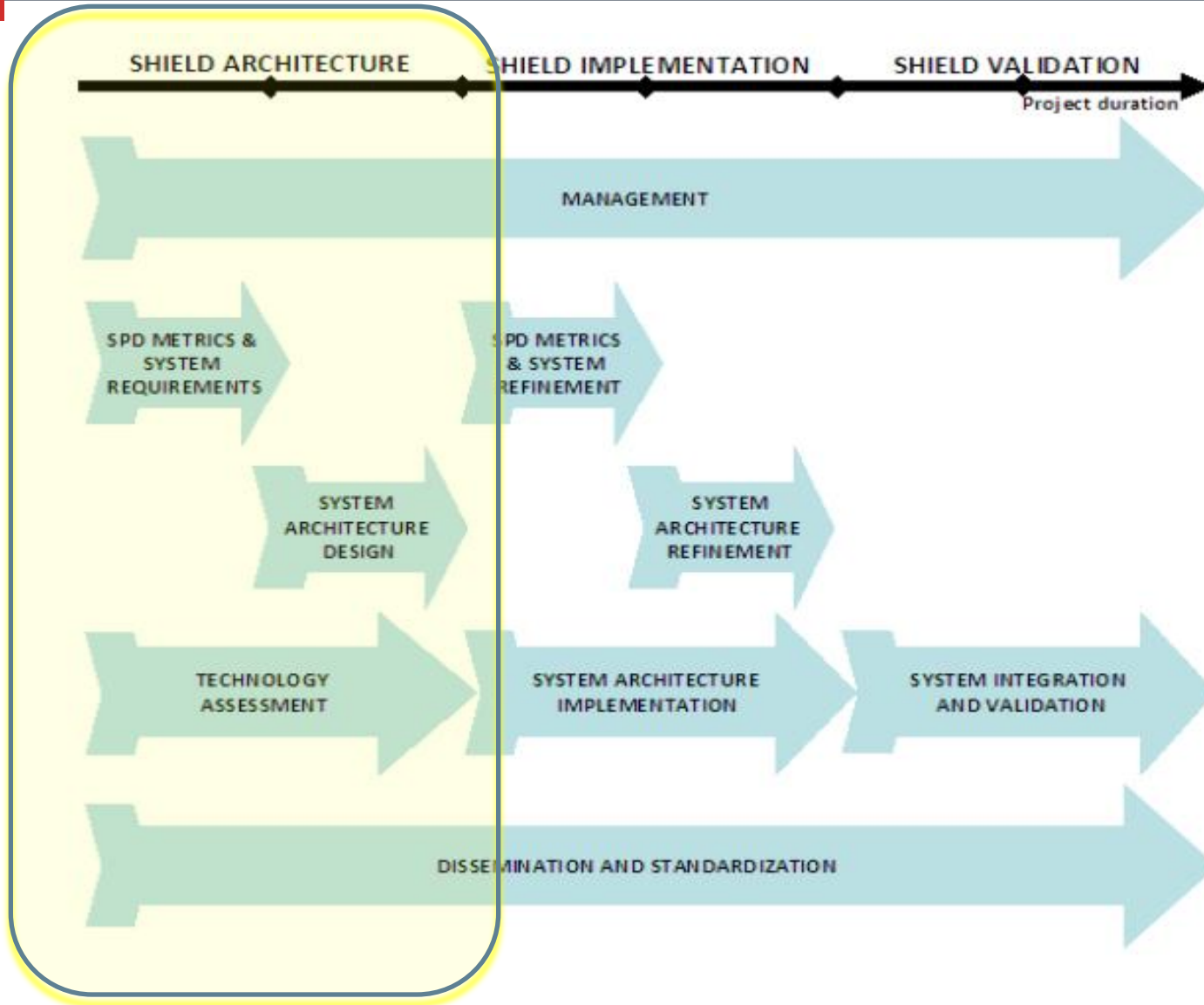
- **First Official Review will be held in Rome on October the 17th 2012**
- **On October the 16th (in Rome) all the partners are required to attend to a full day pre-meeting.**
- **All deliverables must be completed by **October the 1st 2012 (14:00:00 Rome Time)**. The wiki page is the SHIELD repository (both PDF and word format have to be uploaded).**
- **On October the 2nd 2012, the deliverables will be transferred to the SHIELD wiki section used for delivering the documents to the JU Officer. This page is only accessible by the JU Officer, Josef Noll and Luigi Trono.**

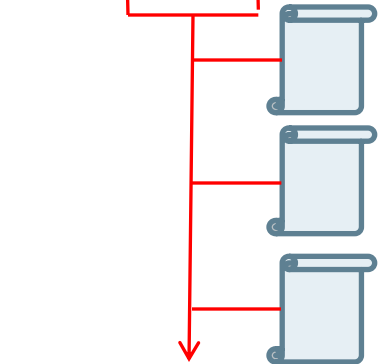
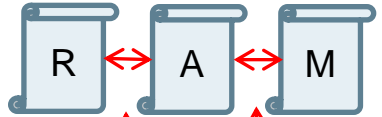


Del. no.	Deliverable name	WP no.	Nature	Dissem. level	Delivery date (proj. month)	Responsible	Status
D1.1	Collaborative tools and document repository	1	O	PP	2	L.Trono	100%
D8.1	Web Site	8	O	PU	2	R.Uribeetxeberria	100%
D1.2	Quality Control Guidelines	1	R	PP	3	L.Trono	100%
D1.3	Liaisons Plan	1	R	PP	3	L.Trono	100%
D2.1	Preliminary System Requirements	2	R	CO	3	S.Drakul	100%
D3.1	SPD node technologies assessment	3	R	CO	4	P.Azzoni	100%
D4.1	SPD network technologies assessment	4	R	CO	5	M.Cesena	90%
D5.1	SPD middleware and overlay technologies assessment	5	R	CO	6	A.Morgagni	90%
D1.4	Periodic Management Report 1	1	R	PP	6	L.Trono	90%
M1	D2.2 Preliminary System Requirements and Specifications	2	R	PU	6	S.Drakul	50% (100%)
D8.2	Dissemination Plan	8	R	PP	6	R.Uribeetxeberria	100%
D8.3	Standardization Plan	8	R	PP	6	L.Trono	90%
D2.3	Preliminary system architecture design	2	R	CO	9	A.Poulakidas	100%
D1.5	Periodic Annual Report 1	1	R	PP	12	L.Trono	20%
M2	D2.4 Reference system architecture design	2	R	PU	12	A.Poulakidas	70%
	D2.5 Preliminary SPD Metrics specifications	2	R	CO	12	I.Eguia	90%
D8.4	nSHIELD Operational Manual v1	8	R	PU	12	R.Uribeetxeberria	0%

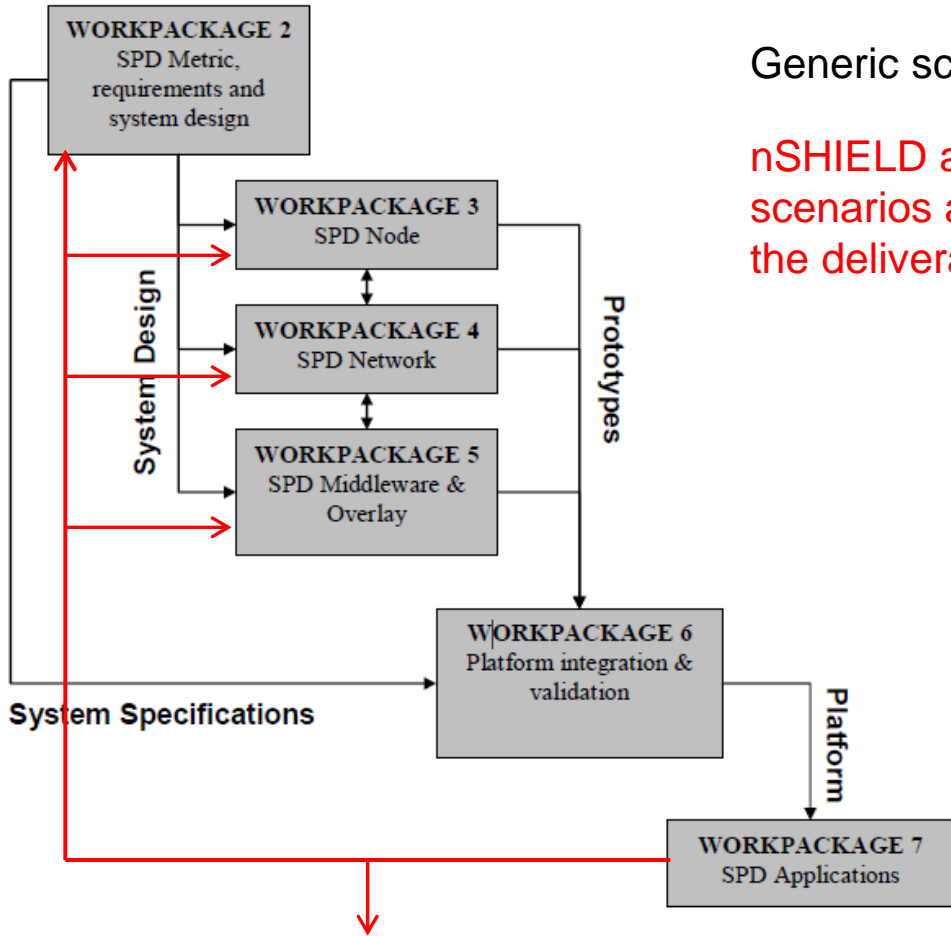
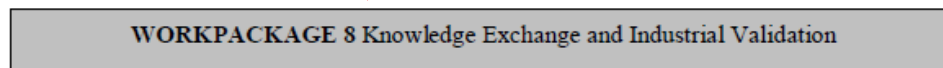
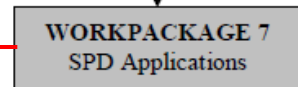
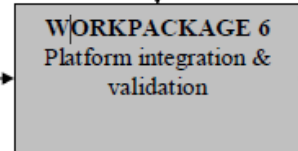
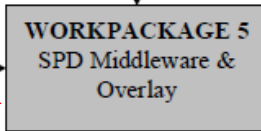
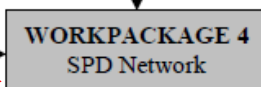
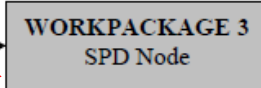
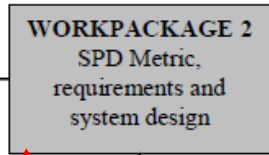
R = Report,
P = Prototype,
D = Demonstrator,
O = Other

PU = Public
PP = Restricted to other programme participants (including the JU).
RE = Restricted to a group specified by the consortium (including the JU).
CO = Confidential, only for members of the consortium (including the JU).





Deliverable consistency



Generic scenario: pSHIELD approach

nSHIELD approach: the four scenarios add specific guidelines to the deliverables.



Deliverable

TABLE 1. DELIVERABLES

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I (proj month)	Delivered Yes/No	Actual / Forecast delivery date	Comments
D1.1	Collaborative tools and document repository	1	SG	O	PP	2	Yes		
D8.1	Web Site	8	MGEP	O	PU	2	Yes		
D1.2	Quality Control Guidelines	1	SG	R	PP	3	Yes		
D1.3	Liaisons Plan	1	SG	R	PP	3	No	June 2012	
D2.1	Preliminary System Requirements	2	THYIA	R	CO	3	Yes		
D3.1	SPD node technologies assessment	3	ETH	R	CO	4	No	April 2012	
D4.1	SPD network technologies assessment	4	SE	R	CO	5	No	April 2012	
D5.1	SPD middleware and overlay technologies assessment	5	SE	R	CO	6	No	June 2012	
D1.4	Periodic Management Report 1	1	SG	R	PP	6	Yes		
D2.2	Preliminary System Requirements and Specifications	2	THYIA	R	PU	6	No	March 2012	A second version of this document might be needed. Discussion is in progress.
D8.2	Dissemination Plan	8	MGEP	R	PP	6	Yes		
D8.3	Standardization Plan	8	SG	R	PP	6	No	June 2012	

TABLE 2. MILESTONES

Milestone no.	Milestone name	Work package no	Lead beneficiary	Delivery date from Annex I	Achieved Yes/No	Actual / Forecast achievement date	Comments
M1	Preliminary System Requirements and Specification	WP2	THYIA	M6	No	March 2012	

TABLE 1. DELIVERABLES

Del. no.	Deliverable name	WP no.	Lead beneficiary	Nature	Dissemination level	Delivery date from Annex I (proj month)	Delivered Yes/No	Actual / Forecast delivery date	Comments
D1.5	Periodic Annual Report 1	1	SG	R	PP	12	No	September 2012	
D2.4	Reference system architecture design	2	HAI	R	PU	12	No	September 2012	
D2.5	Preliminary SPD Metrics specifications	2	Tecnalia	R	CO	12	No	September 2012	
D8.4	nSHIELD Operational Manual v1	8	MGEP	R	PU	12	No	September 2012	

TABLE 2. MILESTONES

Milestone no.	Milestone name	Work package no	Lead beneficiary	Delivery date from Annex I	Achieved Yes/No	Actual / Forecast achievement date	Comments
M2	Preliminary SPD metrics and System Architecture Design	WP2	THYIA	M12	No	September 2012	D2.2.1, D2.3.2

R = Report,

P = Prototype,

D = Demonstrator,

O = Other

PU = Public

PP = Restricted to other programme participants (including the JU).

RE = Restricted to a group specified by the consortium (including the JU).

CO = Confidential, only for members of the consortium (including the JU).

Railways security

Voice/Facial Recognition

Dependable Avionic Systems

Social Mobility

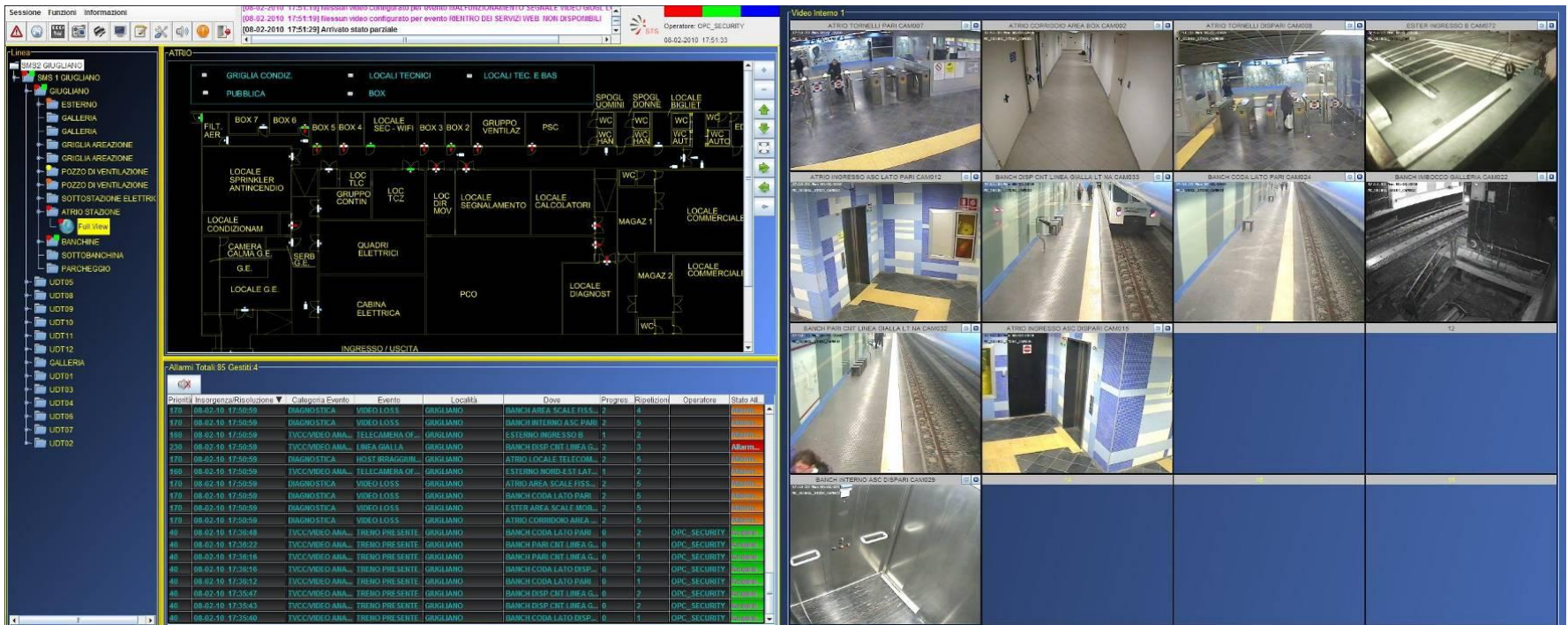
ASTS Scenario Security Management System for railway security



- Rail-based mass transit systems are vulnerable to many criminal acts, ranging from vandalism to terrorism.
- Asset: Tunnel, Train Board, Platform and public area, Technical Control room, Depots.
- In SMS (Security Management System), heterogeneous intrusion detection, access control, intelligent video-surveillance and abnormal sound detection devices are integrated.
- Redundancy both in sensor dislocation and hardware apparels (e.g. by local or geographical clustering) improve detection reliability, through alarm correlation, and overall system resiliency against both random and malicious threats.



- The core is a web-based software application featuring a graphical user interface.
- The Architecture is distributed and hierarchical, with both local and central control rooms collecting.
- In case of emergencies, the procedural actions are orchestrated by the SMS.
- Video-analytics is essential, since a small number of operators would be unable to visually control the large number of cameras which are needed to extensively cover all the areas needing to be protected. Therefore, the visualization of video streams is activated automatically when an alarm is generated.

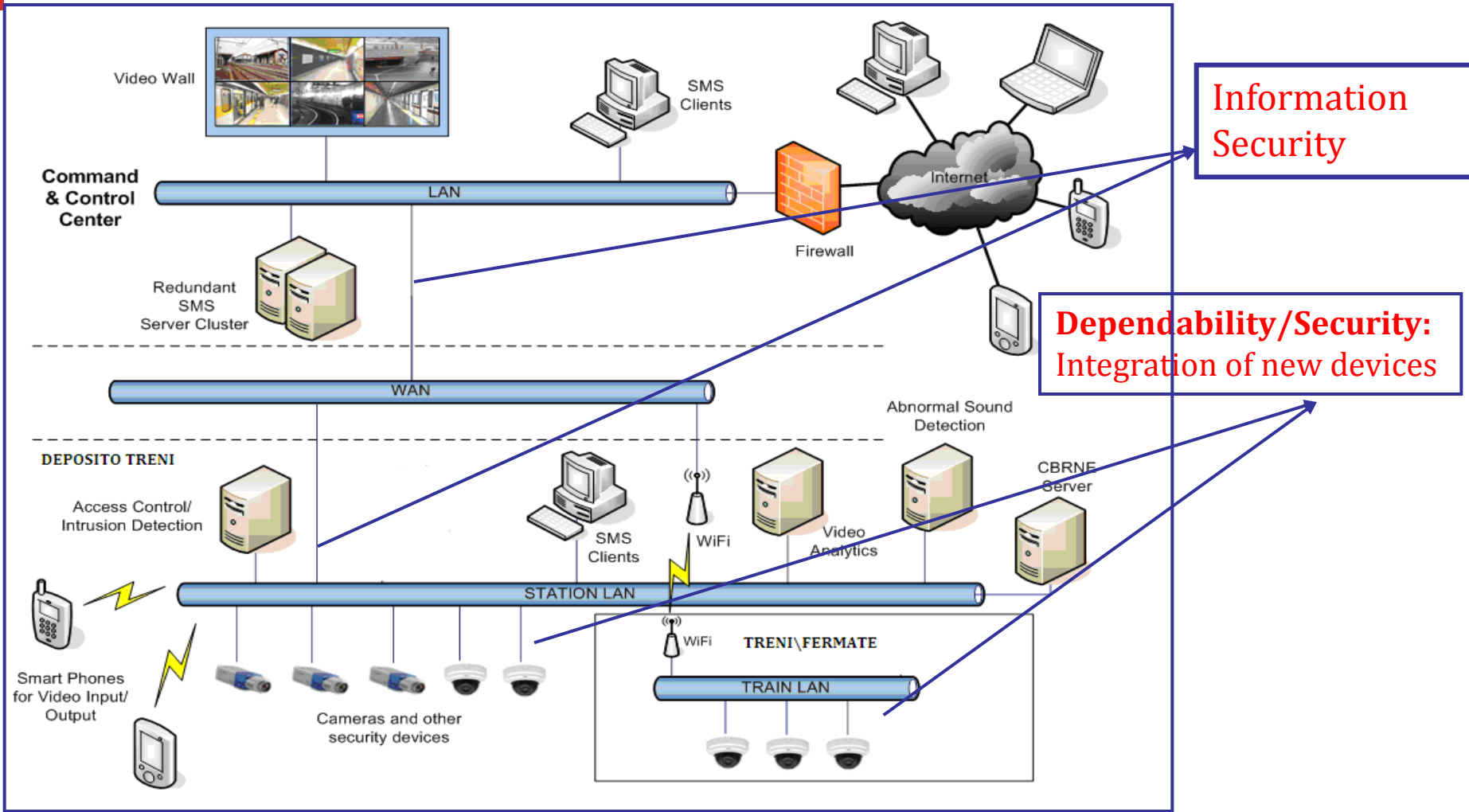


The screenshot displays the SMS interface with the following components:

- Top Bar:** Session information, date/time (08-02-2010 17:51:23), and operator details (Operatore: OPC_SECURITY).
- Left Panel:** A tree view of the facility layout, including areas like 'SMS 1 GIUGLIANO', 'ESTERNO', 'GALLERIA', and 'UDT05' through 'UDT13'.
- Main Panel:** A detailed floor plan of the 'ATRIO' area, showing various rooms such as 'GRIGLIA CONDIZ.', 'LOCALI TECNICI', 'LOCALI TEC. E BAS', 'SPOGLI UOMINI', 'SPOGLI DONNE', 'WC', 'MAGAZ 1', 'MAGAZ 2', and 'INGRESSO / USCITA'.
- Bottom Panel:** An 'Alarmi' (Alarms) table with 4 total events. The table columns include:

Id	Descrizione	Località	Data	Progresso	Risoluzione	Operatore	Stato
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	BANCH AREA SCALE FISS.	2	4		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	BANCH INTERNO ASC PARI	2	5		Alarmi...
188	TWCC/VIDEO ANA... TELECAMERA OF...	GIUGLIANO	ESTERNO INGRESO SO B.	1	2		Alarmi...
230	TWCC/VIDEO ANA... LINEA GIALLA	GIUGLIANO	BANCH DISP CNT LINEA G.	2	3		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	ATRIO LOCALE TELECOM...	2	5		Alarmi...
188	TWCC/VIDEO ANA... TELECAMERA OF...	GIUGLIANO	ESTERNO INGRESO EST LATA	1	2		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	ATRIO AREA SCALE FISS.	2	5		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	BANCH CODA LATO PARI	2	5		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	ESTER AREA SCALE SMOGL.	2	5		Alarmi...
170	DIAGNOSTICA VIDEO LOSS	GIUGLIANO	ATRIO CORRIDORO AREA...	2	5		Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO PARI	0	2	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH PARI CNT LINEA G.	0	1	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH PARI CNT LINEA G.	0	1	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO DISP.	0	2	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO PARI	0	1	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH DISP CNT LINEA G.	0	2	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH DISP CNT LINEA G.	0	2	OPC_SECURITY	Alarmi...
80	TWCC/VIDEO ANA... TRENO PRESENTE	GIUGLIANO	BANCH CODA LATO DISP.	0	1	OPC_SECURITY	Alarmi...
- Right Panel:** A grid of 16 video camera feeds showing various interior views of the station, including hallways, escalators, and platform areas.

SMS - Typical Architecture and problems



Information Security

Dependability/Security: Integration of new devices

Dependability: Faults of components and/or whole system

Today Gaps	SHIELD Advantages	RAILWAY SECURITY Scenario
Information Security	Cryptographic protocols improve data security.	Requirements, Architecture, Node layer, Network layer, Middleware layer
Integration of new devices	SHIELD permits the integration of new systems and the evaluation of impact on the overall system dependability.	Requirement, Architecture, Metrics, Node layer, Network layer, Overlay layer
Complex Certification	Easy certification of the overall architecture	Requirement, Architecture, Standardisation
Faults Resilience	Automatic reconfiguration	Requirement, Architecture, Metrics, Node layer, Network layer, Overlay layer
Expensive Integration of different standards	SHIELD standard will embrace different standards	Standardisation, Dissemination

- **Why: increase security, improve reliability of access control, allow security cross check based on multiple information, increase autonomous identification system capabilities, embedded and connected solution.**
- **Where: military facilities, barracks, courts, sensible public infrastructure, energy production power plants, ospitals, airports, harbours...**
- **Functionalities:**
 - face recognition and person identification (camera or ID card),
 - voice recognition and person identification,
 - object recognition and identification (i.e. car plate),
 - automatic data base generation and management,
 - recognition process based on ISO standard and respect of privacy.

Face recognition and person identification



Example of a real scenario: access control at turnstile.

1. Face recognition with quality feedback
2. Biometric template generation
3. Comparison with stored biometric profile
4. Access management and alarm generation

Example of a real scenario: access control at a military facility entrance.



- Leaving the camp:
 - Car plate recognition
 - Driver's voice recognition
 - ZigBee Tag association to car and driver
- Entering the camp:
 - Car plate, driver voice and tag recognition
 - Comparison with stored profile
 - Access management and alarm generation

Today Gaps	nSHIELD Advantages	Deliverables
Complex HW/SW recognition systems	nSHIELD provides an embedded/mobile solution	Requirements, Architecture, Node layer, Network layer, Middleware layer, Overlay layer
Resource consuming recognition algorithms	nSHIELD adopts advanced and effective recognition algorithms suitable for embedded systems	Requirements, Architecture, Node layer
Complex distributed multi-device solutions	Simple solution based on a single device that autonomously provides identification on site.	Requirements, Architecture, Node layer, Network layer, Middleware layer, Overlay layer
Difficult to provide real time recognition in dynamic scenarios	People recognition in static and also in dynamic scenarios.	Requirements, Architecture, Node layer
Trusted data communication and privacy	New Algorithms improve data security and guarantee users privacy	Requirements, Architecture, Network layer, Middleware layer
Complex Certification	Easy certification of the overall architecture	Requirements, Architecture, Standardization
Scalability	Improves low cost and efficient scalability	Standardization, Dissemination

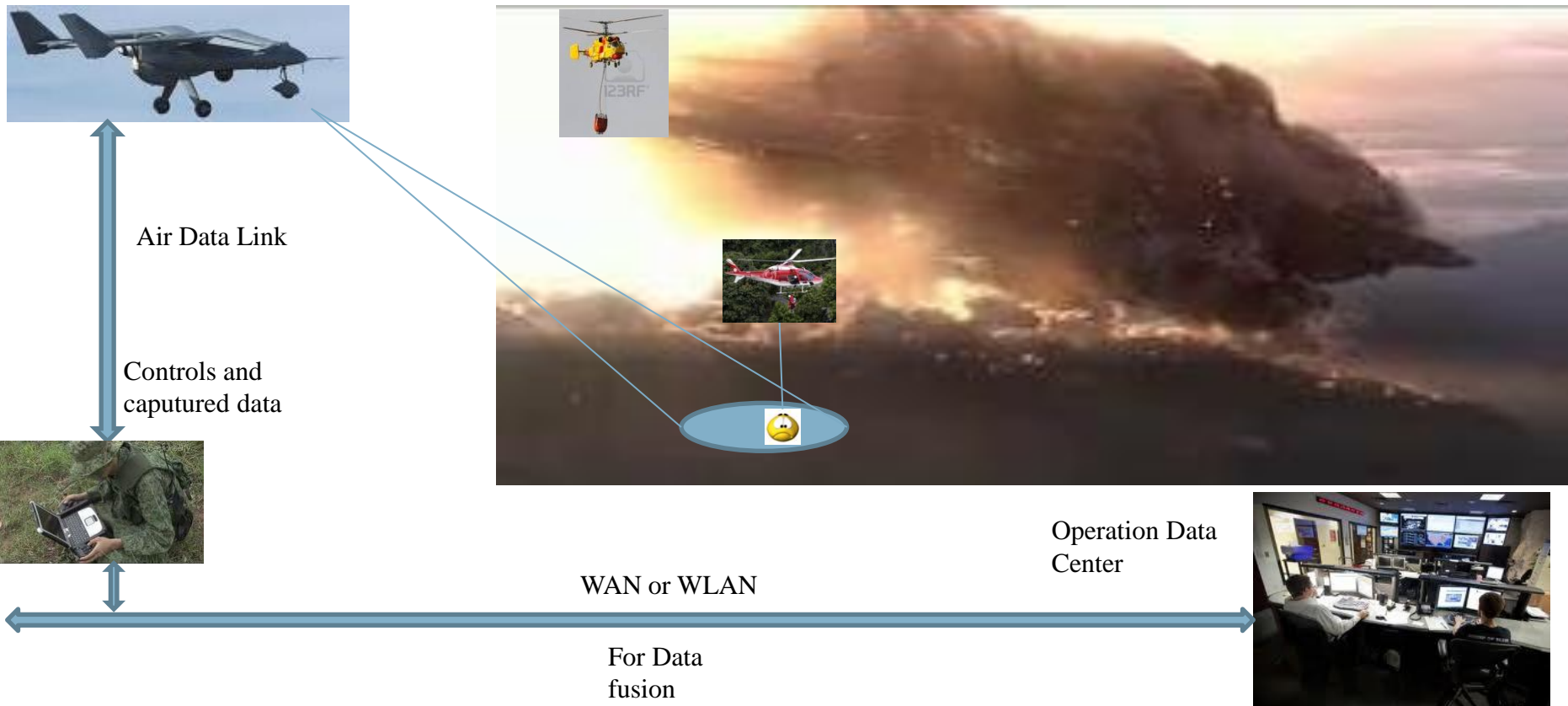
UAV Applications

- **Remote sensing:** Biological sensors are sensors capable of detecting the airborne presence of various microorganisms and other biological factors. Chemical sensors use laser spectroscopy to analyze the concentrations of each element in the air
- **Commercial aerial surveillance:** Aerial surveillance of large areas is made possible with low cost UAV systems. Surveillance applications include: livestock monitoring, wildfire mapping, pipeline security, home security, road patrol and anti-piracy.
- **Oil, gas and mineral exploration and production:** UAVs can be used to perform geophysical surveys, in particular geomagnetic surveys where the processed measurements of the differential Earth's magnetic field strength are used to calculate the nature of the underlying magnetic rock structure. A knowledge of the underlying rock structure helps trained geophysicists to predict the location of mineral deposits. The production side of oil and gas exploration and production entails the monitoring of the integrity of oil and gas pipelines and related installations.
- **Scientific research:** Unmanned aircraft are uniquely capable of penetrating areas which may be too dangerous for piloted craft. An UAV can fly into a hurricane and communicate near-real-time data directly to the National Hurricane Center.
- **Search and rescue:** Search for missing person. A concept of coherent change detection in SAR images allows for exceptional search and rescue ability: photos taken before and after the storm hits are compared and a computer highlights areas of damage.

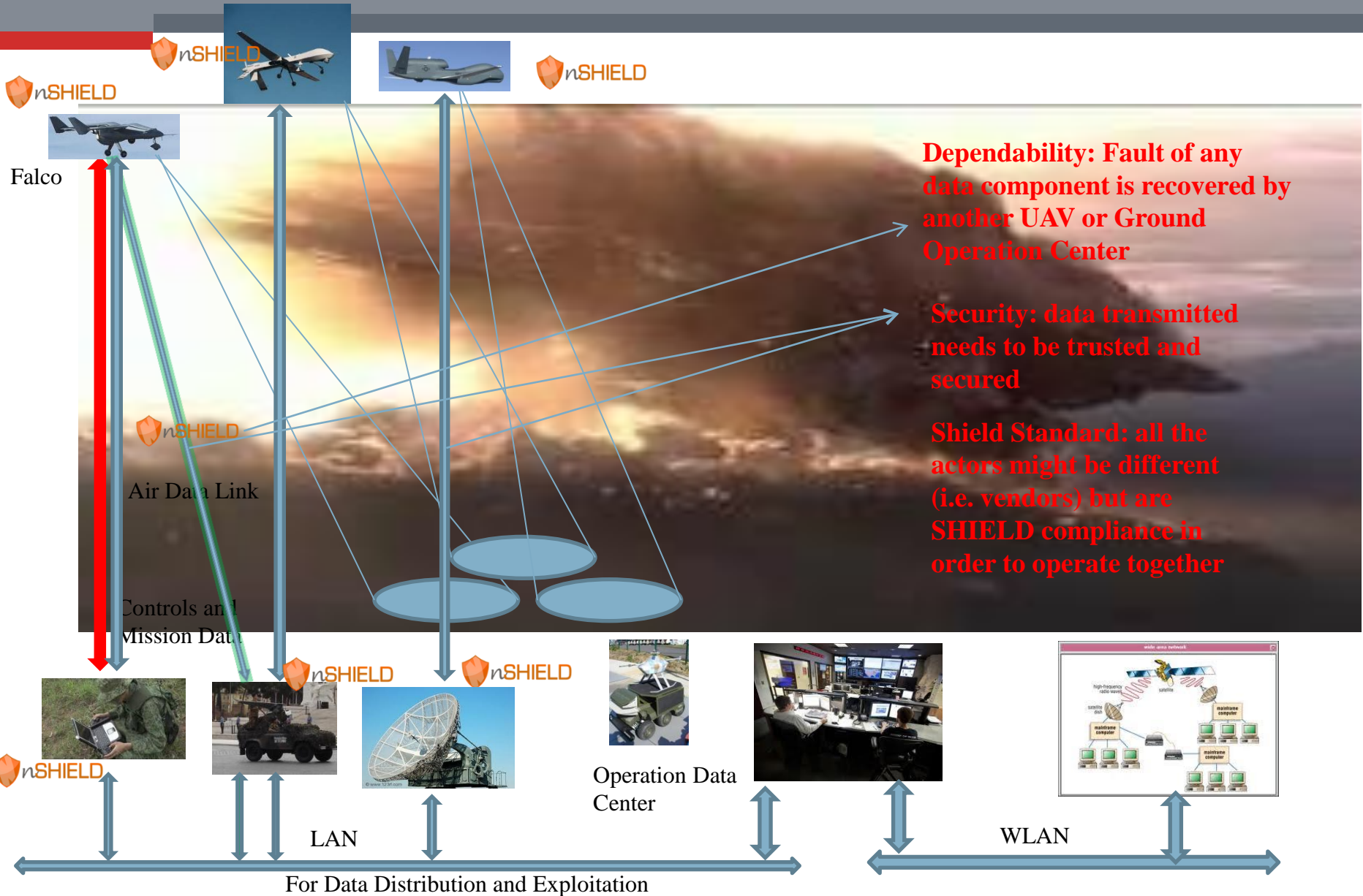


As a result of advances in communication, computation, sensor and energy storage technologies, as well as carbon fiber-reinforced plastic materials, micro unmanned aerial vehicles (UAV) are available at affordable prices. On this basis many new application areas, such as the in-depth reconnaissance and surveillance of major incidents, will be possible. Uncontrolled emissions of liquid or gaseous contaminants in cases of volcanic eruptions, large fires, industrial incidents, or terrorist attacks can be analyzed by utilizing UAV (Figure 1). Hence, the use of cognitive Unmanned Aerial Systems (UAS) for distributing mobile sensors in incident areas is in general a significant value added for remote sensing, reconnaissance, surveillance, and communication purposes

Falco



Dependable Search and Rescue Architecture



Today Gaps	SHIELD Advantages	Avionics Scenario
Eterogeneous Network not fully supported	SHIELD compliancy permits communication between not eterogeneous data	Requiments, Architecture, Node layer, Network layer, Middleware layer
Partial integration, only with same family systems	SHIELD permits the integration of new systems and subsystems	Requiments, Architecture, Metrics, Node layer, Network layer, Overlay layer
Complex Certification	Easy certification of the overall architecture	Requiments, Architecture, Standardisation
Only HW redudancy	Redudancy guarantied throught the SHIELD compliance	Requiments, Architecture, Metrics, Node layer, Network layer, Overlay layer
Trusted Data communication	New Algorithms improve data security.	Requiments, Architecture, Middleware layer
Scalability allowed with added engineering effort	Scalability always allowed with fast module reconfiguration and low engineering cost.	Requiments, Architecture, Metrics, Overlay layer
Expensive Integration of different standards	SHIELD standard will embrace different standards	Standardisation, Dissemination
Sensitive to cyber attacks	Resilience to cyber attacks (UAVs architecture changes continuosly) (polymorphism)	Requiments, Architecture, Metrics, Node layer, Network layer, Overlay layer

