SeCoServ2

Saving Lives but keeping Privacy

PSCE-Conference, Graz 27-28 May 2015

Project funded by:

Bundesministerium
für Bildung
und Forschung

Program Execution Organisation

VDI|VDE|IT

Consortium Members

X-LANE move beyond

VOMATEC®

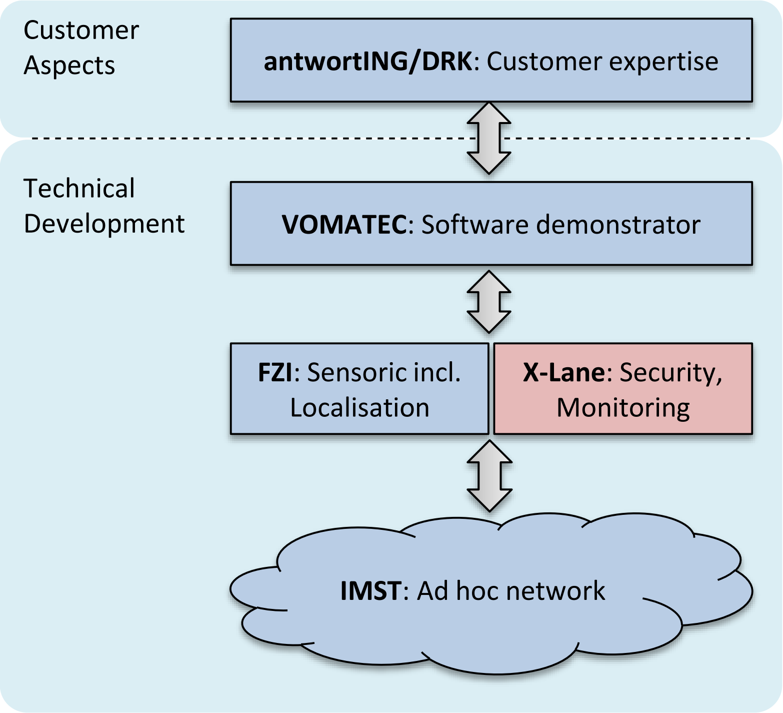
IMST

FZI

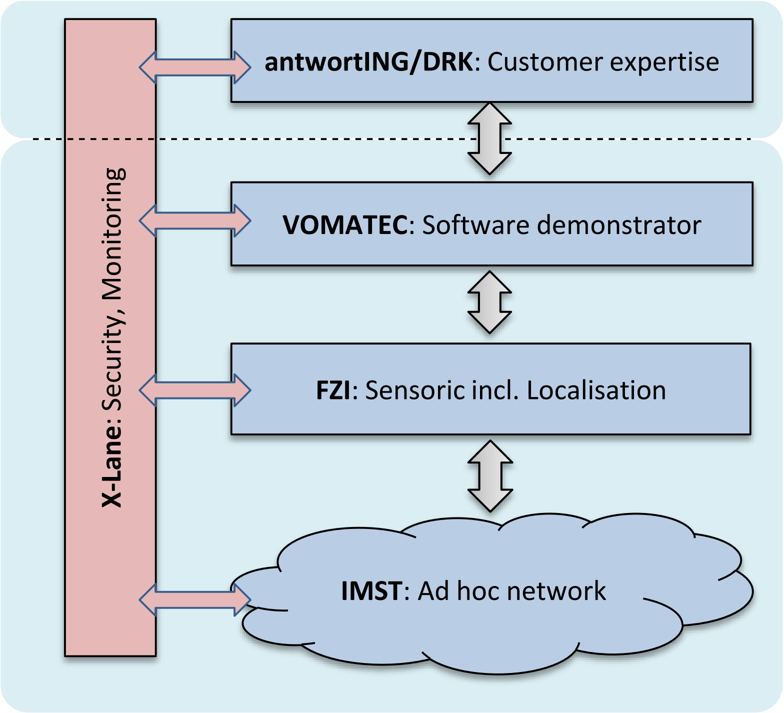
aw ING

Project Evolution

- Kick-off project plan


Customer Aspects
antwortING/DRK: Customer expertise
Technical Development
VOMATEC: Software demonstrator
FZI: Sensoric incl. Localisation
X-Lane: Security, Monitoring
IMST: Ad hoc network

- Midterm project plan


X-Lane: Security, Monitoring
antwortING/DRK: Customer expertise
VOMATEC: Software demonstrator
FZI: Sensoric incl. Localisation
IMST: Ad hoc network

Bundesministerium
für Bildung
und Forschung

Early Lessons learned

SeCoServ2

The **original** project **plan** was,
to apply security tools like:

Attack Trees,
Protection Profiles
Security by Design
…

Early observation for this:
a nearly stable development plan would have been required.

However:

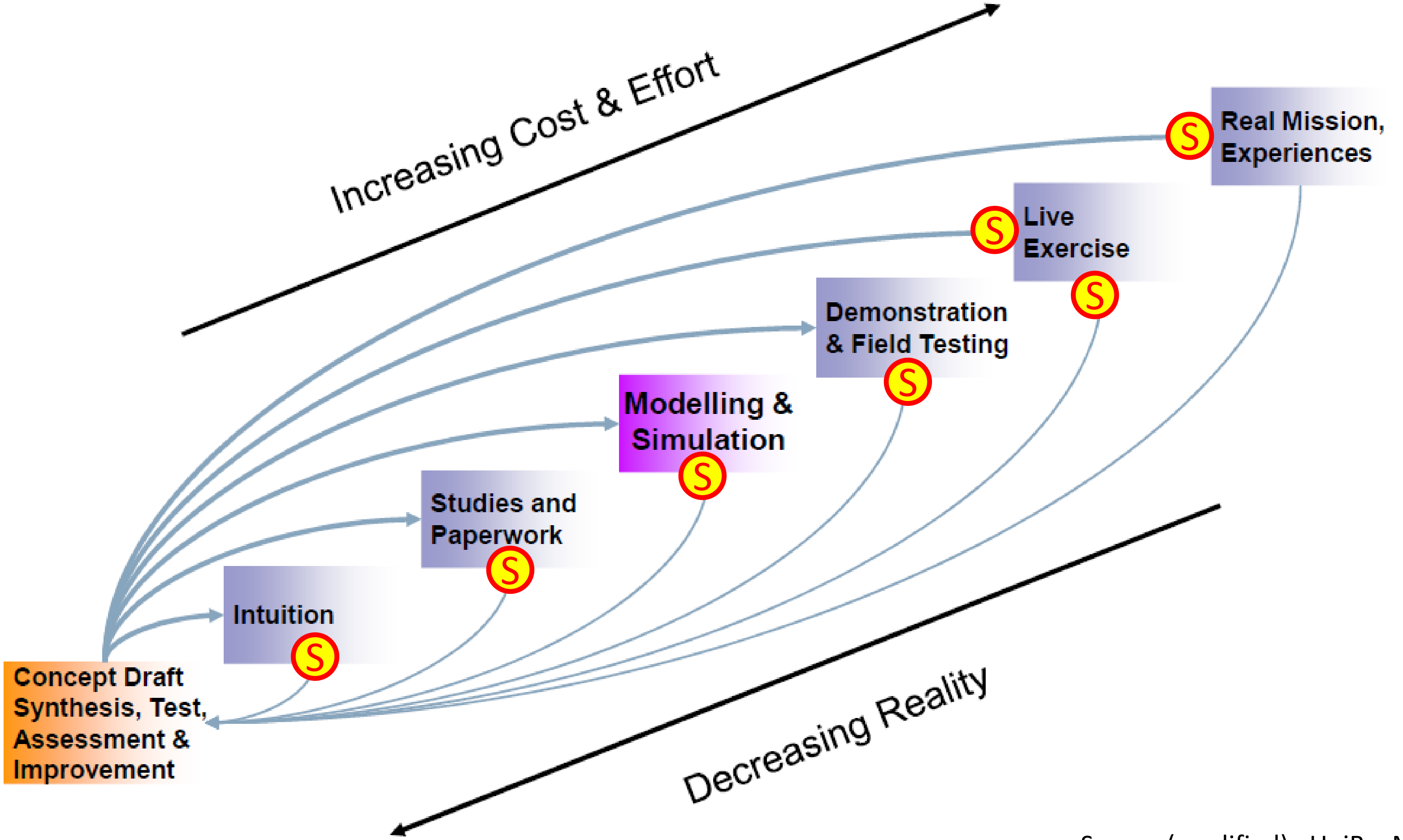
- SeCoServ2 (re)started from scratch
- was based previous experience from the Project MANET.
- Basic models were under discussion

Adjusted plan:

- Understanding the functionality to be developed
  - Following the development process continously
- Observing the user behavior
  - Collecting knowledge at all demonstrations

▶ Video: Table Test & Evaluation 10.05.2013

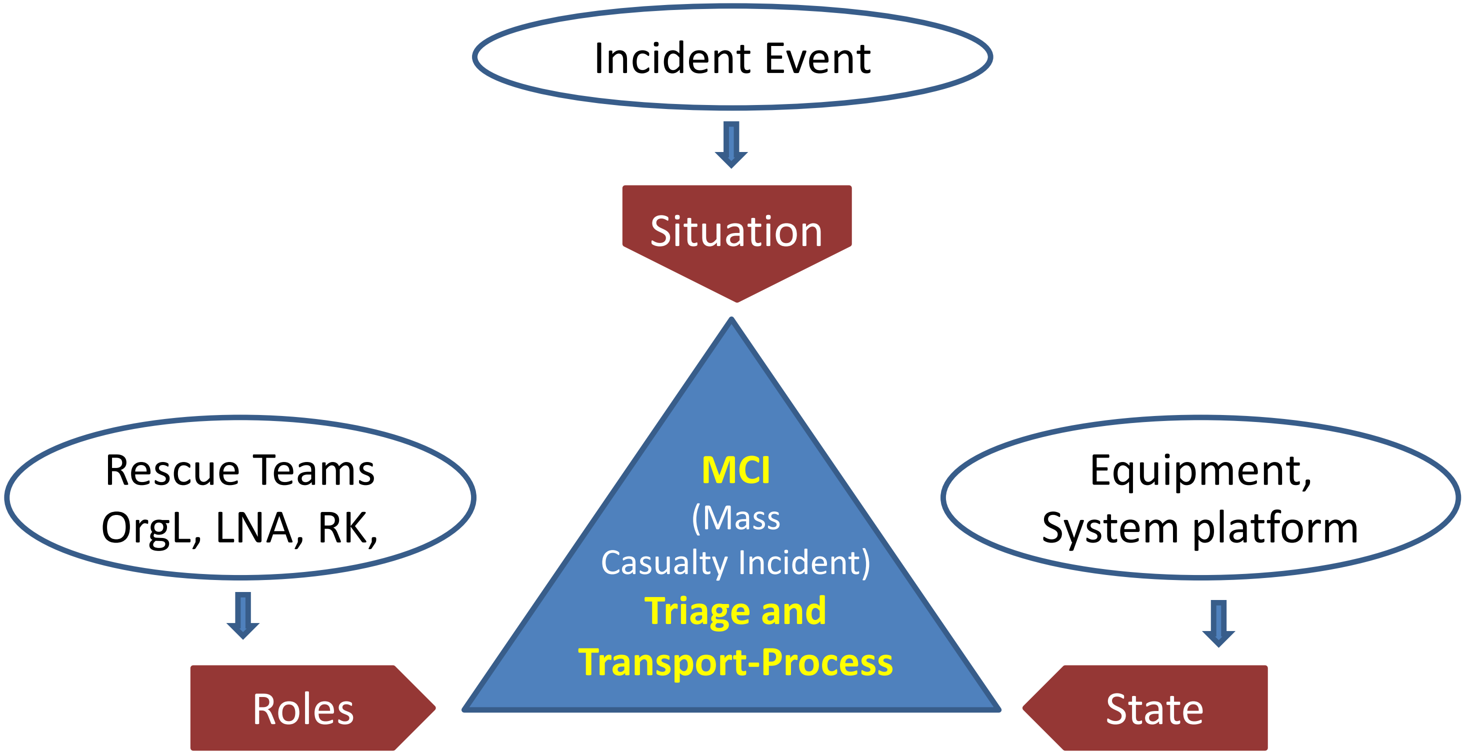
As security accompanied the development process (Security by evolution)



Source (modified): UniBw Munic

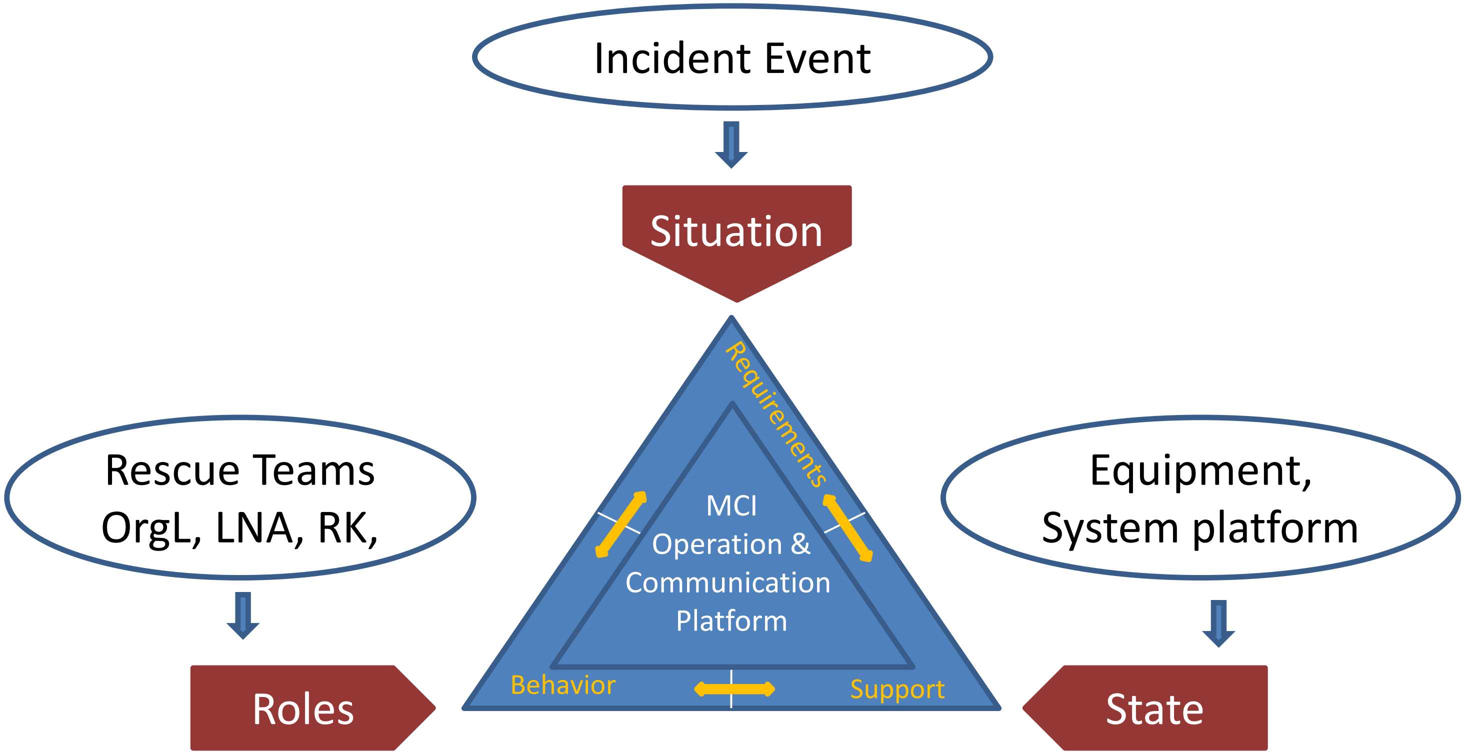
Bundesministerium
für Bildung
und Forschung

Basic Process Structure



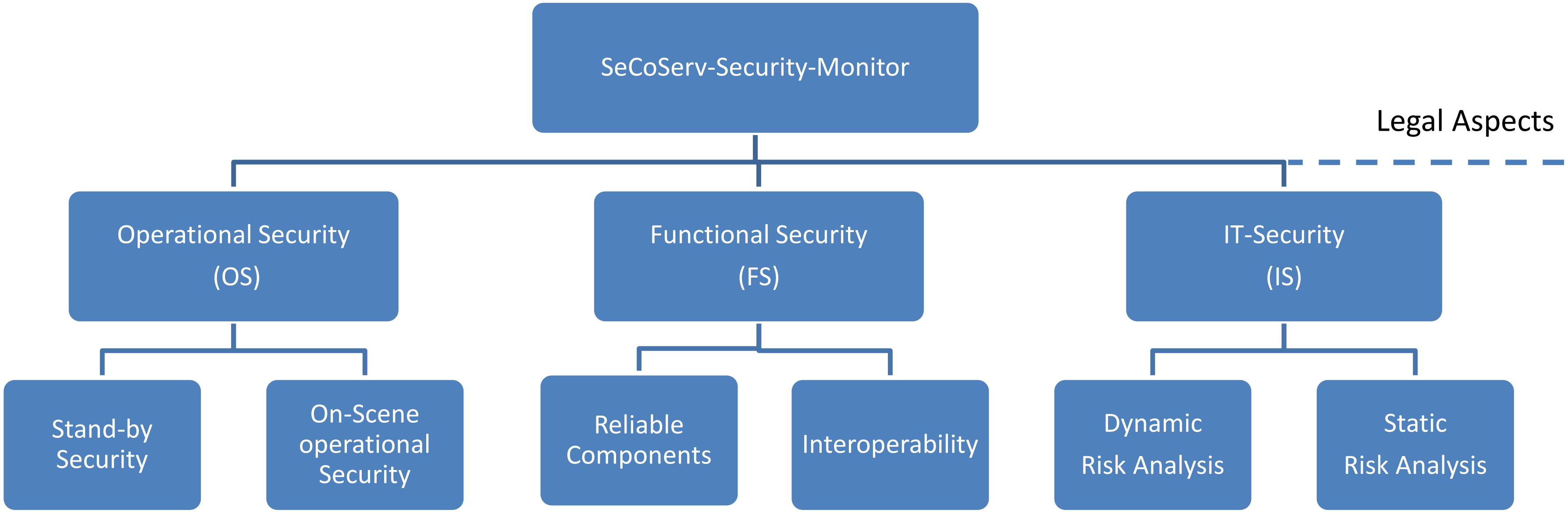
Bundesministerium
für Bildung
und Forschung

Basic Process Structure

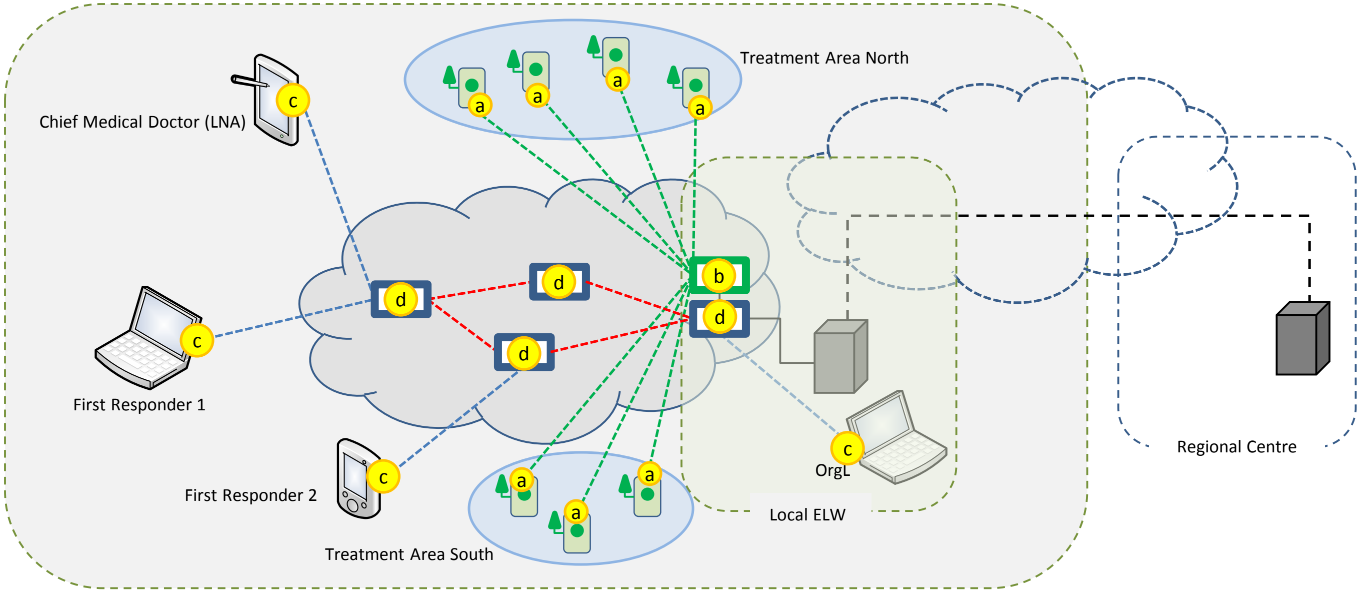


Bundesministerium
für Bildung
und Forschung

Monitoring Security



Types of Security Modules (Incident Area Network)



(a) SeCoTag-Security Interface

(b) SeCoTag-Receiver Security Interface

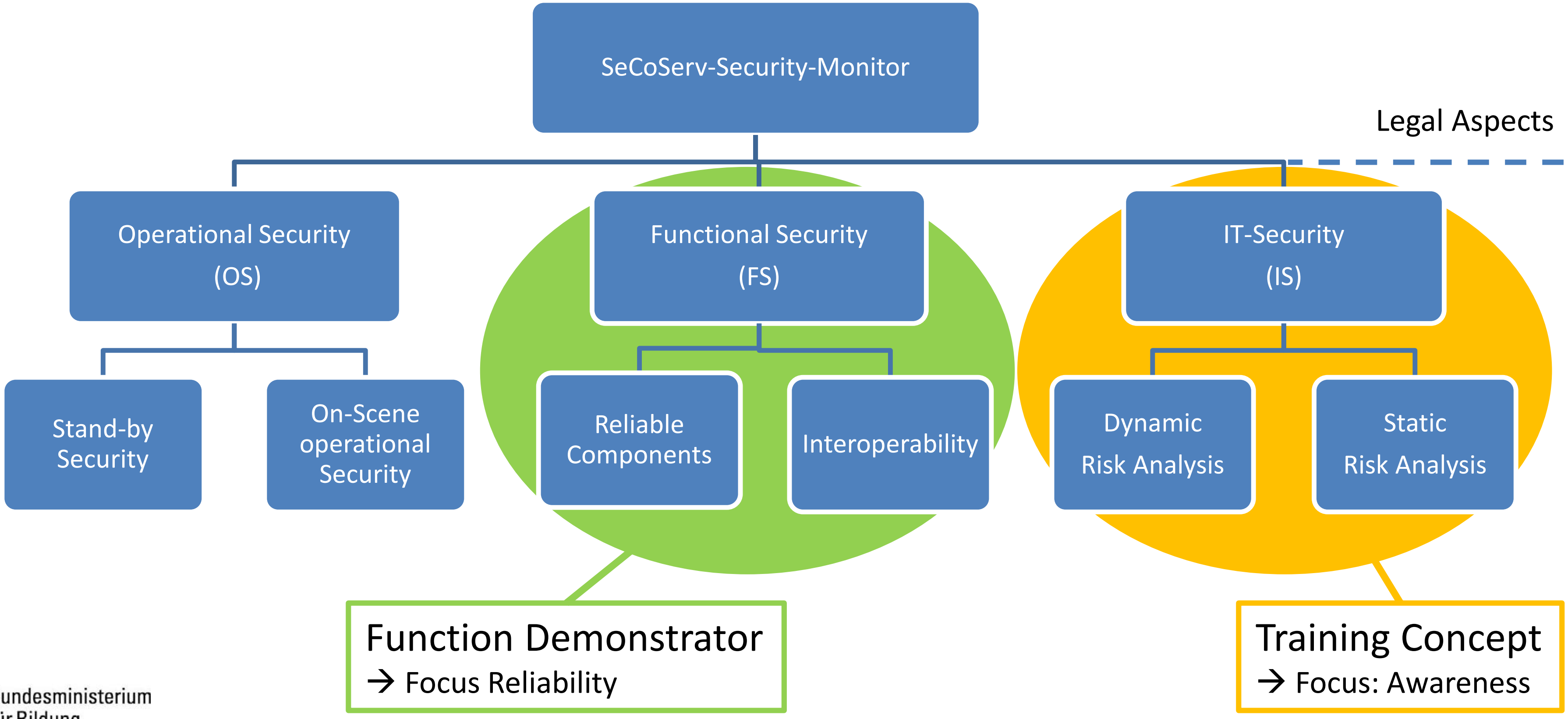
(c) Device Security Interface

(d) IAN-Mesh-Node-Security Interface

●	SeCoTag	🟩	SeCoTag-Receiver	🟦	IAN-Mesh-Node
-----	868 MHz	-----	IEEE 802.11a/b/g/n	-----	IEEE 802.11s

Bundesministerium
für Bildung
und Forschung

Monitoring Security



Function Demonstrator
→ Focus Reliability

Training Concept
→ Focus: Awareness

Bundesministerium
für Bildung
und Forschung

Electrical Power Supply as a functional Security Example

What could happen?

- Battery empty
- Generator break
- Local Power Net fails
- Blocked radio link
- …

!! Not unlikely, especially during a MCI

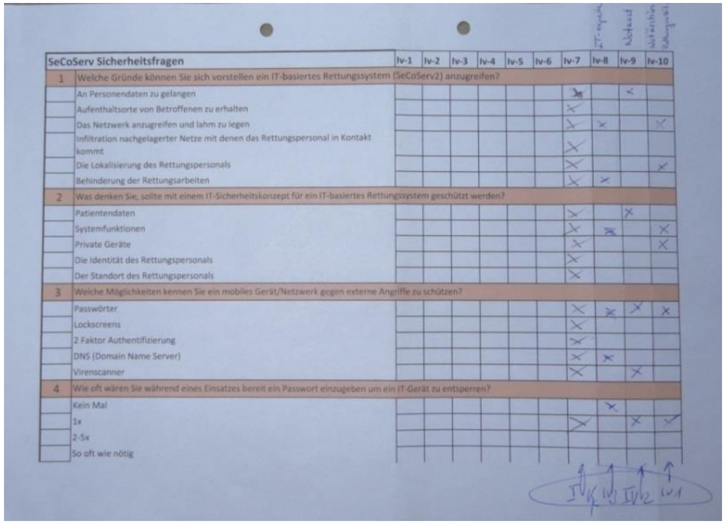
Demonstrator:

[http://www.humanquality.org/]

▶ But let's go for the Security Training Concept, first observing an MCI Field-Test - Video: MCI exercise Oelde

Positions of interviewees

→ The aim was to benefit from the large number of present rescue people and to create a state of opinion with a condensed questionnaire



									IT-Experte	Notarzt	Notärztin Rettungs[illegible]
SeCoServ Sicherheitsfragen		Iv-1	Iv-2	Iv-3	Iv-4	Iv-5	Iv-6	Iv-7	Iv-8	Iv-9	Iv-10
1	Welche Gründe können Sie sich vorstellen ein IT-basiertes Rettungssystem (SeCoServ2) anzugreifen?										
	An Personendaten zu gelangen							X		X	
	Aufenthaltsorte von Betroffenen zu erhalten							X			
	Das Netzwerk anzugreifen und lahm zu legen							X	X		X
	Infiltration nachgelagerter Netze mit denen das Rettungspersonal in Kontakt kommt							X			
	Die Lokalisierung des Rettungspersonals							X			X
	Behinderung der Rettungsarbeiten							X	X		
2	Was denken Sie, sollte mit einem IT-Sicherheitskonzept für ein IT-basiertes Rettungssystem geschützt werden?										
	Patientendaten							X		X	
	Systemfunktionen							X	X		X
	Private Geräte							X			X
	Die Identität des Rettungspersonals							X			
	Der Standort des Rettungspersonals							X			
3	Welche Möglichkeiten kennen Sie ein mobiles Gerät/Netzwerk gegen externe Angriffe zu schützen?										
	Passwörter							X	X	X	X
	Lockscreens							X			
	2 Faktor Authentifizierung							X			
	DNS (Domain Name Server)							X	X		
	Virenscanner							X		X	
4	Wie oft wären Sie während eines Einsatzes bereit ein Passwort einzugeben um ein IT-Gerät zu entsperren?										
	Kein Mal								X		
	1x							X		X	X
	2-5x										
	So oft wie nötig										

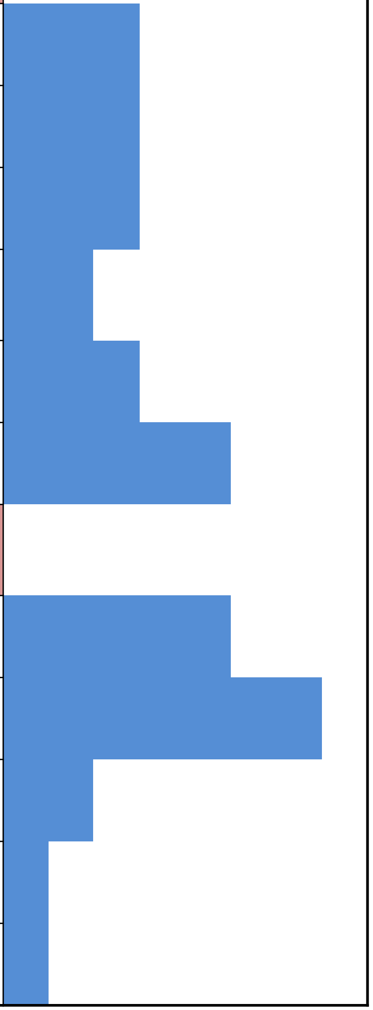
IV/4 IV/3 IV/2 IV/1

Emergency doctor
IT-Expert
Organization leader (decommissioned)
Strategic observer
Rescue assistant
Paramedic

→ *The following survey is not intended as a statistically significant measure, but rather it is a very good first impression on the problems of the situation concerning IT-Security*

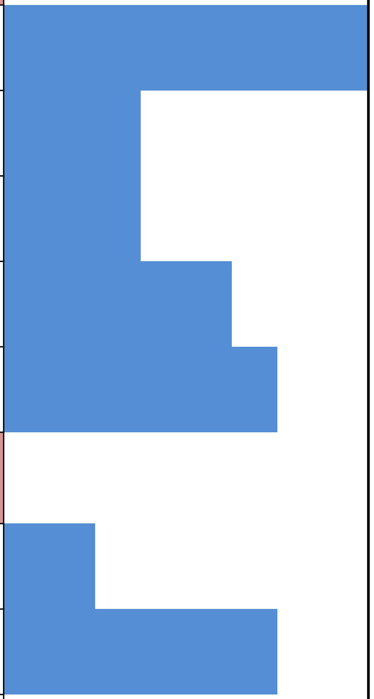
Questionnaire (1)

1	Which reasons can you imagine in order to attack an IT-based rescue system like SeCoServ2 ?	%
	Gain access to personal data	37,5
	Obtain whereabouts of the person concerned	37,5
	Attack and paralyze the network	37,5
	Infiltration downstream networks with which the rescue workers to come into contact	25,0
	The localization of the emergency personnel	37,5
	Obstruction of rescue work	62,5
2	What do you think should be protected with an IT security concept in an IT-based rescue system?	%
	Patient information	62,5
	System functions	87,5
	Private facilities/equipment	25,0
	The identity of the rescue personnel	12,5
	The location of the emergency personnel	12,5



Questionnaire (2)

3	What options do you know, to protect a mobile device / network against external attacks?	%
	Passwords	100,0
	Lockscreens	37,5
	2-factor authentication	37,5
	DNS (Domain Name Server)	62,5
	Antivirus software	75,0
4	**How often would you accept to enter a password during an operation to unlock an IT device?**	**%**
	No times	25,0
	1x	75,0
	2x	0,0
	As often as necessary	0,0

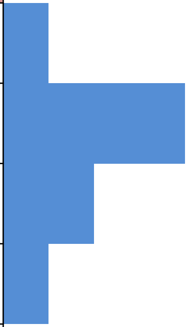


Questionnaire (3)

5	Is there in your opinion a time delay caused by IT security measures that is acceptable before triage of patient?	%
	No	0,0
	0-2 seconds	62,5
	2-5 seconds	37,5
	5-10 seconds	25,0
	>10 seconds	0,0
6	**How much time do you use in total after arriving on scene in order to exclude natural hazards? (e.g. gas leaks, etc.)**	**%**
	No time	0,0
	10-15 seconds	0,0
	15-60 seconds	62,5
	1-3 minutes	12,5
	>3 minutes	25,0

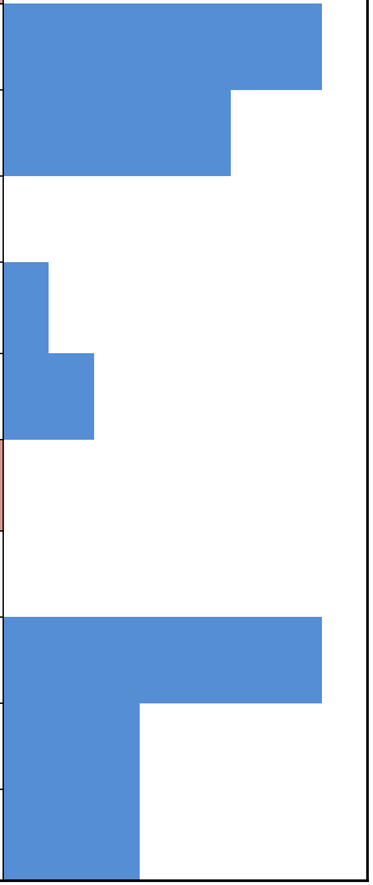
Questionnaire (4)

7	How severe do you assess the effects of the absence of security issues?	**Averg.**
	(1 not severe, 10 extremely severe)	
	For ordinary safety aspects (1-10)	8,75
	For IT-related security issues (1-10)	5,25
8	Would you change your answer to question 5 in consideration of questions 6 and 7?	**%**
	No time	12,5
	10-15 seconds	50,0
	15-60 seconds	25,0
	1-3 minutes	12,5
	>3 minutes	0,0



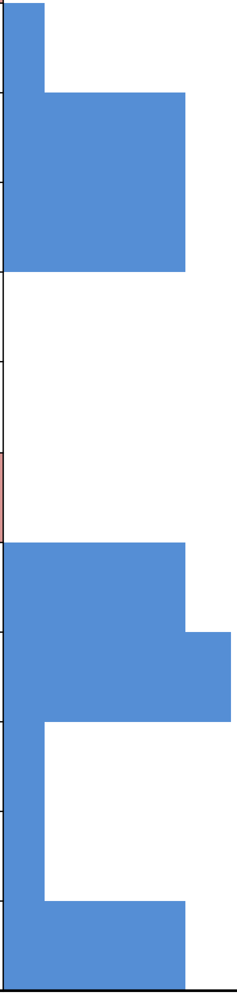
Questionnaire (5)

9	How do you protect personal belongings (mobile phone, purse, ..) during a rescue operation?	%
	I do not take them with for use	87,5
	I always wear them on the body	62,5
	I don't protect them at all	0,0
	The objects are unprotected once I remove the clothes in which I keep them	12,5
	I keep them locked in the command vehicle	25,0
10	**How do you protect prescription drugs / expensive rescue equipment during a mission?**	**%**
	Not at all	0,0
	We keep them / it under lock and key	87,5
	It remains in the rescue cars	37,5
	We have a designated person who is taking care of the those	37,5



Questionnaire (6)

11	How often would you be willing to participate in a regular IT security training?	%
	Not at all, please do no regular training	12,5
	Please only one (additional) training per year	50,0
	Twice per year one hour	50,0
	1/2 hour per month shall be sufficient	0,0
	1 hour per month. It is indeed also an IT security training for home	0,0
12	What should be practiced in an IT security training, what should be the focus?	%
	To protect patient data	50,0
	Keep SeCoServ2 system functions upright	62,5
	Personal safety aspects	12,5
	IT security for home use	12,5
	Time saving	50,0



Conclusion - Basic Principal

- The goal of SeCoServ2 and follow up activities is, to give emergency personnel an IT security concept at hand, which protects them in its primary activity, saving lives, but does not interfere with their implicit responsibility for downstream aspects related to the privacy of patients.
- It is not to hinder or disturb the rescue flow, but to avoid that victim/patient data can be accessed or tampered/manipulated during the rescue process by unauthorized persons.

Conclusion - Next steps

- To develop an IT-security table evaluation tool adapted to rescue scenarios ranging from small incidents to MCIs.
- Designing an IT-Security Training offer respecting conditions like question 11.
- Expending our consulting expertise in functional Security focusing on mobile rescue infrastructures.
- Taking Early Warning Systems for Public into account (the digital society continues maturing, IoT, Big data, data privacy will change, …).

SeCoServ2

THANKS‘
FOR LISTENING