



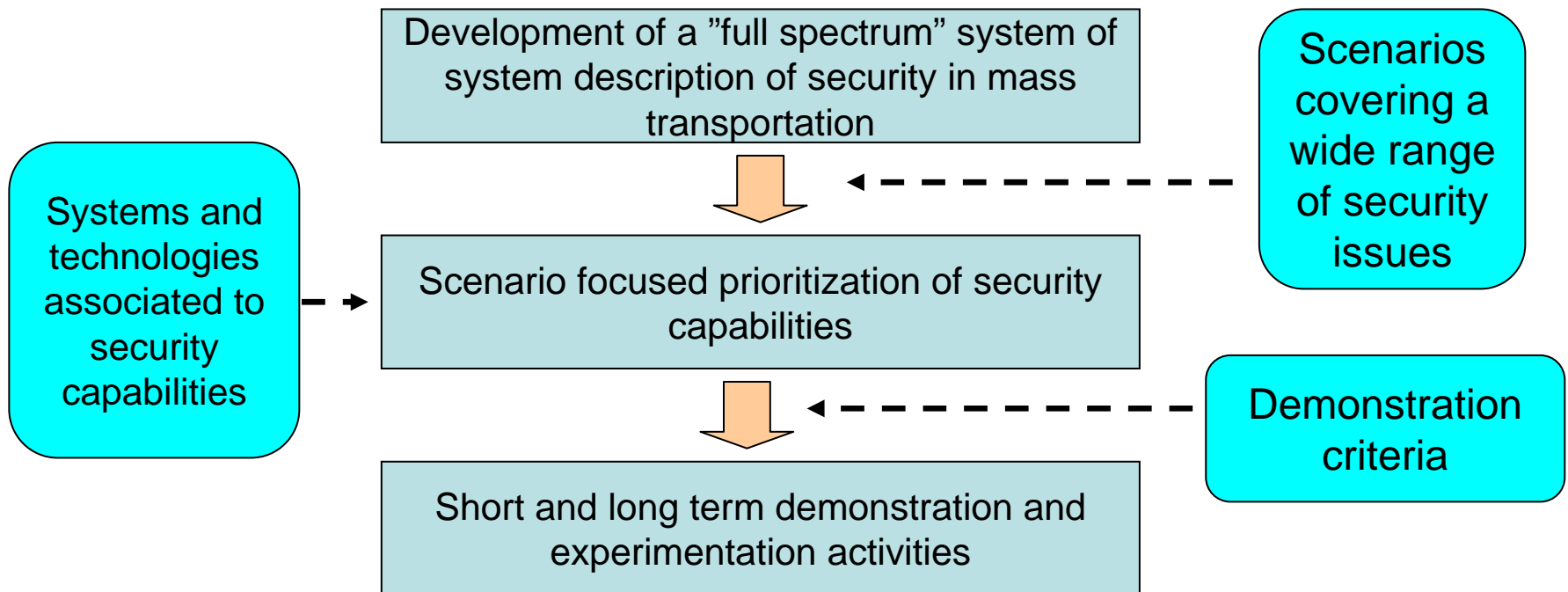
# Roadmap for Experimentation and Demonstration Mass Transport Security

DEMASST Presentation at Final Forum to  
discuss the preliminary roadmap

Bruxelles 28 April 2010

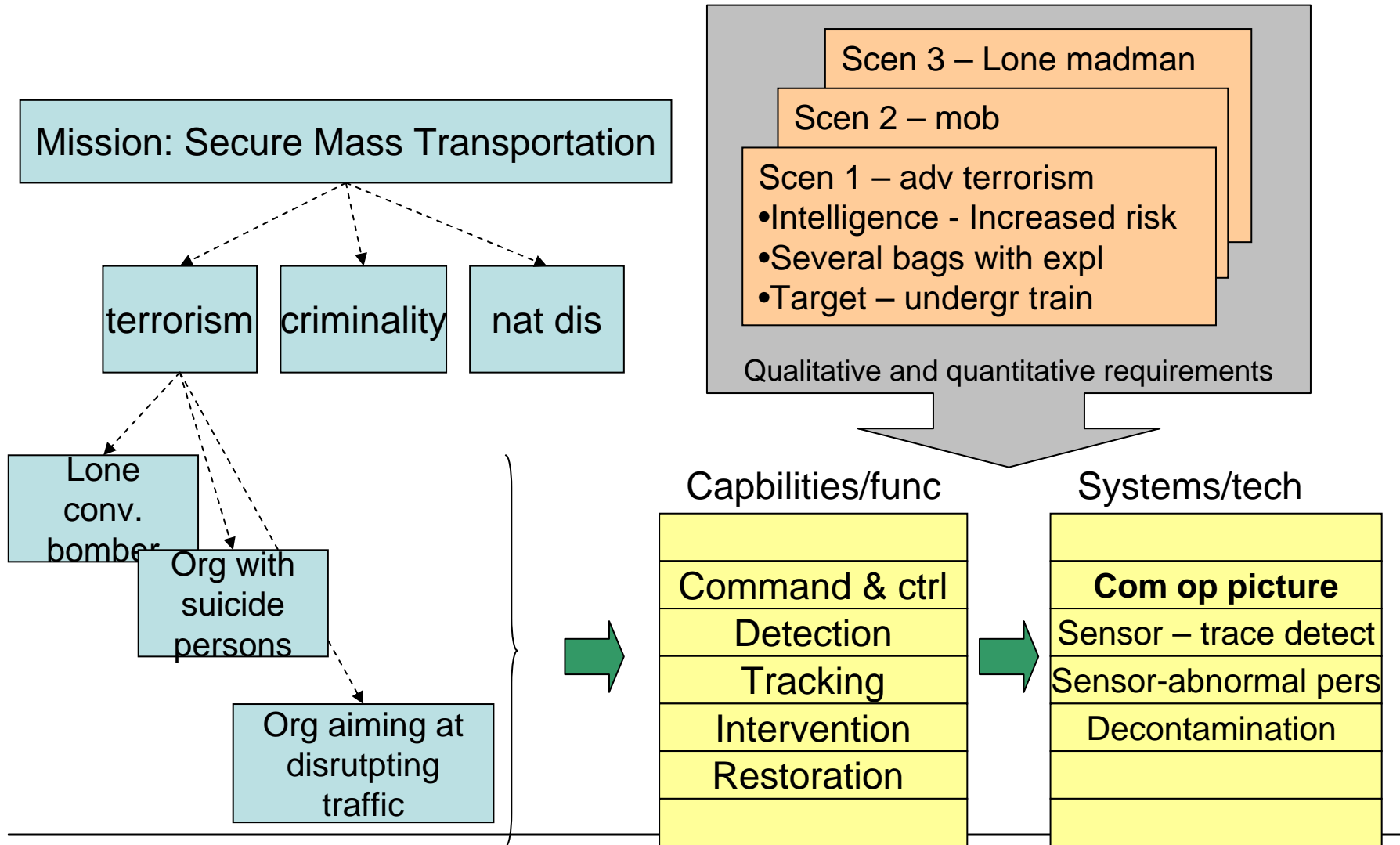
Dr S. Holmberg, FOI  
DEMASST  
[demasst@foi.se](mailto:demasst@foi.se)

# Principal method in development of the roadmap



The roadmap draws on information from all Work Packages in DEMASST

# Method – prioritization of capabilities



# “Capabilities”

**1 Internal security management systems and procedures**

**2 External security guidelines**

**3 Risk assessment-based command and control capabilities**

**4 Interoperability and information interfaces**

**5 Intelligence capabilities**

**6 Learning and training capabilities**

**7 Threat identification and detection capabilities**

**7b Tracking and identification**

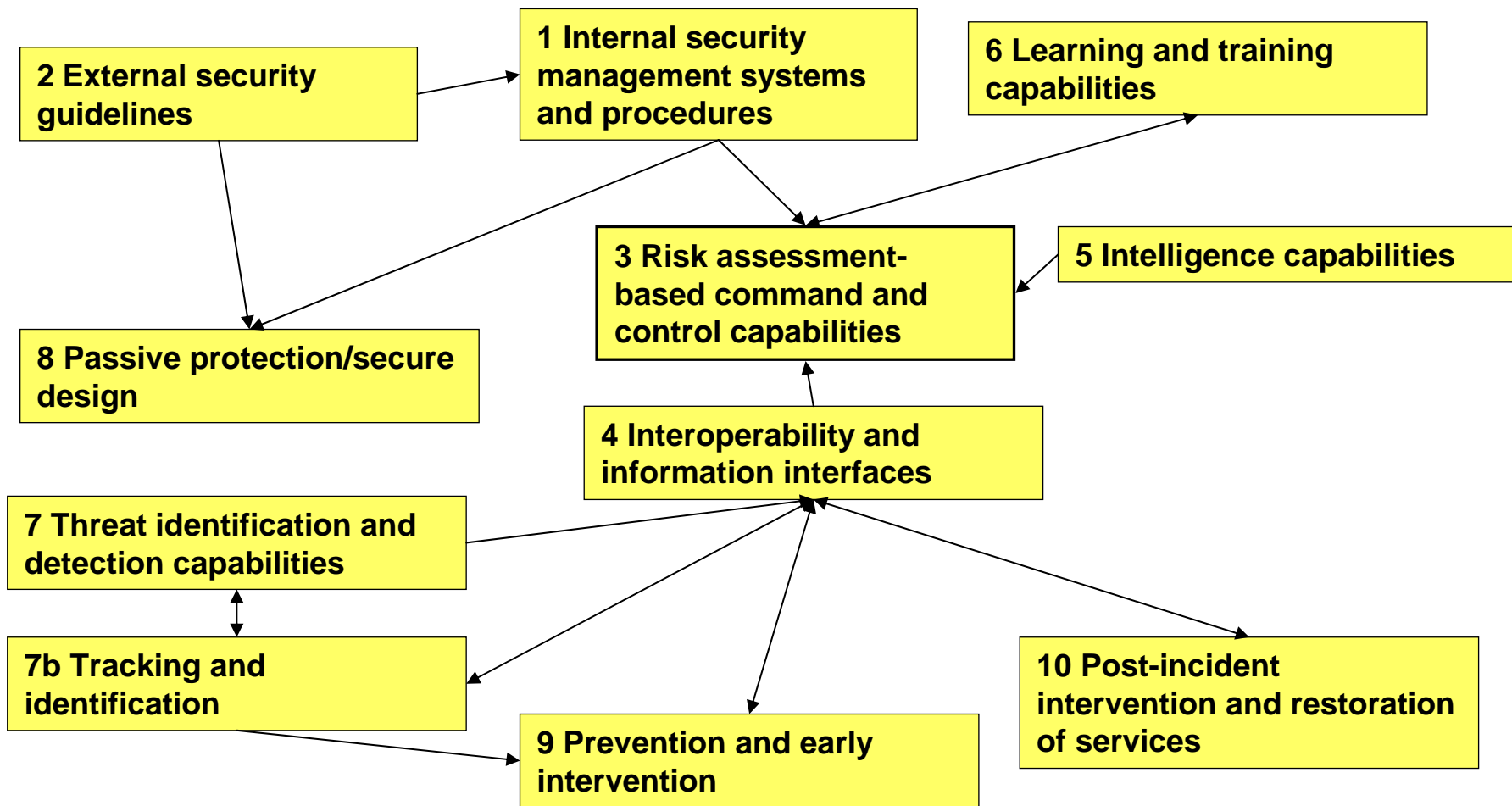
**8 Passive protection/secure design**

**9 Prevention and early intervention**

**10 Post-incident intervention and restoration of services**

- The set of capabilities cover all security issues
- The set could have a different phrasing depending on focus of work

# Relations between Capabilities



# “Sub Capabilities”

**1 Internal security management systems and procedures**

**2 External security guidelines**

**3 Risk assessment-based command and control capabilities**

**4 Interoperability and information interfaces**

**5 Intelligence capabilities**

**6 Learning and training capabilities**

**7 Threat identification and detection capabilities**

**7b Tracking and identification**

**8 Passive protection/secure design**

**9 Prevention and early intervention**

**10 Post-incident intervention and restoration of services**

- Scenario-based prediction tools
- “Common operating picture for all relevant stakeholders
- Procedures for preventive actions based on internal intelligence or data
- Real time management of crowds
- Simulation tool to simulate security events and identify lack of security
- Optimal design of security control centre

- Detection and identification of strange/left behind objects
- Detection/identification of abnormal behaviour by persons or crowds
- Detection/identification of CBRN devices
- Detection/identification of explosive devices
- Detection/identification of unauthorized physical access to parts of the transport system
- Detection/identification of intrusion attempts and abnormal activity on ICT system
- Detection/identification of electronic threats
- Detection/identification of fire/smoke
- Detection/identification of natural hazards
- Biometric identification of passengers

# Some capabilities not suitable for demonstration

Capability (need)
<b>Internal security management systems and procedures</b>
Security culture and planning
Clear procedures and responsibilities for transport security
Plans/procedures for rapid evacuation
<b>External security guidelines</b>
Standards and guidelines for minimum security levels
<b>Learning and training capabilities</b>
Realistic/real-time exercises on security incidents
Training of staff to recognize threats
<b>Passive protection/secure design</b>
Guidelines/standards for secure (incl. evac) and resilient architecture

...but still of great value for security

# Capabilities and sub capabilities

## 1 Internal security management systems and procedures

- Security culture and planning
- Clear procedures and responsibilities for transport security
- Dedicated human resources for transport security
- Emergency plans and procedures for security
- Plans/procedures for rapid evacuation
- Alternate travel solutions plans
- Risk relocation plans and models

## 2 External security guidelines

- European rules and directives for mass transportation security
- Standards and guidelines for minimum security levels

## 3 Risk assessment-based command and control capabilities

- Scenario-based prediction tools
- "Common operating picture" tools, for all relevant stakeholders
- Procedures for preventive actions based on internal (intelligence? Eller ny subfunk?) data
- Real time management of crowds (fd syst)
- Simulation tool to simulate security events and

## 5 Intelligence capabilities

- Coordination with external intelligence service
- Data collection and analysis
- Procedures/systems for preventive actions based on external intelligence
- Threat assessment based on background intelligence

## 4 Interoperability and information interfaces

- Adaptive communication in fast changing environment
- Communication with first responders and other stakeholders
- Communication with passengers
- Solutions for communication and vision without power/low visibility
- Secure systems for coordination with external intelligence services
- Situational picture for single stakeholder or situational awareness

- Tabletop/discussion based exercises on security incidents
- Realistic/real-time exercises on security incidents
- Training of staff to recognize threats
- Training of passengers to manage threats/incidents
- Crisis management- staff training
- Security event simulations

## 7b Tracking and identification

- Tracking of people and objects (vehicle)
- Biometric identification of passengers

## 9 Prevention and early intervention

- Staff monitoring
- Flexible intervention solutions, to isolate and/or neutralize attacks
- Way around tools to track (steer?) the individual till safe locations to intervene
- Way to neutralize suspect objects
- Fast inspection of non-cooperative passengers
- Non-lethal weapons for use against identified attackers

## 7 Threat identification and detection capabilities

- Detection and identification of strange/left behind objects
- Detection/identification of abnormal behaviour by persons or crowds
- Detection/identification of CBRN means and devices
- Detection/identification of explosive means and devices
- Detection/identification of unauthorized physical access to parts of the transport system
- Detection/identification of intrusion attempts and abnormal activity on ICT system
- Detection/identification of electronic threats/hazards
- Detection/identification of fire/smoke
- Detection/identification of natural hazards
- Biometric identification of passengers

## 8 Passive protection/secure design

- Guidelines/standards for secure and resilient infrastructure
- Blast-proof infrastructure and objects
- Fire proof infrastructure and objects

## 10 Post-incident intervention and restoration of services

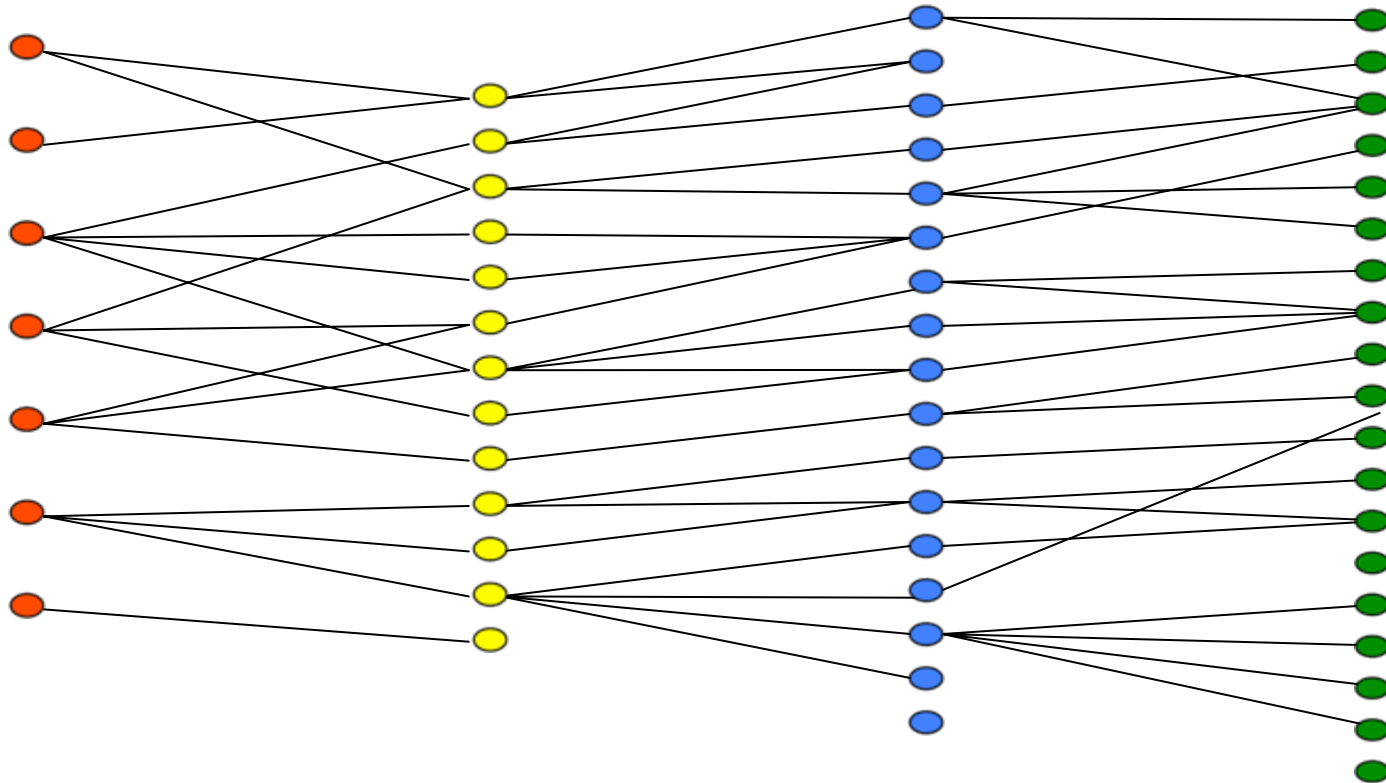
- Event proof evidence collection (black box like)
- Forensics procedures
- Emergency habitats
- Decontamination measure and facilities
- Solutions to help protect the driver and passengers
- Victims tagging and follow up
- Medical countermeasures

Missions /  
Objectives

Capabilities

Systems

Technologies



# Capabilities and systems

**1 Internal security management systems and procedures**

**2 External security guidelines**

**3 Risk assessment-based command and control capabilities**

**4 Interoperability and information interfaces**

**5 Intelligence capabilities**

**6 Learning and training capabilities**

**7 Threat identification and detection capabilities**

**7b Tracking and identification**

**8 Passive protection/secure design**

**9 Prevention and early intervention**

**10 Post-incident intervention and restoration of services**

One example is  
sensors

## Sensors

- Sensors to detect explosives
- Sensors to detect chemical
- Sensors to detect biological agents
- Sensors to detect radioactivity
- Mobile identification systems
- Multi sensor system, recording, power loss

# Systems and technologies

## Sensors

- Sensors to detect explosives
- Sensors to detect chemical
- Sensors to detect biological agents
- Sensors to detect radioactivity
- Mobile identification systems
- Multi sensor system, recording, power loss

19: Biometric identification of suspect within crowds and of staff

23: Luminescent sensors based on nanotechnologies

21: DNA identification of/for staff

1: mm-wave technology

13: Mobile sensing devices

15: Mobile x-imaging

18: THz and RQN scanners

20: Chemical contamination imaging in real time; LIDAR, surface analysis by LIBS for chemical toxics

4: Radiological contamination imaging for fast contamination mapping

# TRL – Technological Readiness Level

Technology Readiness Level	
1. Basic principles observed and reported	}
2. Technology concept and/or application formulated	
3. Analytical and experimental critical function and/or characteristic proof of concept	
4. Component and/or breadboard validation in laboratory environment	}
5. Component and/or breadboard validation in relevant environment	
6. System/subsystem model or prototype demonstration in a relevant environment	}
7. System prototype demonstration in an operational environment	
8. Actual system completed and 'flight qualified' through test and demonstration	}
9. Actual system 'flight proven' through successful mission operations	

- TRL only an indication of time to proven system
- Some flexibility in TRL estimations – linked to performance

# Evaluation against scenarios - examples

Capability	"bomb" scenario	Hooligans	Mentally deranged person
1 Internal security management systems and procedures	3	3	3
2 External security guidelines	1	1	1
3 Risk assessment-based command and control capabilities	3	3	3
4 Interoperability and information interfaces	3	2	2
5 Intelligence capabilities	3	2	1
6 Learning and training capabilities	2	2	2
7 Threat identification and detection capabilities	3	1	3
7b Tracking and identification	3	2	3
8 Passive protection/secure design	3	1	1
9 Prevention and early intervention	3	3	3
10 Post-incident intervention and restoration of services	3	1	1

# C2 – Common Operational Picture

- Fusion of information
  - From sensor data
  - From Intelligence system
  - From the personnel
  - ...
- Man machine interface
  - Alarm characterization system
  - Adaptable content in operational picture depending on user requirement
- Information sharing system

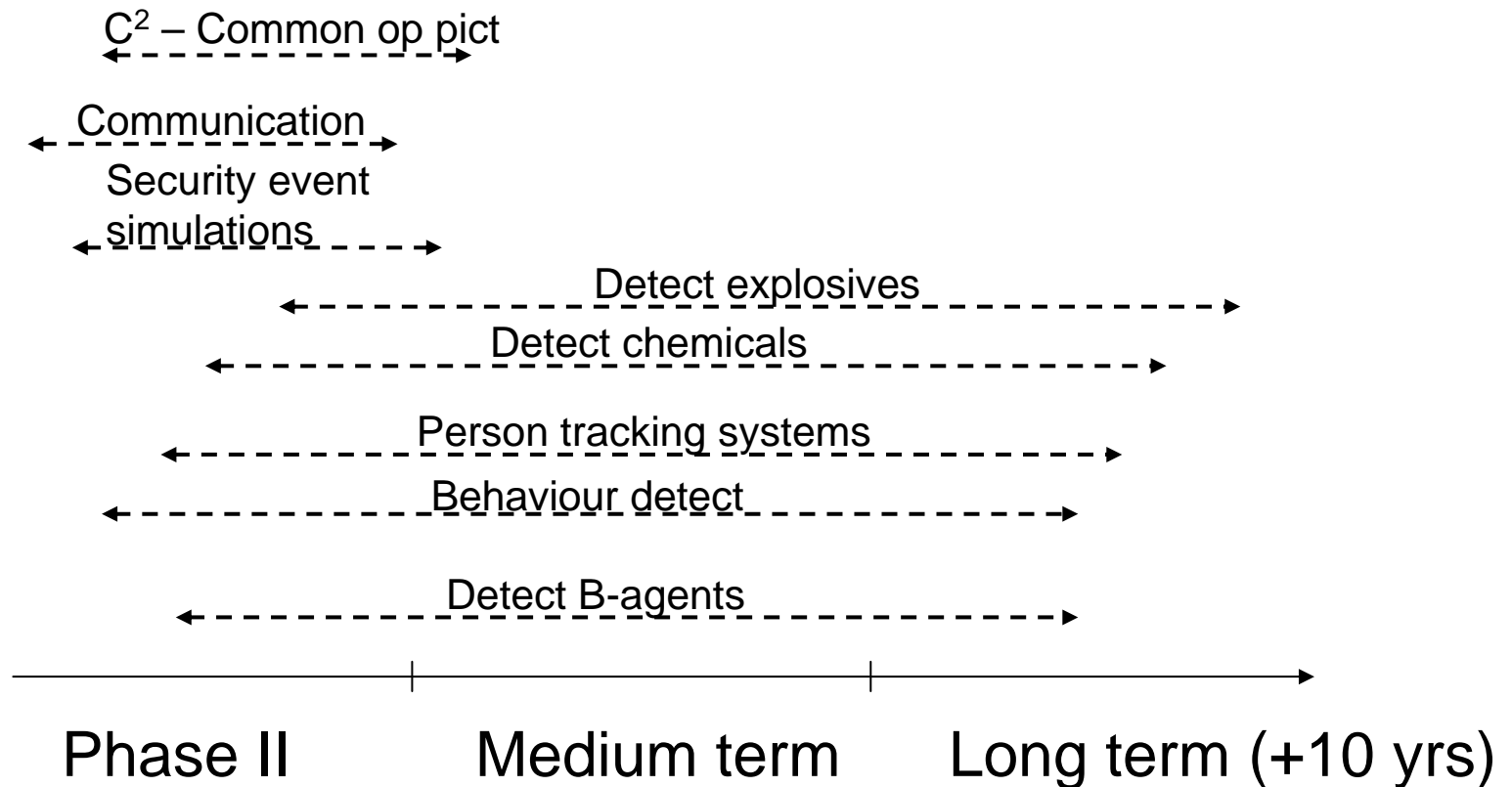
# Preliminary candidates for demonstrations and experimentation

	Increased security	TRL	affordable	disturbing
<b>3 Risk assessment-based command and control capabilities</b>				
5: Tools for simulation of substance	2	high	ok	no
6a Common operational picture tools	3	med	ok	no
6b Systems for risk analysis	2	med	ok	no
11: Simulation systems of human (passenger) behaviour	1	med	ok	no
<b>4 Interoperability and information interfaces</b>				
8: communication	3	high	ok*	no
<b>7 Threat identification and detection capabilities</b>				
2: Sensors (substance detection)				
Sensor to detect explosives	3	low	no	no*
Sensors to detect chemical agents	3	low*	ok*	no
Sensors to detect RN	1	high	ok	no
Sensor for biological agents	2	low*	no*	no
3a: systems for tracking	3	low	ok	integ
3b: behaviour detection systems	2	med	ok	integ
4: Vehicle – surveillance and detection systems	1	med	ok	integ
9: Localization and coordination systems	2	med	no?	no

# Preliminary candidates for demonstrations and experimentation

	Increased security	TRL	affordable	disturbing
<b>7b Tracking and identification</b>				
3a: systems for tracking	3	low	ok	integ
<b>9 Prevention and early intervention</b>				
2: Sensors_A				
Sensor to detect explosives	3?	low	no	no
Sensors to detect chemical agents	3?	low*	ok	no
Sensors to detect RN	1	high	ok	no
Sensor for biological agents	2	low*	n/a	no
3a: systems for tracking	3	med	ok	no
9: Localization and coordination systems	2	med	no?	no
<b>10 Post-incident intervention and restoration of services</b>				
2: Sensors				
Sensors to detect chemical agents	3	2	ok	no
Sensors to detect RN	2	high	ok	no
Sensor for biological agents	2	low	n/a	no
1: first aid	2	low?	ok?	no
10: Damage mitigation systems, decontamination	3	med	ok?	no

# Candidates for demonstrations and experimentation



# Demonstrations in a more demanding context - Large crowd management

- Basically a variant of general detection, tracking, intervention, probably less challenging.
- Two large crowds, showing aggressive behaviour move through the system.
- Cameras, acoustic sensors, observations used to track the crowds.
- Intervention is to redirect passenger flow and keep the two crowds separated, through closing of certain passages etc.

Near time perspective

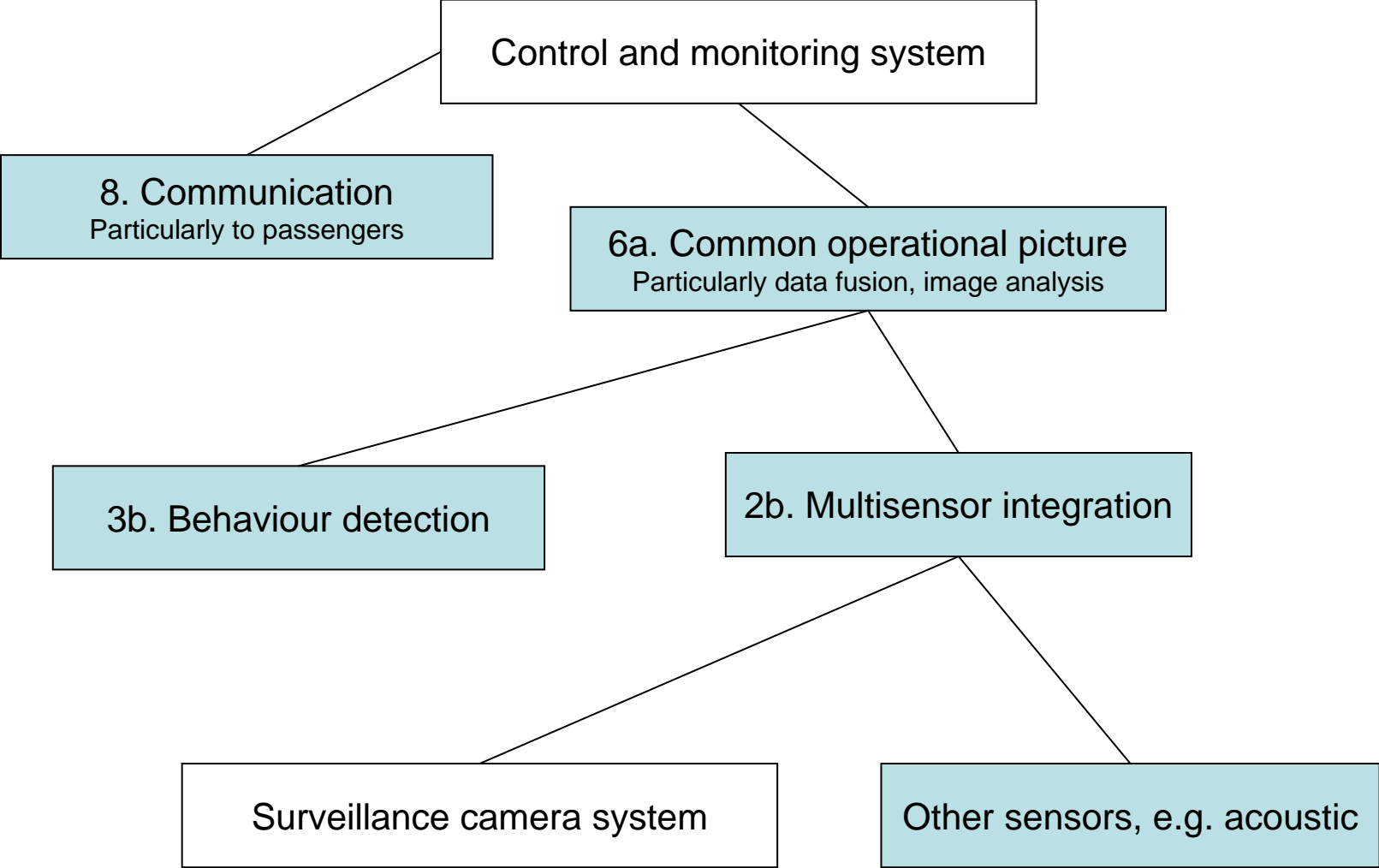
Detect

Localise, track

Intervene

**(Existing system)**

**(Demo system)**



# Some conclusions

- Maturity gaps for many attractive candidate solution - Several technologies like the detection of human behaviour are too immature to be used for threat detection on a regular basis today.
- Associated with proper procedures e.g. command and control, such technologies are nevertheless relevant for demonstration and experimentation with a more limited scope and will improve security during phase II.
- Some of the immature technologies correspond to important security needs and RTD must be pursued
- The phase II activities and the associated stakeholder communities will be a unique source of requirements for such parallel and subsequent RTD activities
- See the research and innovation infrastructure developed in phase II as an asset also for the future
- Don't see phase II as the ultimate step towards MT security