

# Challenges and approaches to enhance security of CNS/ATM systems – the researcher's view

T. H. Stelkens-Kobsch, German Aerospace Center (DLR)

Engage Thematic Workshop – Vulnerabilities and Global Security of the CNS/ATM systems



Knowledge for Tomorrow



## Russian hackers penetrate US power stations

© 24 July 2018



## It's Scarily Easy To Hack A Traffic Light



Kristen Lee  
8/16/16 8:50am • Filed to: HACKING ✓



## Car hacking remains a very real threat as self-driving cars become more common

67 3

Progress in protecting vehicles from cyber attacks is real and could get increasingly serious in the future as cars start talking to each other.

# Report: Air traffic control system vulnerable to cyberattack

By Aaron Cooper

Updated 1954 GMT (0354 HKT) March 2, 2015

cnn.com

targeting a uranium enrichment plant in Iran, according to a report from the International Atomic Energy Agency (IAEA). How did the hackers proceed? What were their intentions? What means of protection exist today for industrial sites? Here is an overview of this case study in cyber-security.

www.sentryo.net

## Nearly half of UK manufacturers hit by cyber attacks

Nearly half of UK manufacturers have been hit by a cyber security incident, according to a report by an industry organisation, which calls for greater government focus on the specific security needs of the sector

www.computerweekly.com



Model cars run in a city miniature at the Elektrobit booth to show how software for highly automated driving works during CES 2018 on January 9, 2018 in Las Vegas, Nevada. Alex Wong, Getty Images

eu.usatoday.com



# Holistic Approach to Controls

## Operation of ICT Systems

- Systems isolated
- Network security
- Backups
- Change mgmt

## Organisation, Culture & Management

- Clear roles & Responsibilities
- Risks managed

## Technical Mechanisms & Infrastructure

- Access control – networks, OS, applications, user mgmt.

## Compliance

- Legal, Policy, Standards

## Monitoring & Audit

- Logging
- Audits

## Human Resources

- Training
- Vetting

## Physical & Environmental Security

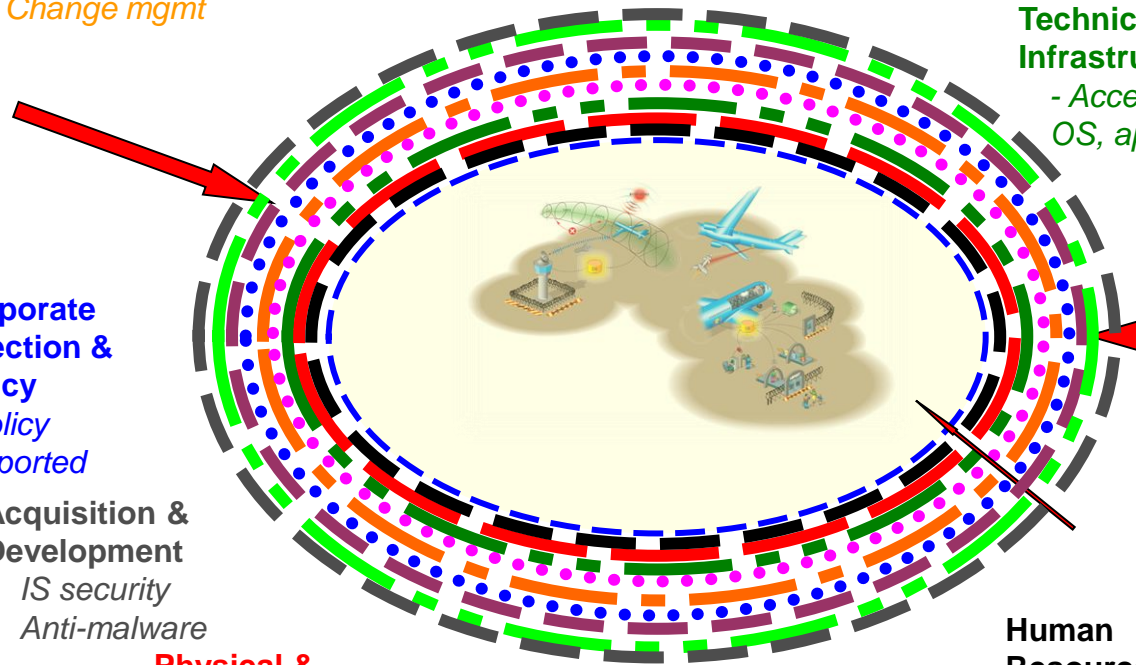
- Secure perimeter
- Equipment maintenance
- ...

## Corporate Direction & Policy

- Policy supported

## Acquisition & Development

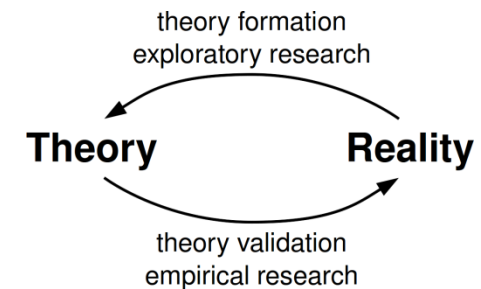
- IS security
- Anti-malware



*If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.* Bruce Schneier

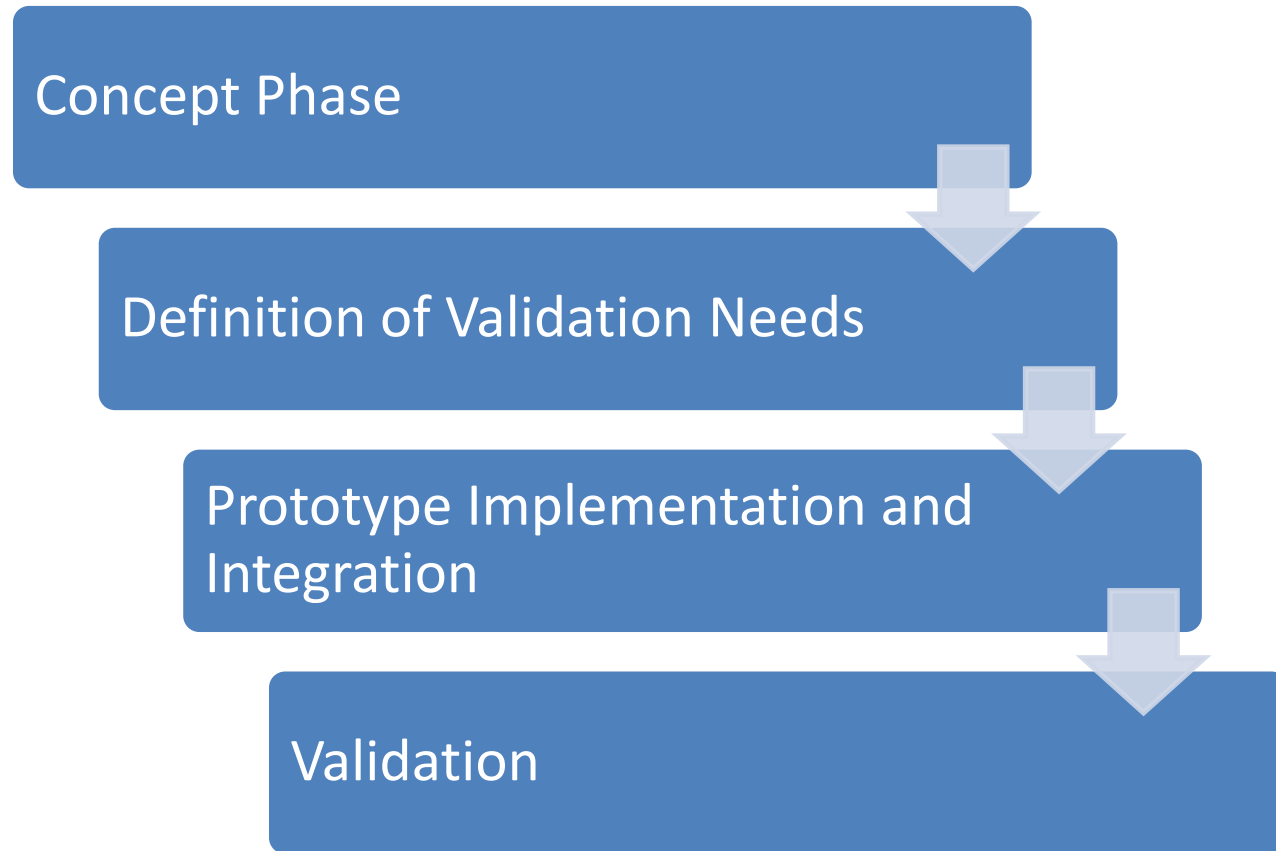
# Context establishment for validations

- Validations in aviation originally were dedicated to questions of airworthiness of aircraft and certificates.
- Validations widely used in research and industry (Banking, aviation, software, microelectronics, nuclear power, ...).
- Validations applied in nearly all areas of life.
- Several validation methodologies have been developed (V-model, OCVSD, ...).





# Global Objective: to demonstrate the improvement in security management in case of security incidents



# GAMMA Project

- FP7 Project, 2013-2017, 15 Mio. €, 19 European partners

<http://www.gamma-project.eu/>

- Goals:
  - Develop solutions to emerging air traffic management vulnerabilities backed up by practical proposals for the implementation of these solutions (prototypes).
  - Develop a complete ATM Security Management Concept.
  - Develop a validation methodology and conduct trials (single & integrated).
- Publications:
  - 34th DASC Prague, ICNS 2016, ARES 2016, CogInfoCom 2016, DLRK 2016, 35th DASC Sacramento, AESS Magazine, DLRK 2017, 36th DASC St. Petersburg, CEAS Aeronautical Journal, 37th DASC London ...

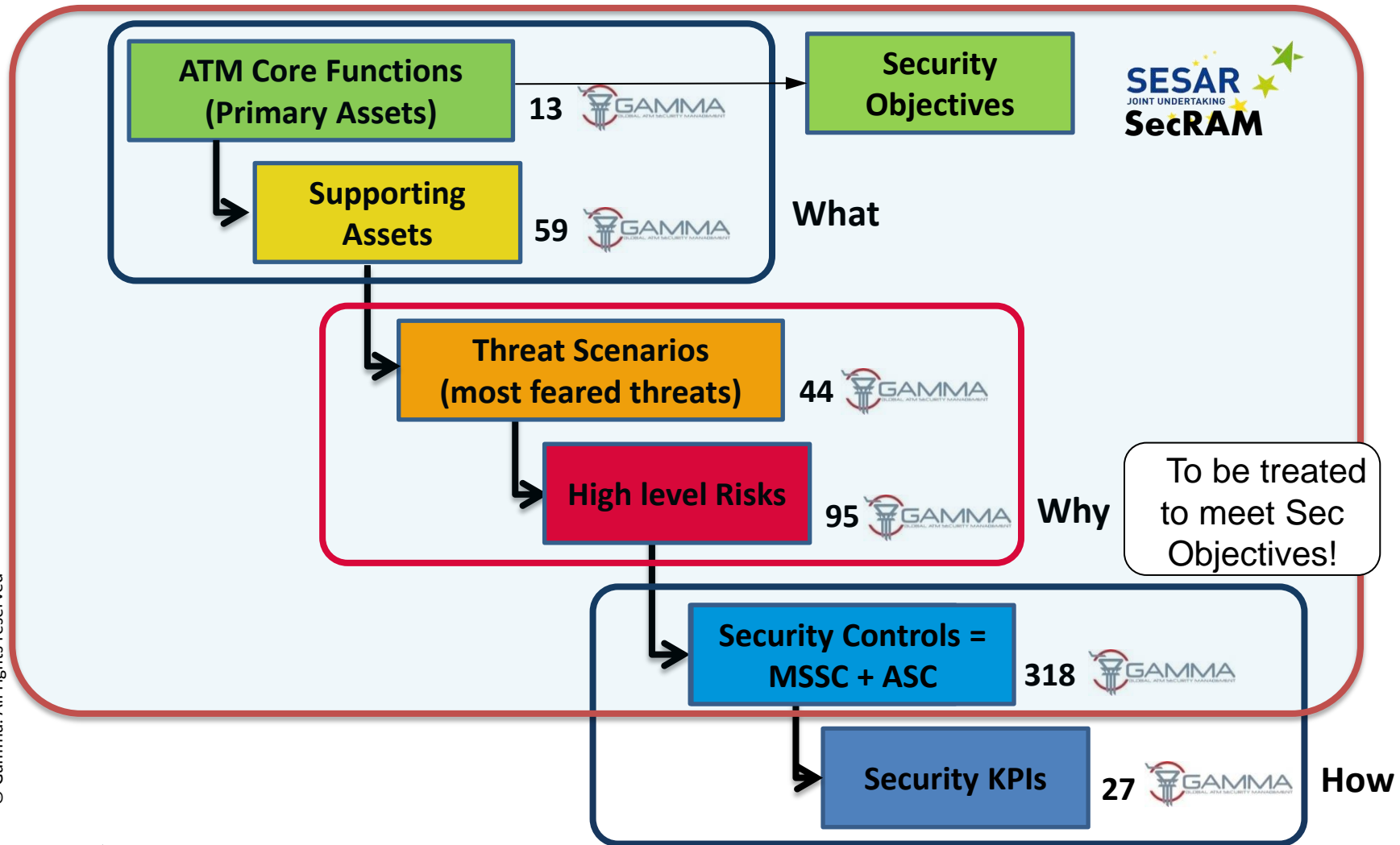


# GAMMA - Security Risk Assessment - Summary

- Security is not a fundamentally new problem.
  - Understanding of ATM Security as a component of Aviation Security has matured over the last 15 years.
  - ATM System is undergoing a fundamental transformation (new technologies, new concepts of operations).
  - While SESAR and NextGen used to address security on a transversal system engineering level (i.e. security risk assessment), the development of security solutions is minimal, and deployment activities / opportunities are not used.
  - GAMMA addressed this void!
- 
- ➔ Structured security risk assessment process building on SESAR.
  - ➔ Security solution prototype development and targeted validation.
  - ➔ Security Function a fundamental enabler for security management.



# Security Risk Assessment and Treatment in GAMMA

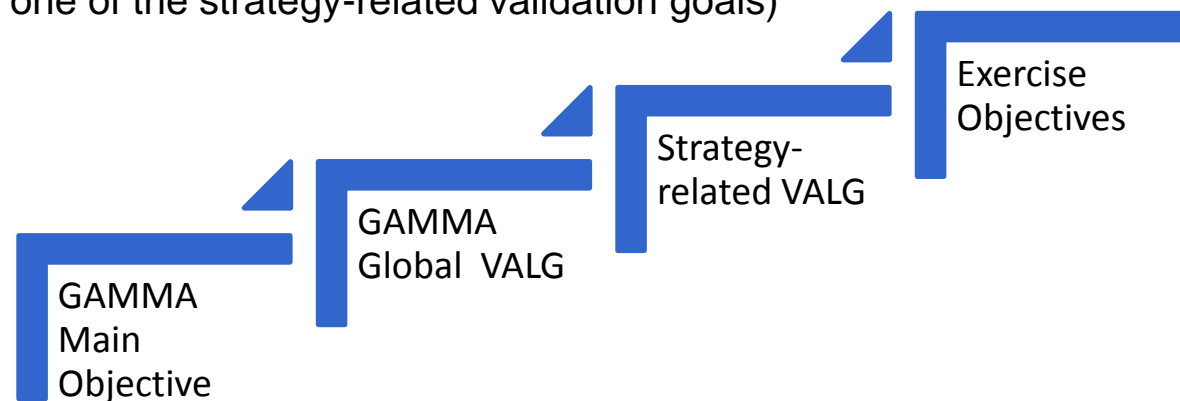




# Validation Exercises

## Validation Methodology for ATM Security Prototypes

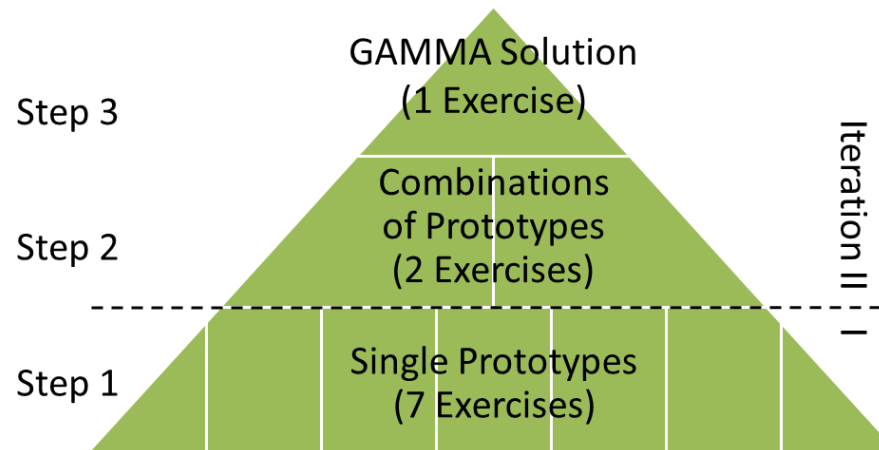
- In order to achieve the main GAMMA objectives and to comply with specific needs identified, **different levels of validation goals were proposed**:
  - **Global GAMMA validation goals** applying to all type of validation exercises and linked to these.
  - **Strategy-related validation goals**, applicable to each types of validation exercises (linked to global validation goals), dependent on validation approach chosen.
    - there are three types of strategy-related validation goals:
      - focused on validation of individual prototypes
      - focused on partial integration of prototypes (event detector prototypes + national level of SMP) and
      - focused on a full integration of GAMMA solution (event detector prototype + National level of SMP + European level of SMP)
- Each validation exercise defined **specific exercise objectives** (linked to at least one of the strategy-related validation goals)



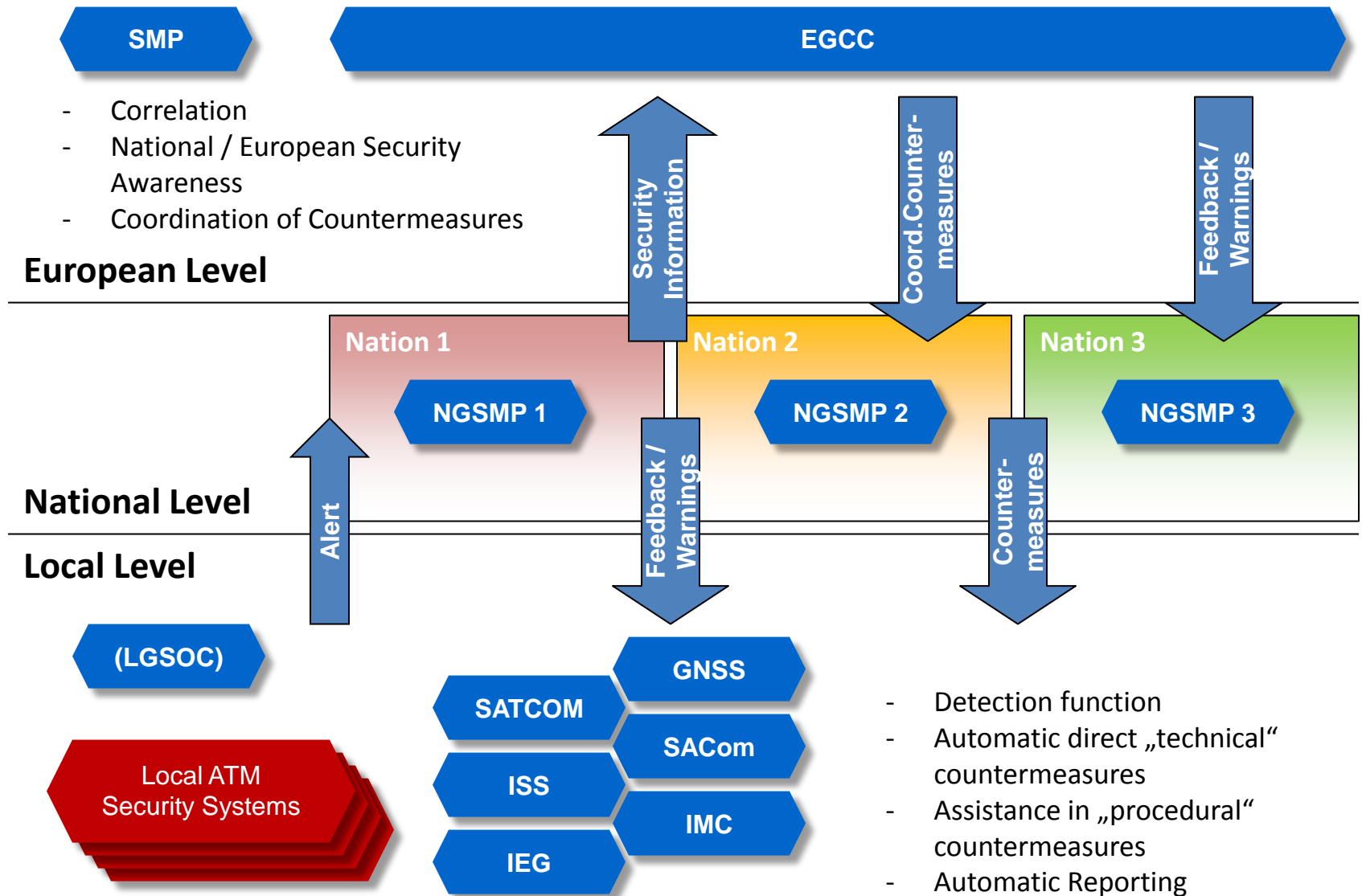
# Validation Exercises

## Validation Strategy

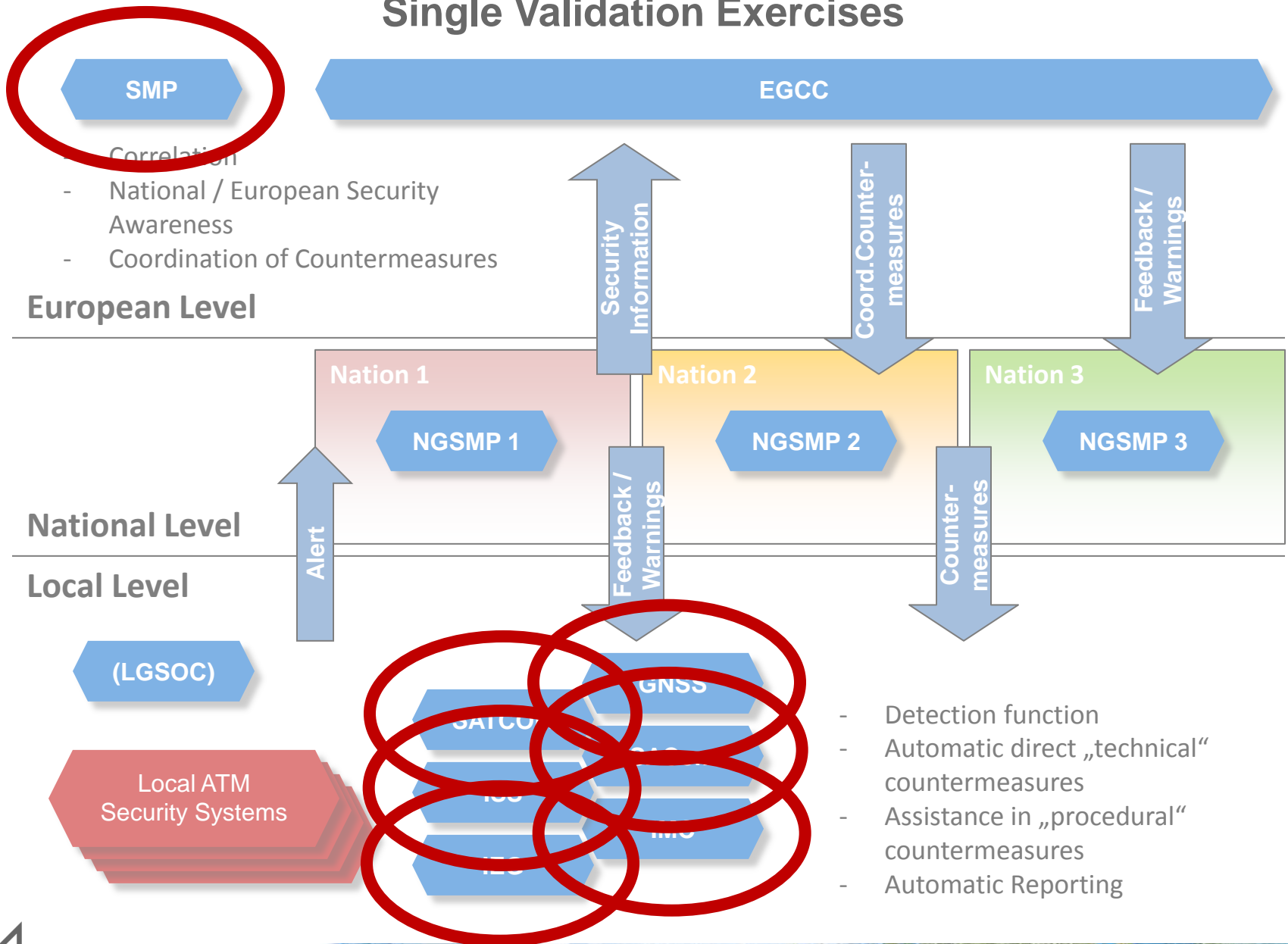
- **Validation** followed **ATM-security-incidents-centered approach** (not prototype-driven approach)  
→ validation scenarios were specified for the selected threats identified
- **Most important objective** of validation exercises:  
**demonstrate improvement in security management when security incidents occur**
- **Information regarding operational concepts' feasibility and benefits** had to be **obtained on threat scenario level and for collective validation** (summed over all validation exercises).
- **Validations can be conducted in three steps:**
  - **Single prototype validation**
  - **Validation of combination of prototypes** (partially integrated architecture)
  - **Concept validation** (fully integrated architecture)



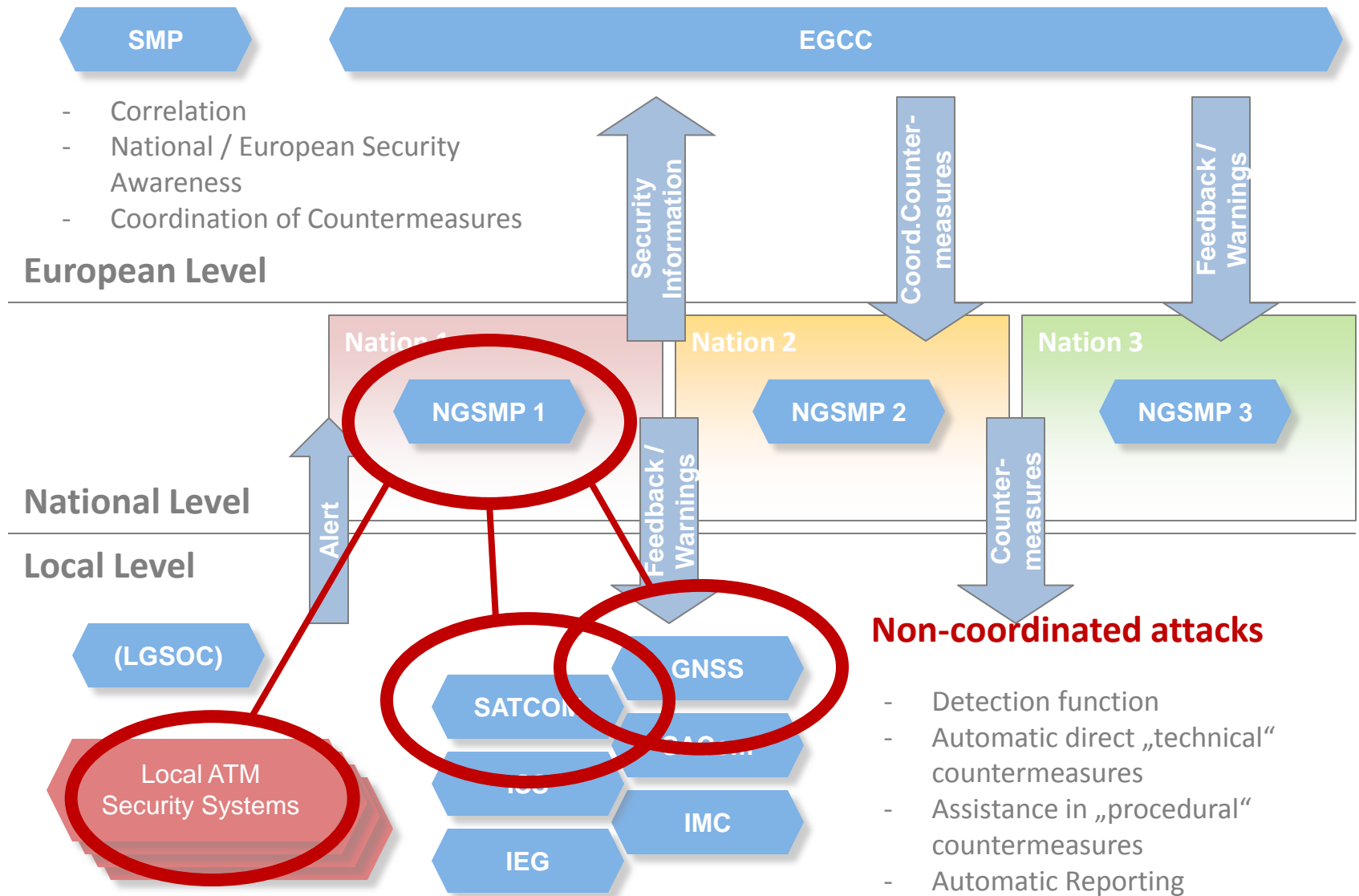
# GAMMA concept



# Single Validation Exercises

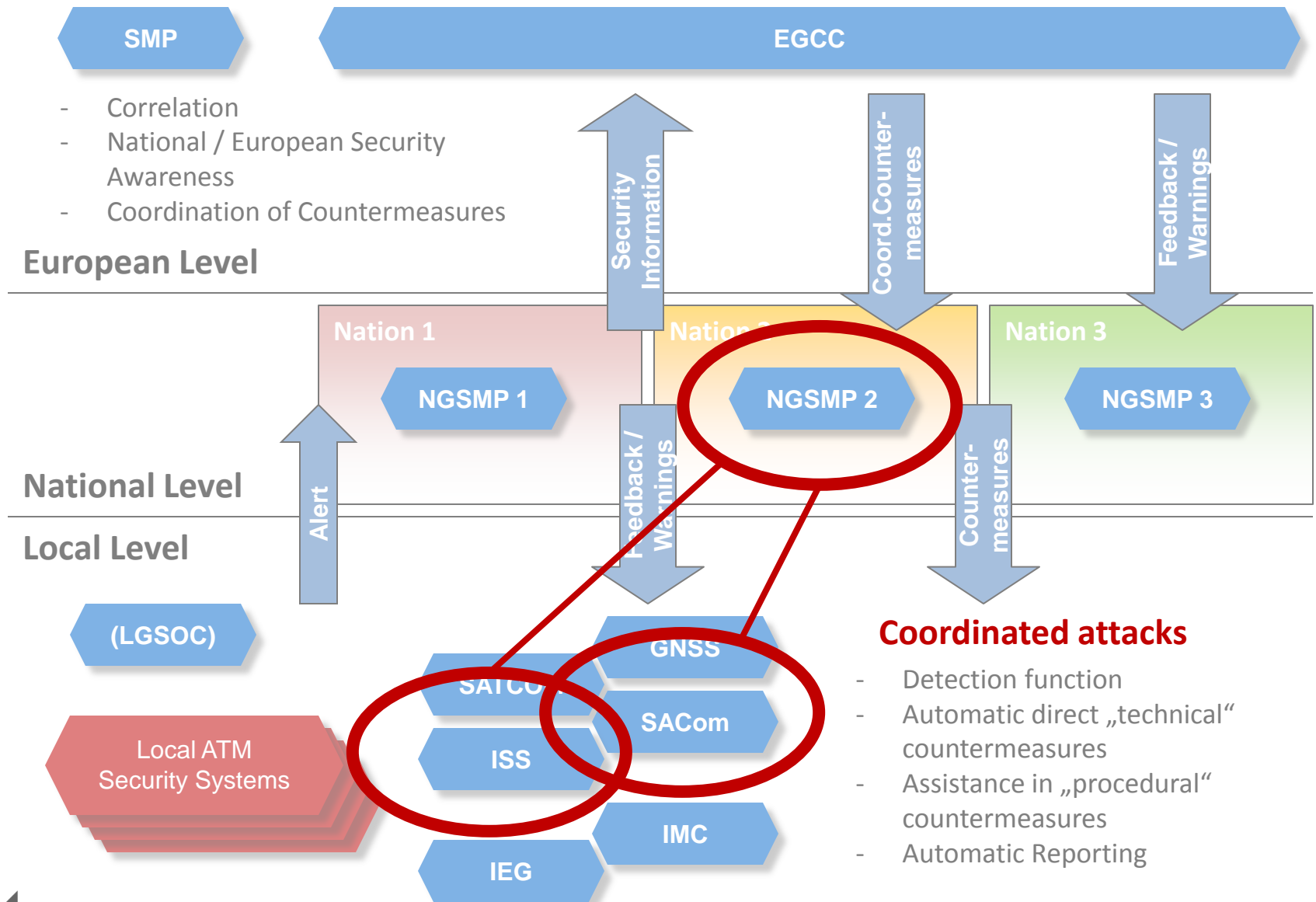


# Partially Integrated Validation Exercise 1

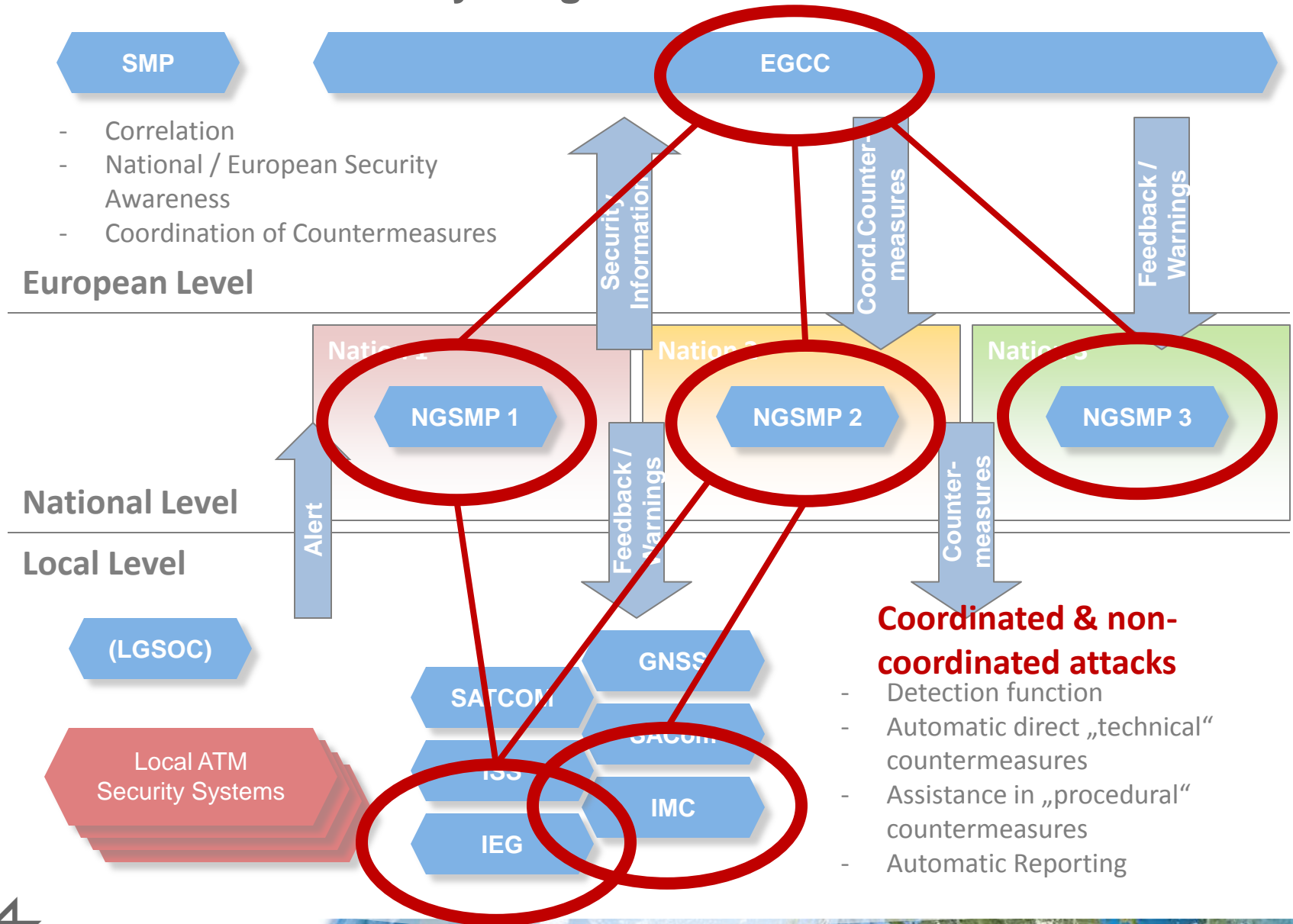




## Partially Integrated Validation Exercise 2



# Fully Integrated Validation Exercise 3



## Highlights on Validation Results

1/3

### **GAMMA paves the way forward in ATM security research**

**Validation exercises have proven that the GAMMA Security Management concept and related technologies are:**

- Fit for purpose
- Providing measurable benefits:
  - fast detection of threats
  - trusted and secure information dissemination
  - Fast dissemination of alerts to military authorities
  - Increase in situation awareness and selection of proper countermeasures
- Contributing significantly towards the evolvement in managing security in the future ATM System complementing SESAR



## Highlights on Validation Results

2/3

### **GAMMA paves the way forward in ATM security research**

#### **What the ATM community says:**

- Stakeholders and Subject Matter Experts (civil and military) agree that GAMMA is providing a real benefit to the ATM community
- Urgent need for changes of the existing ATM towards more cyber-security was recognised  
→ solution could be provided by GAMMA
- ATM security must be handled as a European topic, therefore be addressed in a collaborative way  
→ as suggested by GAMMA
- FI3 exercise: „an eye-opening event“ (wrt. to security awareness)



## Highlights on Validation Results

3/3

### **GAMMA paves the way forward in ATM security research**

#### **What SESAR gets:**

- Security controls identified or designed reside in the reference model, but they could also be taken out and used separately
- Security Prototypes as example of integration of security within ATM operation
- Security controls (as well stand-alone, combined with legacy and integrated in new ATM systems)
- Security KPI
- Security Architecture
- Blueprint for Validation methodology





# Challenges of security prototype validations



- General Validation Requirements
  - Security incident appears without any pre-warning
  - ***compare performance of unsupported human operator (=“baseline”) with pure technical performance of the system***
- Avoidance of raised attention
  - knowing that “something” will happen
    - level of attention is higher than it would be in real environment
  - ***very little information about GAMMA project and no information about design and functions of SCom prototype was provided***
- Avoidance of habituation effects
  - test person raises attention and prepares reactions when facing same situation again
  - ***each (short) scenario was unique***
    - ***same event, traffic situation and impact did not appear a second time in same exercise with same participant***



# Challenges of security prototype validations (cont.)



- Maintaining surprise effects
  - preparation and briefing of test person shall be kept to a minimum
  - ***scenarios and simulated events have been designed to be of unexpected nature***
- Modelling of security incidents
  - All conceivable aspects which may play a role for replication of situation must be accurately defined (comparability)
  - ***During simulations, features and effects of attack were reproduced. Pseudo pilots trained to act.***
- Modelling of options
  - test person will use a high level of creativity and flexibility. Therefore simulation must offer several options to (counter)act
  - ***Holding instructions, reporting, coordination, ...***
- Sensitivity of data
  - Adhere to well established regulations
  - ***Pseudonymization, declaration of consent, anonymous publication of recorded data, separate administrative from experiment data***





[www.gamma-project.eu](http://www.gamma-project.eu)

The research leading to this presentation has received funding from the European Community's Seventh Framework Programme under grant agreement nr. 312382

