Predictive Security Analysis for Event-driven Processes

Roland Rieke and Zaharina Stoynova
email: {roland.rieke,zaharina.stoynova}@sit.fraunhofer.de

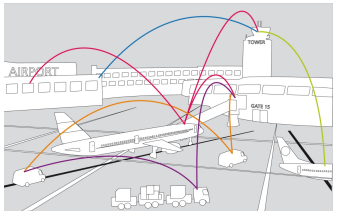
Fraunhofer Institute for Secure Information Technology SIT, Darmstadt, Germany

MMM-ACNS, September 2010

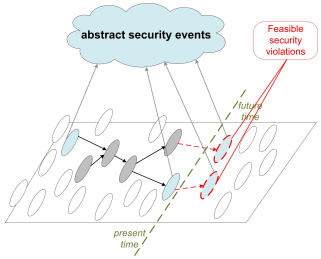
Overview

1. Understand System's Behaviour and Predict Effects
2. Security Requirements Elicitation
3. Use of Process Knowledge for Reachability Analysis
4. Security Reasoning in Freight Forwarder Scenario
5. Blueprint of Predictive Security Evaluation Engine & Further Development

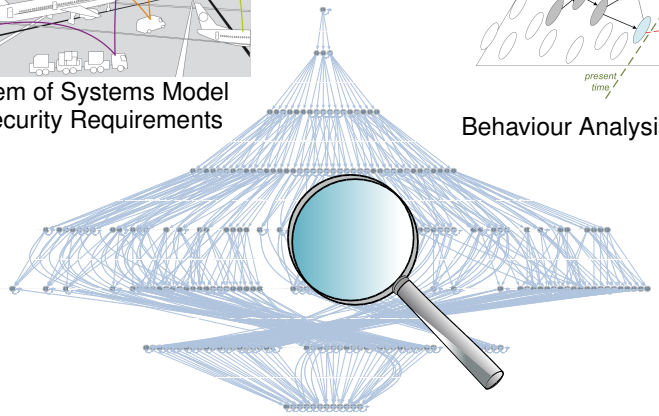
Understand System's Behaviour and Predict Effects



System of Systems Model & Security Requirements

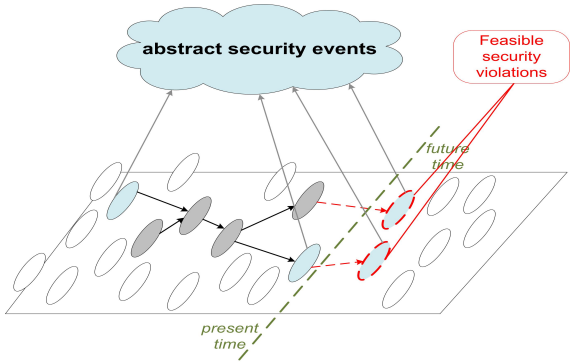


Behaviour Analysis (at runtime)



Behaviour Analysis (at SoS design time)

Predictive Security Analysis



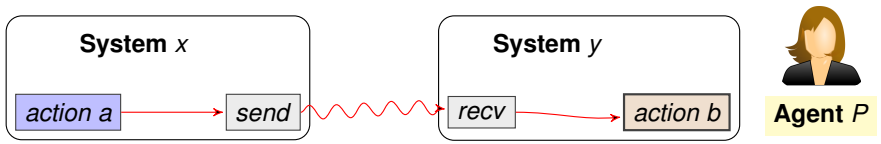
Based on

- Security Requirements, e.g. by Elicitation from Functional Dependencies,
- Process Knowledge (use BAM and Process Mining but add close-future Predition by Reachability Analysis), and
- Advanced Security Information and Event Management (SIEM) using Complex Event Processing (CEP) applied in Security Domain.

Security Requirements from Functional Dependencies

Security goal

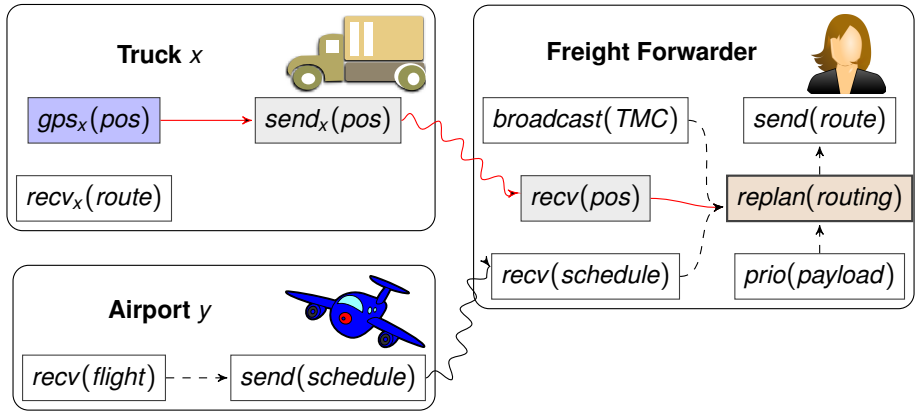
Whenever a critical action happens,
the input actions that presumably led to it must actually have happened.



Security requirement $auth(a, b, P)$

Whenever an action b happens, it must be authentic for an agent P that in any course of events that seem possible to him, a certain action a has happened.

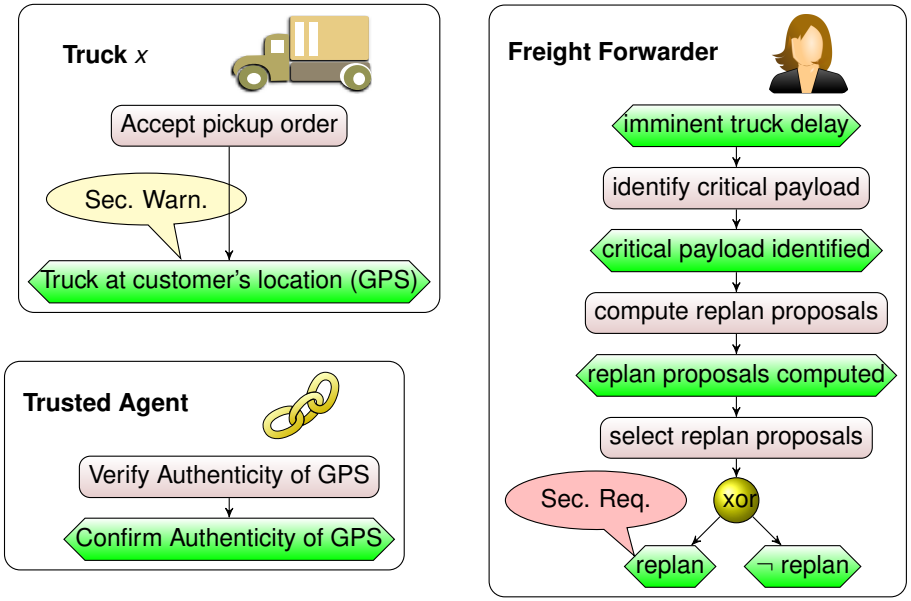
Security Requirement Elicitation



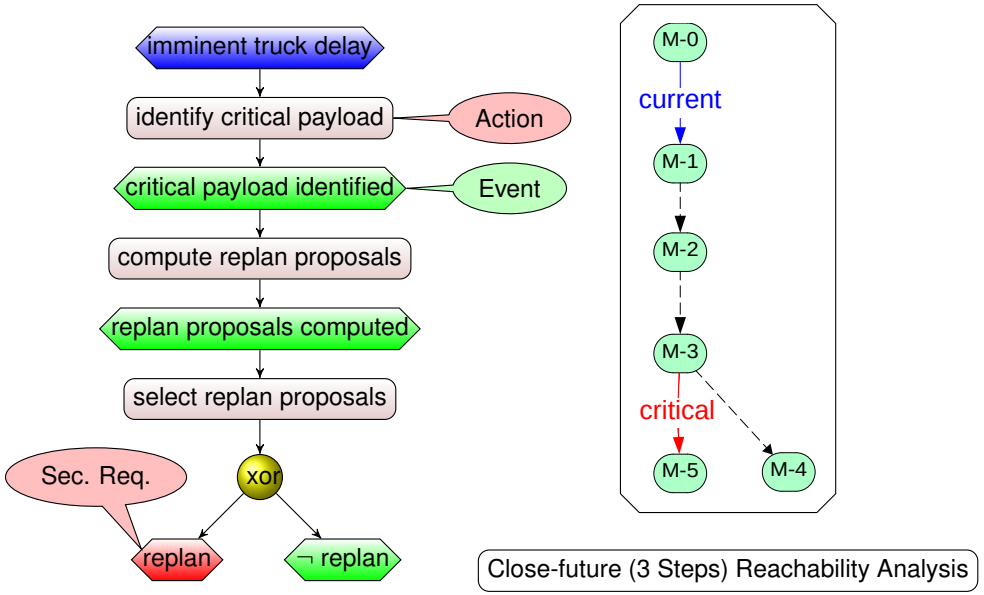
Security Requirement

$auth(gps_x(pos), replan(routing), scheduler)$

Business Process (EPC notation)

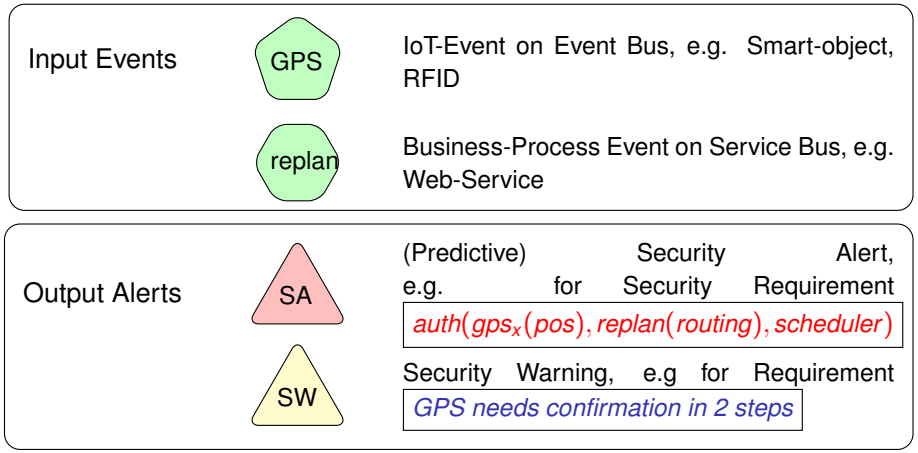


Use of Process Knowledge for Reachability Analysis

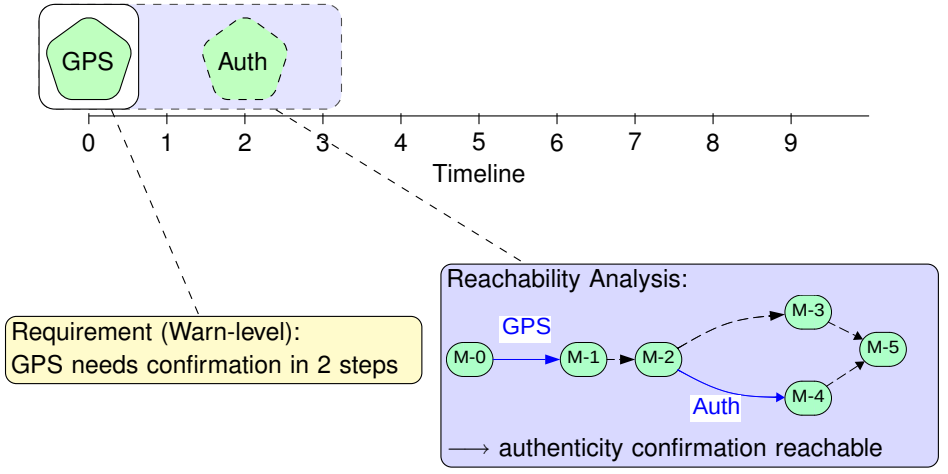


Close-future (3 Steps) Reachability Analysis

Freight Forwarder Scenario - Events and Alerts



Security Reasoning - Authenticity Approval of GPS Event

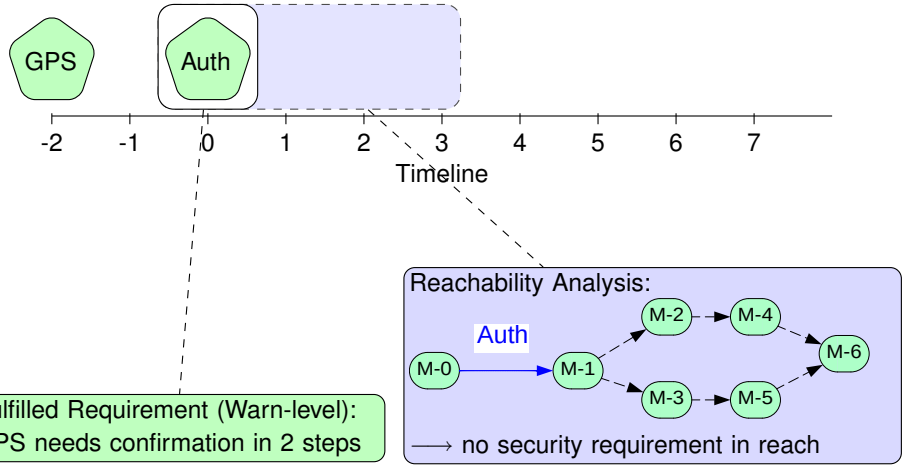


Conclusion:

- Everything ok

A future event might confirm authenticity of GPS

Security Reasoning - Authenticity Approval of GPS Event

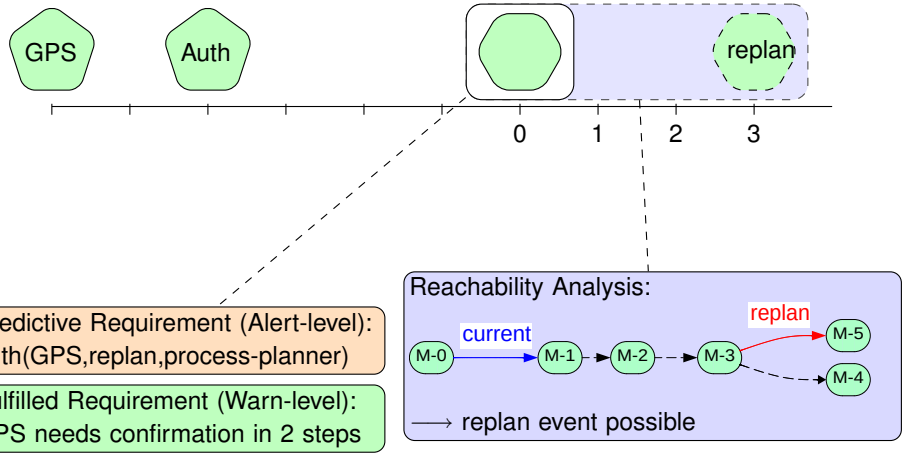


Conclusion:

- Everything ok

GPS approved authentic

Security Reasoning - Authenticity Approval of GPS Event

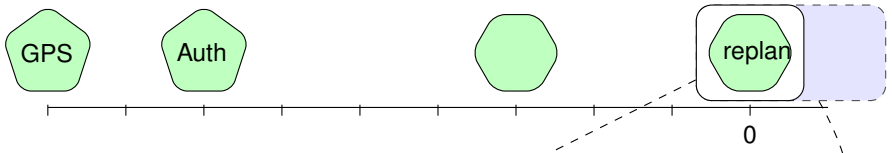


Conclusion:

- Everything ok

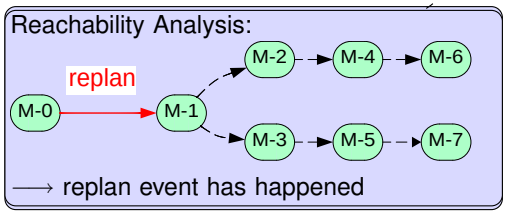
replan event with security requirement is possible

Security Reasoning - Authenticity Approval of GPS Event



Requirement (Alert-level):
auth(GPS,replan,process-planner)

Fulfilled Requirement (Warn-level):
GPS needs confirmation in 2 steps

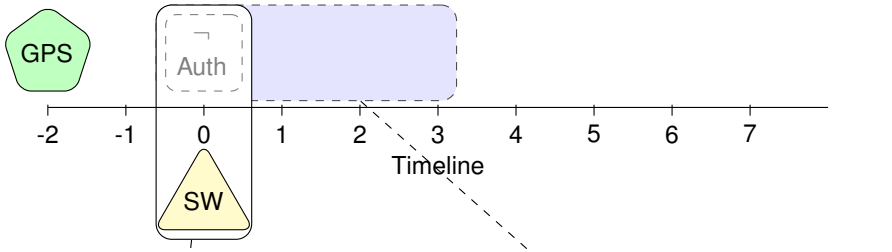


Conclusion:

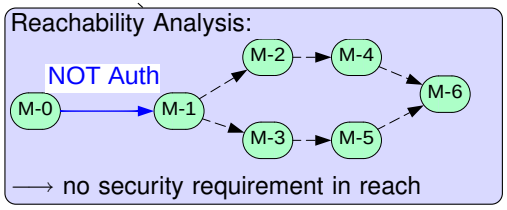
- Everything ok

security requirement of replan event is fulfilled

Security Reasoning - No Authenticity Approval of GPS Event



Broken Requirement (Warn-level):
GPS needs confirmation in 2 steps

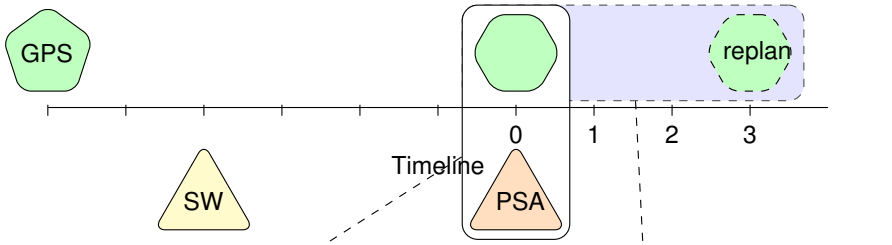


Conclusion:

- Security Warning

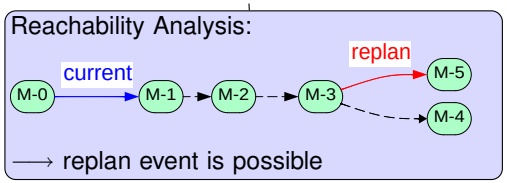
some future event might require authenticity of GPS

Security Reasoning - No Authenticity Approval of GPS Event



Predictive Requirement (Alert-level):
auth(GPS,replan,process-planner)

Broken Requirement (Warn-level):
GPS needs confirmation in 2 steps

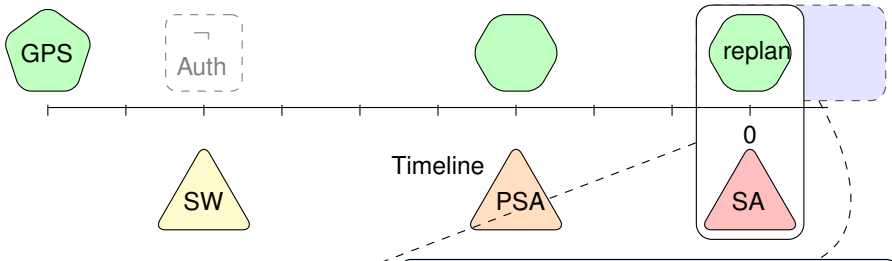


Conclusion:

- Predictive Security Alert

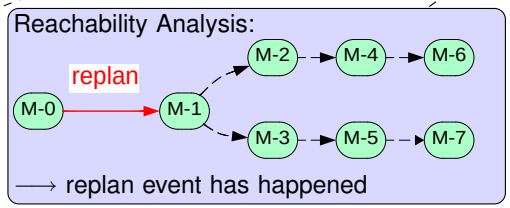
replan event with broken security requirement is possible

Security Reasoning - No Authenticity Approval of GPS Event



Broken Requirement (Alert-level):
auth(GPS,replan,process-planner)

Broken Requirement (Warn-level):
GPS needs confirmation in 2 steps

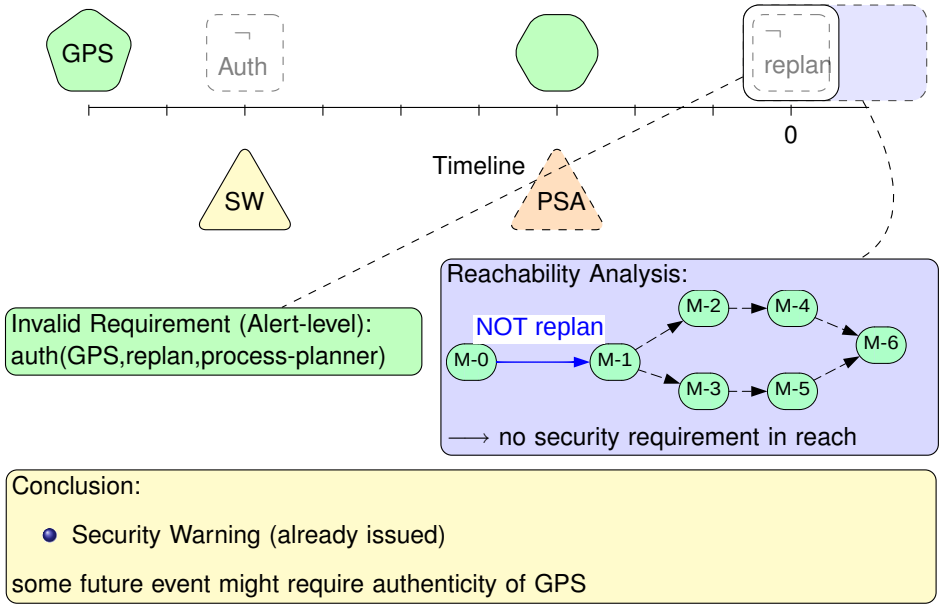


Conclusion:

- Security Alert

replan event with broken security requirement has happened

Security Reasoning - No Authenticity Approval of GPS Event

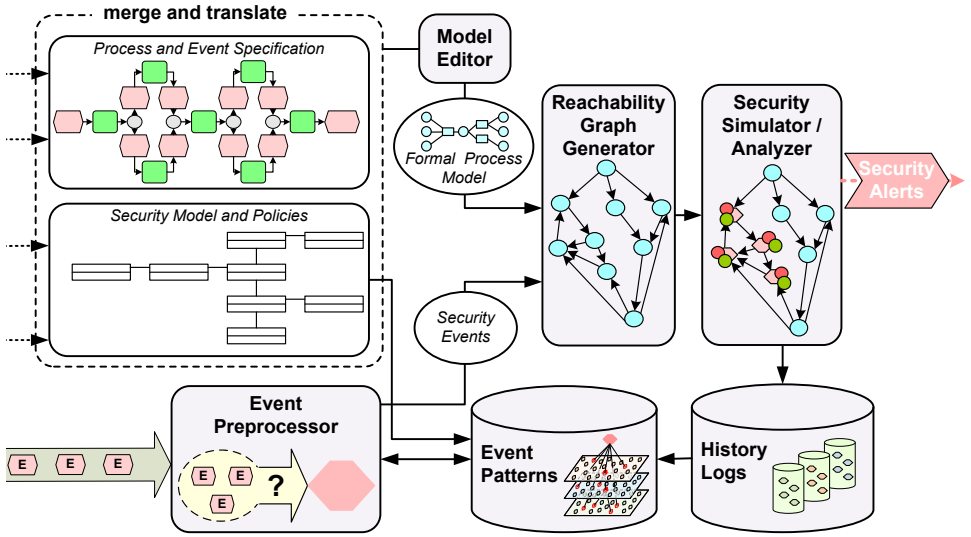


Conclusion:

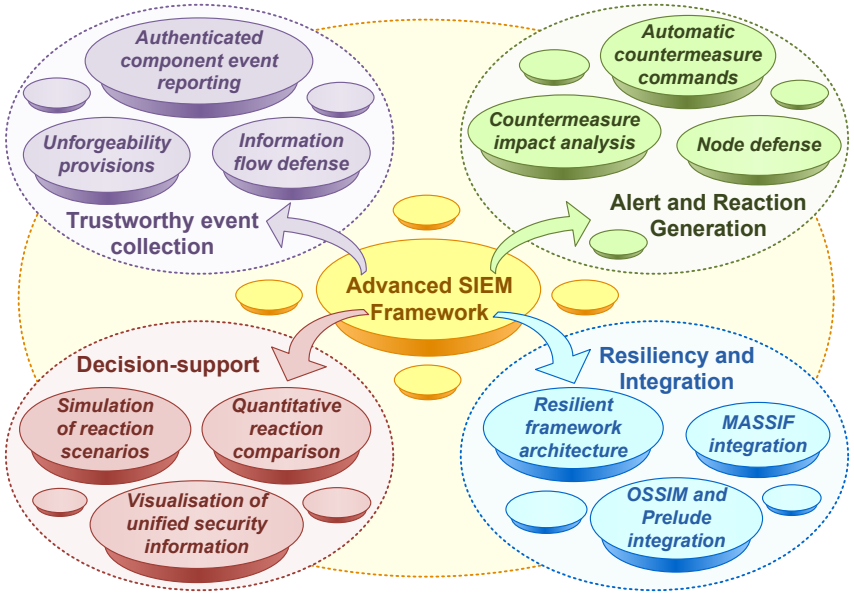
- Security Warning (already issued)

some future event might require authenticity of GPS

Blueprint of Predictive Security Evaluation Engine



Further Work - MASSIF (FP7) Advanced SIEM Framework



References

Andreas Fuchs, Sigrid Gürgens, and Carsten Rudolph.
A Formal Notion of Trust - Enabling Reasoning about Security Properties.
In *4th IFIP WG 11.11 International Conference on Trust Management*. Springer, 2010.

Andreas Fuchs and Roland Rieke.
Identification of Authenticity Requirements in Systems of Systems by Functional Security Analysis.
In *Workshop on Architecting Dependable Systems (WADS 2009), in Proceedings of the 2009 IEEE/IFIP Conference on Dependable Systems and Networks, Supplementary Volume*, 2009.

Andreas Fuchs and Roland Rieke.
Identification of Security Requirements in Systems of Systems by Functional Security Analysis.
In C. Gacek A. Casimiro, R. de Lemos, editor, *Architecting Dependable Systems 7*. Springer, 2010.

Peter Ochsenschläger and Roland Rieke.
Uniform Parameterisation of Phase Based Cooperations.
Technical Report SIT-TR-2010/1, Fraunhofer SIT, 2010.

Roland Rieke.
Abstraction-based Analysis of Known and Unknown Vulnerabilities of Critical Information Infrastructures.
International Journal of System of Systems Engineering (IJSSE), 1:59–77, 2008.

http://private.sit.fraunhofer.de/~rol/