Benefits of Security-informed Safety-oriented Process Line Engineering

Barbara Gallina [1],
(With contribution from Laurent Fabre [2])

[1] School of Innovation, Design and Engineering,
Mälardalen University, Västerås, Sweden
barbara.gallina@mdh.se

[2] Critical Systems Labs, Vancouver, Canada
laurent.fabre@cslabs.com

17th March 16, **4th Scandinavian Conference System and Software Safety (SCSSS), 2016**

Context

- Aircraft connectivity increasing
- New aircraft systems (networks) / New aircraft architecture (IMA)
- Pervasiveness of COTS

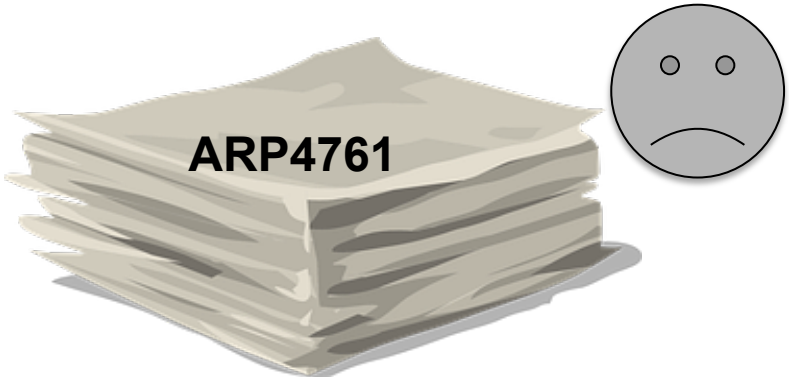
➔ Favorable grounds for cyber-security attacks

Adapted from:
https://pixabay.com/en/airplane-plane-aircraft-vehicle-26560/
https://pixabay.com/en/wifi-wi-fi-wireless-web-internet-43872/

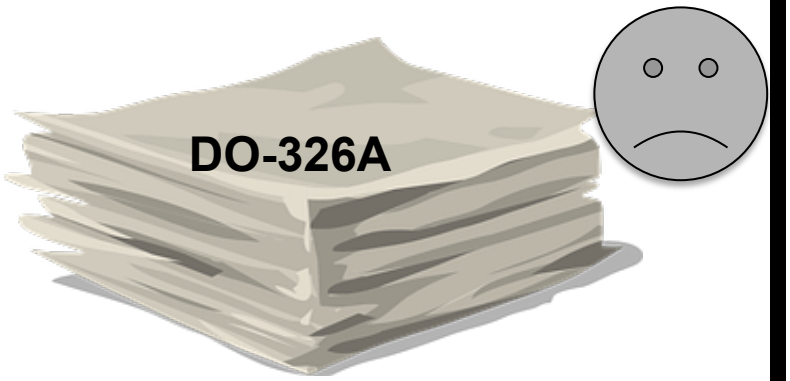
security-informed safety is crucial

Motivation

- Process engineer addressing the safety process



- Process engineer addressing the security process



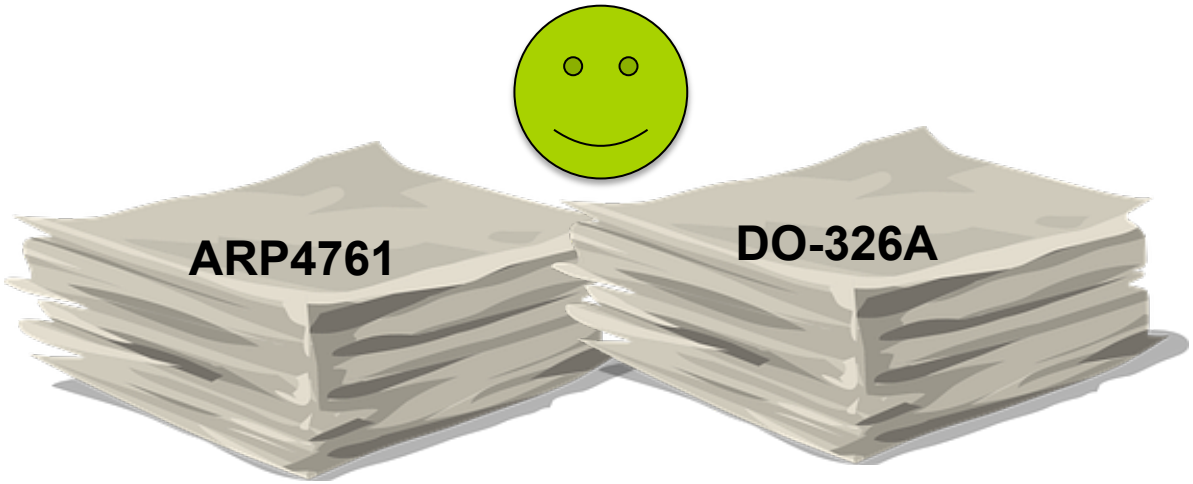
→ **Redundant and conflicting documentation/solutions**
→ **Waste of time and money**
→ **Risk for lower quality**

Motivations for aligning the safety and security assessment processes

- If security assessment is performed without ties to the safety assessment, it may be performed inadequately and potentially not completely
- Security threats or causes to threats may need to be fed back into the safety process
- Avoid interference between Safety and Security decisions regarding mitigations and architecture
- Allow presenting a combined safety-security picture to Certification Authorities. Faster approval!

Vision

- Process engineer(s) addressing the security & safety process



→ **Synergically conceived documentation/solutions**
→ **Saving of time and money**
→ **Increased quality**

Talk outline

- Background
  - Safety, security, and security-informed safety
  - RTCA DO-326A/ED-202A
  - ARP4761
  - Safety-oriented process lines engineering
  - Safety-oriented process line modeling
- SiSoPLE
- Applying SiSoPLE: an example
- Related work
- Conclusion and future work

Safety, security, and security-informed safety

[Avizienis et al 04] , [Bloomfield et al 13]

- Safety- absence of catastrophic consequences on the user(s) and the environment
- Security is defined as a composite attribute:
  - Availability - readiness for correct service
  - Confidentiality - absence of unauthorized disclosure of information
  - Integrity - absence of improper system alterations

- Security-informed safety – notion aimed at indicating:

  "For a system to be safe, it also has to be secure"

RTCA DO-326A/ED-202A

- Document (Published 2014) that provides guidance to handle the threat of intentional unauthorized electronic interaction to aircraft safety
  - Defines the Airworthiness Security Process through a set of:
    - risk assessment activities and
    - security architecture / measures development activities
  - Security risk assessment
    - Preliminary Aircraft Security Risk Assessment (PASRA), aimed at identifying threat conditions and threat scenarios and assessing all security risks at aircraft level

Remark: DO-356 describes methods to perform security-focused activities described in DO-326

SAE ARP4761

- Document that provides guidance to perform system safety assessment
- Defines the Airworthiness Safety Assessment Process:
  - Functional Hazard Assessment (FHA), aimed at identifying failure conditions and assessing all safety risks at aircraft level
  - Preliminary System Safety Assessment (PSSA): systematic evaluation of the proposed architecture and design to ensure that it can meet the safety requirements.
  - System Safety Assessment (SSA): verification that the system, as implemented, meets the system safety requirements established by the FHA and the PSSA

Safety-oriented process lines engineering

- Concurrent engineering of a set of safety-oriented processes
  - Why? To reuse systematically!

- Which consists of:
  - Scoping
  - Domain engineering (full and partial commonalities, variabilities)
  - Process engineering

Gallina et al 2012

Gallina et al 2014a

Gallina et al 2014b

Safety-oriented process lines modeling

- S-TunExSPEM (SPEM2.0 extension)

Task	Role	Tool	Work product	Guidance	Phase
					

Gallina et al 2014c

- vSPEM (SPEM2.0 extension)

Concept	Variation point	Variant
Task		

Talk outline

- Background
- SiSoPLE
  - Overview
  - SiS terminological framework
  - SiSoPLE modeling
- Applying SiSoPLE: an example
- Related work
- Conclusion and future work

SiSoPLE: Overview

- SoPLE extension aimed at addressing SiS-related processes

Why?

To realize our vision!

SiSoPLE: SiS terminological framework

- Mapping between terminologies used by
  - safety community
  - security community

- Examples:
  - Incompetence fault ←→ vulnerability
  - External fault ←→ attack

SiSoPLE modeling

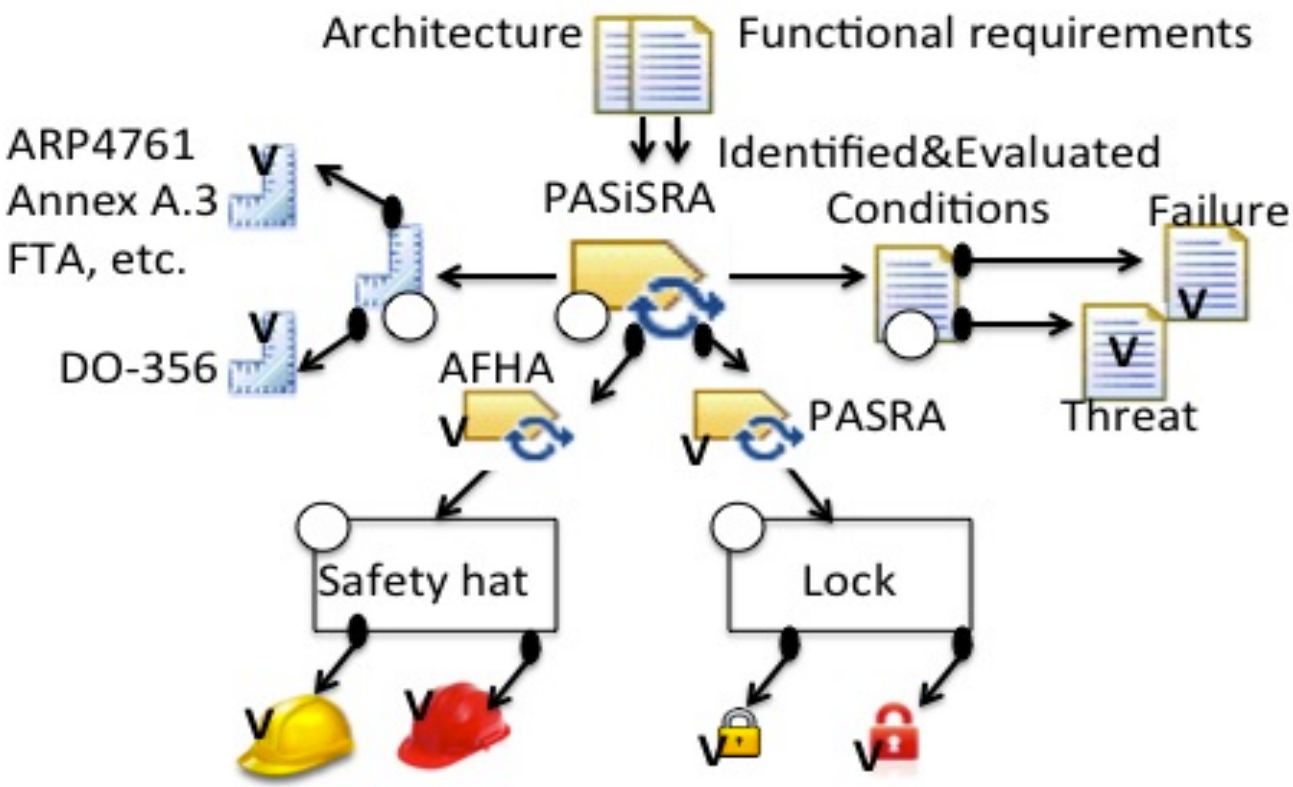
- Extension of the combination of S-TunExSPEM and vSPEM
  → Towards SiS-TunExSPEM

Novel language construct: security lock 

Applying SiSoPLE: an example

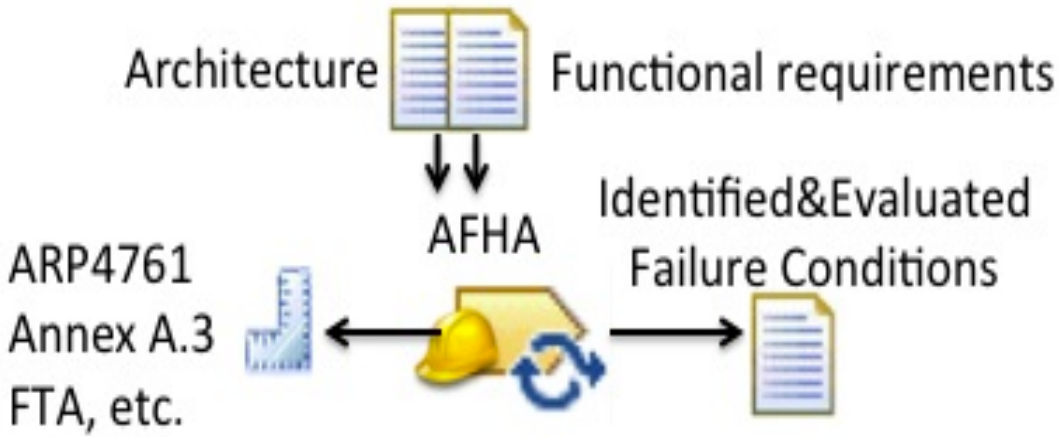
- SiSoPL – scoping
  - AFHA
  - PASRA
- Domain engineering
  - identification and comparison of certification-relevant process elements (tasks)
  - identification of commonalities and variabilities
- Single-process engineering

Applying SiSoPLE: an example



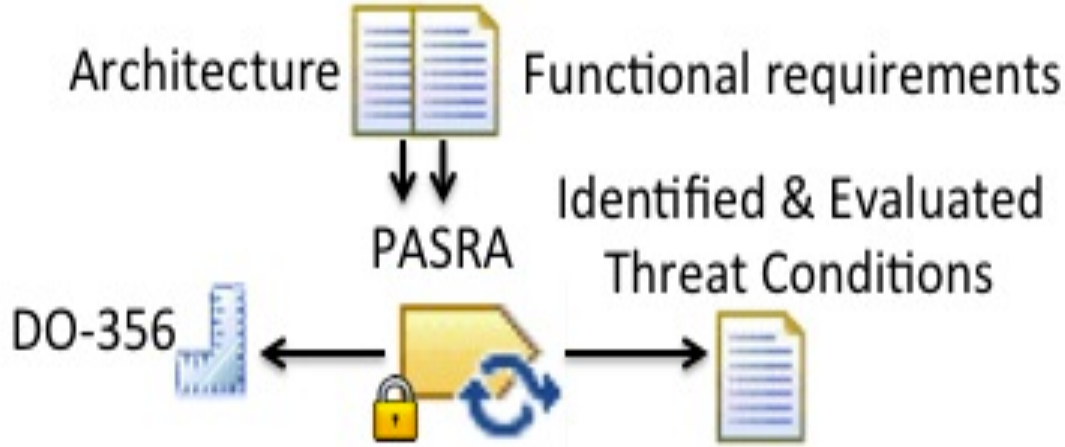
Applying SiSoPLE: an example

(AFHA derivation)



Applying SiSoPLE: an example

(PASRA derivation)



Lessons learnt

- General soundness
- Scalability
- Effectiveness
- Applicability

Related work

- Within the MAFTIA project [MAFTIA], researchers have worked on a common terminological framework to harmonize/cross fertilize safety&security

- Within the SafSec project [SafeSec], researchers have worked on common methodology for security accreditation and safety assurance

Conclusion and future work

- SiSoPLE: SoPLE extension for dealing with multi assurance concerns and enabling time and cost reduction during the provision of process-related deliverables via reuse
  - Benefits:
    - Duplication reduction
    - Synergies creation
    - Quality increase

- SiSoPLE further development
  - Clearly scoping and fully engineer our SiSoPL
  - Defining metrics
  - Investigating modelling capabilities targeting SiSoPLs
  - Enabling model-based certification

AMASS

AMASS

Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems

- PhD student in Applied Ontology and Knowledge Engineering http://www.mdh.se/hogskolan/jobb/phd-student-in-applied-ontology-and-knowledge-engineering-1.86385
- PhD student in Variability Modeling and Management http://www.mdh.se/hogskolan/jobb/phd-student-in-variability-modeling-and-management-1.86388
- Postdoc in Applied Ontology and Knowledge Engineering http://www.mdh.se/hogskolan/jobb/postdoc-in-variability-modeling-and-management-1.86403
- Postdoc in Variability Modeling and Management http://www.mdh.se/hogskolan/jobb/postdoc-in-applied-ontology-and-knowledge-engineering-1.86407

References

- [Gallina et al. 2015] B. Gallina, L. Fabre. Benefits of Security-informed Safety-oriented Process Line Engineering. IEEE 34th Digital Avionics Systems Conference (DASC-34), Prague, Czech Republic, September 13-17, 2015.
- [Gallina et al. 2014] B. Gallina, K. Lundqvist and K. Forsberg. THRUST: A Method for Speeding Up the Creation of Process-related Deliverables. IEEE 33rd Digital Avionics Systems Conference (DASC-33), doi:10.1109/DASC.2014.6979489, Colorado Springs, CO, USA, October 5-9, 2014.

References

- [Avizienis et al 04] Avizienis, A., J.-C., Laprie, B., Randell, C., Landwehr, 2004, Basic concepts and taxonomy of dependable and secure computing. In: IEEE Trans. Dependable Sec. Comput. 1(1): 11-33.
- [Bloomfield et al 13] Bloomfield, R., R. Stroud, 2013, Security-Informed Safety "If it's not secure, it's not safe". Marc-Olivier Killijian. Proceedings of the International Conference on. Computer Safety, Reliability and Security (SafeComp) FastAbstract, Toulouse, France. pp.NC. <hal-00926459>.
- [MAFTIA] The MAFTIA project, http://research.cs.ncl.ac.uk/cabernet/ www.laas.research.ec.org/maftia/
- [SafeSec] Praxis High Integrity Systems, SafSec: Integration of Safety & Security Certification, November 2006.

Related publications

- B. Gallina, Z. Szatmari. Ontology-based Identification of Commonalities and Variabilities among Safety Processes. Proceedings of the 16th International Conference on Product-Focused Software Process Improvement (PROFES), Springer, LNCS, Bolzano, Italy, December 2-4, 2015.
- B. Gallina, L. Provenzano. Deriving Reusable Process-based Arguments from Process Models in the Context of Railway Safety Standards. 20th International Conference on Reliable Software Technologies-Industrial Presentation- (Ada-Europe), Madrid, Spain, June, 2015.
- B. Gallina. Towards Enabling Reuse in the Context of Safety-critical Product Lines. 5th International Workshop on Product LinE Approaches in Software Engineering (PLEASE), joint event of ICSE, Florence, Italy, May 19th, 2015.
- B. Gallina, K. Lundqvist and K. Forsberg. THRUST: A Method for Speeding Up the Creation of Process-related Deliverables. IEEE 33rd Digital Avionics Systems Conference (DASC-33), doi: 10.1109/DASC.2014.6979489, Colorado Springs, CO, USA, October 5-9, 2014.
- B. Gallina, K. R. Pitchai and K. Lundqvist. S-TunExSPEM: Towards an Extension of SPEM 2.0 to Model and Exchange Tuneable Safety-oriented Processes. 11th International Conference on Software Engineering Research, Management and Applications (SERA), SCI 496, Springer, ISBN 978-3-319-00947-6, Prague, Czech Republic, August 7-9, 2013, 2014.

Related publications

- B. Gallina. A Model-driven Safety Certification Method for Process Compliance. 2nd IEEE International Workshop on Assurance Cases for Software-intensive Systems (ASSURE), Naples, Italy, doi:10.1109/ISSREW.2014.30, pp. 204-209, November 3-6, 2014.

- B. Gallina, S. Kashiyarandi, K.Zugsbrati and A. Geven. Enabling Cross-domain Reuse of Tool Qualification Certification Artefacts. Proceedings of the 1st International Workshop on DEvelopment, Verification and VAlidation of cRiTical Systems (DEVVARTS), Springer, LNCS 8696, ISBN: 978-3-319-10556-7, pp. 255-266, Florence (Italy), 8 September, 2014.

- B. Gallina, S. Kashiyarandi, H. Martin and R. Bramberger. Modeling a Safety- and Automotive-oriented Process Line to Enable Reuse and Flexible Process Derivation. Proceedings of the 8th IEEE International Workshop on Quality-Oriented Reuse of Software (QUORS), joint workshop at COMPSAC conference, IEEE Computer Society, doi: 10.1109/ COMPSACW.2014.84, pp. 504-509,Västerås (Sweden), 2014.

- B. Gallina, I. Sljivo, and O. Jaradat. Towards a Safety-oriented Process Line for Enabling Reuse in Safety Critical Systems Development and Certification. Post-proceedings of the 35th IEEE Software Engineering Workshop (SEW-35), IEEE Computer Society, ISBN 978-1-4673-5574-2, Heraclion, Crete (Greece), 2012.

Thank you for your attention!

Discussion time…