Session 1 summary

Presentations:

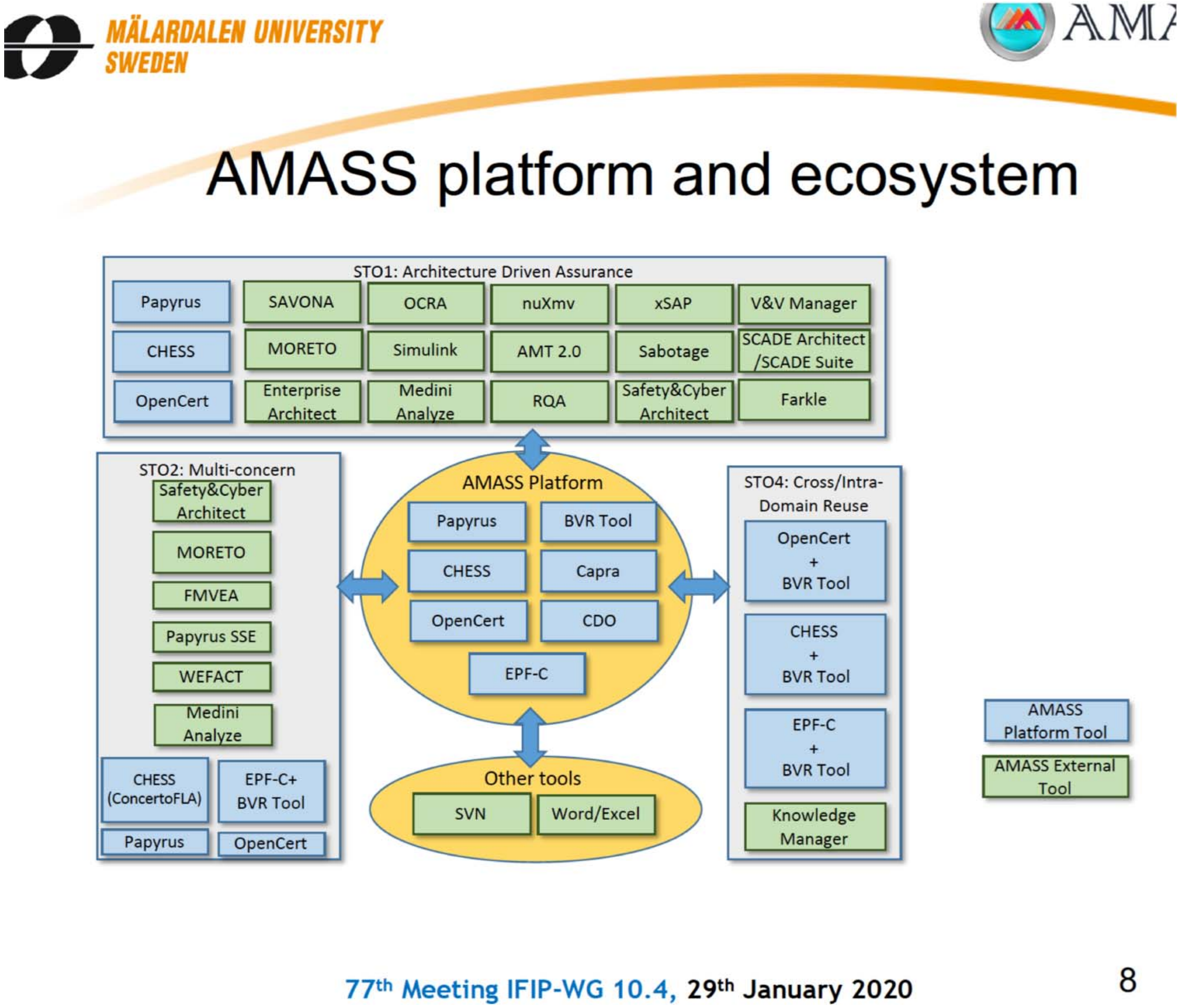
Barbara Gallina: Assurance and Certification of Cyber-Physical Systems within the AMASS platform

Peter Popov: Models of attacks in critical infrastructures

Karthik Pattabiraman: Stopping the Barbarians at the Gate: Protecting End User Devices from Security Attacks

Assurance and Certification [...] AMASS platform

- report on a EU project: AMASS
  (Architecture-driven, Multi-concern and Seamless Assurance and Certification of Cyber-Physical Systems)
- integration of tools so as to support assurance/certification activities



AMASS platform and ecosystem

STO1: Architecture Driven Assurance

Papyrus, CHESS, OpenCert, SAVONA, MORETO, Enterprise Architect, OCRA, Simulink, Medini Analyze, nuXmv, AMT 2.0, RQA, xSAP, Sabotage, Safety&Cyber Architect, V&V Manager, SCADE Architect /SCADE Suite, Farkle

STO2: Multi-concern

Safety&Cyber Architect, MORETO, FMVEA, Papyrus SSE, WEFACT, Medini Analyze, CHESS (ConcertoFLA), EPF-C+ BVR Tool, Papyrus, OpenCert

AMASS Platform

Papyrus, BVR Tool, CHESS, Capra, OpenCert, CDO, EPF-C

Other tools

SVN, Word/Excel

STO4: Cross/Intra-Domain Reuse

OpenCert + BVR Tool, CHESS + BVR Tool, EPF-C + BVR Tool, Knowledge Manager

AMASS Platform Tool

AMASS External Tool

77th Meeting IFIP-WG 10.4, 29th January 2020

8

Assurance and Certification [...] AMASS platform

- aim: efficiently supporting the clerical/syntactic part of assurance cases and compliance checking
- integrates experience about product line development processes

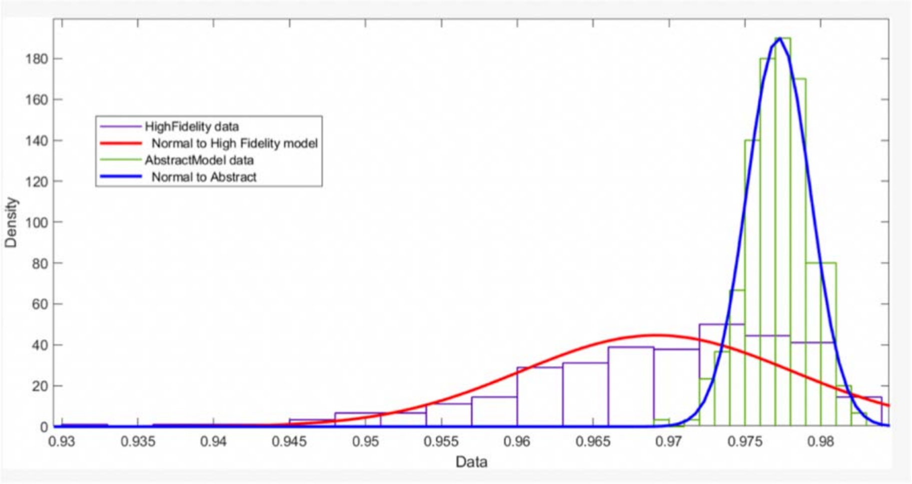
- emphatically not intended to replace expert's role in checking relevance and strength of evidence
  - although could present automated deductions where feasible
  - [rapporteur's thought: once such tools are adopted, it would be useful to survey in which companies they are used as intended, vs reinforcing a box-ticking mindset, and why]

- relevance to "awareness":
  - can be used to direct and support integration between security- and safety-oriented activities
    - + hence support awareness during development and assurance processes
    - + AMASS arguments will include human aspects in complex systems, so will need evidence about situation awareness
    - + case study will demo examples of this

Models of attacks in critical infrastructures

- Research question: “Can we build probabilistic models of *unknown* attacks on Critical infrastructures, which are *useful* for risk assessment?”

- Example: two models for a "benchmark" example, one including detail of attacks' action on physical target, the other one without them
  - markedly different results
  - where it matters most



Models of attacks in critical infrastructures

lessons relevant to security awareness:

- about awareness at system configuration/assessment time (e.g. prioritising defence investment)
  - [rapporteur's observation: results could be used in operation phase: likelihood of symptoms conditional on type of attack could inform diagnosis]

- high fidelity hybrid models are worthwhile though expensive (simulation solutions)
- engineering awareness of "promising" attacks is vital input for this probabilistic risk analysis

Stopping the Barbarians at the Gate

- motivation: we should care about end device security because
  - potential entry point for attackers
  - potential scenarios of large-scale disruptions directly through taking over many end-user devices
- some attacks on Embedded and IoT devices
  - nice videos!
  - limits of "control-based" intrusion detection
  - insight on promising targeting techniques, e.g. small deviations, mode changes
- Intrusion Detection Systems for Smart Devices
  - examples: UAV and artificial pancreas
  - improvements obtained
- Ongoing work
  - e.g. accounting for popular moves from PID control to DNNs

Stopping the Barbarians at the Gate

- about situation awareness
  - brings more engineering awareness about "promising" attacks (cf previous talk)
  - promising directions and tools in intrusion detection

    (and experience about blind alleys)

... hence direct contribution to operation-time situation awareness

Summary

Contributions

- both to pre-operation risk awareness and management
- and to operation time

- three very disparate sets of results with interesting potential links