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

WP4: Multiconcern Assurance Progress and Achievements

First EAB Workshop
Trento, 11 September, 2017

Thomas Gruber
WP4 Leader
WP4 Objectives

Provide research foundation & technologies for extended system safety assurance, including: security, reliability, availability and performance.

Main specific objectives:

1. Determine needs and constraints for the approach to be developed
2. Provide a conceptual framework covering the information needs for multi-concern assurance
3. Refine safety-focused CCL meta-models & vocabulary to include wider assurance concerns relevant to the case studies in the target domain
4. Enrich the AMASS meta-model CACM.
5. Develop an assurance case framework which is capable of
   • supporting the composition of system components
   • adequately dealing with trade-offs between complementary and competing assurance concerns (in multi-dimensional way, not simply pairwise)
   • supporting multiple views of assurance data and argument.
Multi-concern Assurance in the ARTA

AMASS Reference Tool Architecture

**WP4**

- **Architecture-Driven Assurance (STO1)**
  - System Architecture Modeling for Assurance
  - Assurance Patterns Library Management
  - V&V-based Assurance Impact Assessment
  - Contract-Based Assurance Composition
  - Technological Patterns
  - Architectural Patterns

- **Multi-Concern Assurance (STO2)**
  - System Dependability Co-Analysis/Assessment
  - Dependability Assurance Modelling
  - Contract-Based Multi-concern Assurance

- **AMASS Platform Basic Building Blocks**
  - Access Manager
  - Data Manager
  - System Component Specification
  - Assurance Case Specification
  - Evidence Management
  - Compliance Management
  - Common Assurance & Certification Metamodel (CACM)

- **Cross/Intra-Domain Reuse (STO4)**
  - Semantic Standards Equivalence Mapping
  - Product/Process/Assurance Case Line Specification

- **Seamless Interoperability (STO3)**
  - Collaborative Work Management
  - Tool Quality Assessment and Characterization

- **Guidelines in progress**

- **Functionalities identified. Implementation provided and validated (core prototype)**

- **Independent Assessment**
  - Certification Liaison
  - Safety/Security Assessment

- **Product Engineering**
  - Design
  - Validation & Verification
  - Development
  - Quality Management

1st EAB Workshop, Trento, September 11, 2017
### Quality Attributes Treated

- Scope varies from domain to domain
- Safety strongly supported
- Security is recognized except in the Space domain
- Especially in the automotive domain much work towards treating complex ADAS & Cybersecurity
State of the Art in Multiconcern Assurance - Standards

- Standardization activities to include safety & security have proceeded:
  - **Industrial domain**: IEC 62443 "Industrial communication networks – Network and system security" is in force.
  - **Railway**: Security Guideline DIN VDE V 0831-104 based on IEC 62443 (Planned to be issued as IEC standard).
  - **Automotive**: In addition to functional safety oriented ISO26262, SAE J3061 “Cybersecurity Guidebook for Cyber-Physical Vehicle Systems“ is used. Currently ISO 26262 Ed.2 is being elaborated, Annex F on security is planned. Wrt. autonomous driving, the SOTIF "Safety of the intended Functionality" subgroup has been founded (-> ADAS) and joint SAE / ISO Working Group started the development of an automotive security standard.
State of the Art in Multiconcern Assurance – other Projects

- Predecessor Artemis projects **OPENCOSS** and **p+nSafeCer** focused on safety only.
- Artemis project **SESAMO** investigated MB safety and security assessment and used dedicated tool chain (Medini Analyse & CHESS) to specify critical architecture parts.
- **CONCERTO** project: MB, component-oriented toolset (CHESS), WCET and schedulability analysis; Dependability Profile (RAMS but also Human Factors).
- **MERgE** - Model-Based Safety & Security Assessment approach – Sa/Se views in Safety Architect
- **EMC2**
  - Safety and security assurance processes combined (HARA, TARA, STAMP-SEC, FMVEA)
  - Objectives:
    - Establish Multi-Core technology in all relevant Embedded Systems domains
    - Enable mixed-criticality applications.
  - Focus on multi-core platform for multiple domains ensuring safety and security for critical applications.
  - Key achievements for safety and security:
    - Integrate Safety&Security Engineering to handle the impact of security on safety
    - Conditional runtime certification (safety checks of dynamic system compositions)
AMASS deals with
- Security-Aware Safety Case or
- Dependability Case extensions

No fully-fledged (kind of) "Security Case".
- Safety case is an established concept, security case is new => start from safety and extend

Relevant quality attributes for AMASS:
- Algirdas Avizienis’ and Jean-Claude Laprie’s taxonomy (2004)
- Plus more, e.g. robustness
- AMASS takes a generic approach and is open for any attribute
- Most important: Safety & Security!
WP4 - Overview

Other AMASS Platform Building Blocks

- ReqIF
- SysML
- SPEM2.0
- SACM

Data exchange based on

CORE

- Database / Evidence Manager

WP4 boundary

CORE

- AC Pattern Library
- Assurance case Editor

Safety & Security analysis

Multi-concern Contracts

Dependability modelling

Process execution (WEFACT)

Cooperation with WP3

Cooperation with WP5
AMASS Functions to be Provided by WP4

AMASS

Dependability Assurance Modeling

Contract-Based Multi-concern Assurance

System Dependability Co-Analysis/Assessment

Modelling the assurance case with classes:
- Approach taken from the OPENCOSS project
- SACM (Structured Assurance Case Metamodel) of OMG
- Model is displayed in GSN
- Develop multi-concern assurance patterns

Contracts play a role in AMASS in two contexts:
- Component contract
  - entity assures certain guarantees if the assumptions are fulfilled
- Assurance contract
  - Integrates different arguments of the assurance case

Two variants:
- **Separate** analysis of >1 quality attributes
  - = Traditional state of the practice
- **Combined** analysis of >1 quality attributes
  - -> AMASS proposes combined methods
Concepts: Relations between Claims wrt. Quality Attributes

Dependency relationship.
• The claim A of one attribute depends on the fulfillment of claim B of another attribute.
• E.g. a fail-safe claim (safety) depends on safety system not tampered (security).

Conflicting relationship.
• The assurance measure of attribute A is in conflict with the assurance measure of attribute B.
• E.g. “strong password or blocking a terminal after several failed login attempts” (security) conflicts with “emergency shutdown” (safety).
• Resolution of such a conflict needs to be noted in the Assurance Case.

Supporting relationship.
• Assurance measure of attribute A is also applicable to assurance of attribute B => one assurance measure can be used to replace two separate ones.
• E.g., encryption can be used for both confidentiality (security) and to check data integrity instead of checksum (safety).
=> This means two goals can be addressed by one argumentation.
Multiconcern Assurance Processes in the System Lifecycle

1. Start system development
   - System concept
     - Analyses
       - Separate, e.g. HARA + TARA
       - Combined, e.g. FMVEA
     - Safety & security requirements
       - Trade-off analysis
         - Architecture, & design
           - Analysis, formal proof, tests, contracts, evaluation: Requirements wrt. all quality attributes fulfilled?
             - no
             - yes
               - Insert evidences in assurance case
                 - Assurance case established for a period of time
               - Plan argumentation strategy
                 - Model arguments in Assurance case
                   - Workflow e.g. WEFACST

2. Other functional and non-functional requirements
WP4 – Concepts: Co-analysis

Mapping of methods to specific development phase
- Support consideration of multiple attributes during all phases

Focus is on consideration of safety impacts due to security incidents
Prototype Core:

- Basic Building Block "Assurance Case Specification"
- Extended OPENCOSS Assurance Case Editor from OpenCert including pattern library
  - Internally using SACM (Structured Assurance Case Metamodel) of OMG
  - GSN diagrams in the GUI ➢ relevant for industry
- Released as open source tool with documentation and user manual as D4.4 on Jan. 31, 2017
Process-related Co-Assessment with WEFACT

- Requirements from standards wrt. multiple concerns modelled in EPF
- Process model imported in WEFACT and executed for automated multiconcern assessment
Main Achievements Year 1

• Applicable standards identified for different quality attributes in several domains
• State of the art for co-engineering in standards and industrial practice including existing methods investigated and published in D4.1, released on Sept. 30th, 2016
• Concept for co-engineering developed and Multiconcern Assurance tools and methods for second iteration of ARTA proposed & documented in D4.2
• Definition of first multi-concern patterns
• WP4 contribution to the first iteration of the ARTA – the OpenCert Assurance case editor – released with D4.4
Next Steps in WP4

• Release of D4.2
  – Definition of concepts for multiconcern assurance:
    • dependability assurance modelling,
    • system dependability co-analysis/assessment, and
    • contract-based multiconcern assurance

• Definition of Guidelines
  – To be started next in T4.4

• Support for the AMASS second prototype
  – Work started in T4.3, to implement the developed concepts
Thank you for your attention!
FMEA Analysis Process
Security Part in FMVEA is Based on STRIDE / Threat Modeling

- Connect threat modeling (Dataflow based) with system functions and potential hazards => direct identification of hazards caused by threats
WP4 – ARTA Functionalities to Achieve STO2
WEFACT Assurance Workflow Tool

- Prototype WEFACT V2 under development
- Eclipse RCP application using MySQL DB
- Basics incl. EPF import implemented
- First results presented in Sevilla plenary
- Roles/users and report generator to be done
- In terms of AMASS: affects multiconcern assurance workflow and evidence management (WP5)
WEFACT – Basic Workflow Concept

- Requirements-based assurance - as far as possible automated
- Various tool bindings, can treat deliberate quality attributes
- Results are evidenced for the assurance case
- This example depicts the workflow for safety and security co-assurance
• WEFACT is a workflow engine which is currently re-implemented in Eclipse
• Can import process from EPF
• Interconnect process steps with tools
  – Different levels from Command line call to OSLC
• Exchange requirements with tools