SECURITY AND SAFETY MODELLING FOR EMBEDDED SYSTEMS

https://www.sesamo-project.eu

John Favaro, Intecs S.p.A.
Robert Stroud, Adelard LLP

Outline

- Introduction to SESAMO
- SESAMO objectives
- Project organization
- Use cases
- Use case evaluation
- Security-informed safety
- Discussion and outlook
INTRODUCTION TO SESAMO

SESAMO: Artemis 295354

**SESAMO**

*Security and Safety Modelling*

- Starting date: May 1st 2012
- Duration: 36 months
- Total costs: 12.013 k€
- EU contribution: 1.968 k€
- Total planned effort: 1.114 p/m
- 7 Work packages, 31 deliverables

Reducing the cost of building safe and secure products
Consortium

- 20 partners
  - 8 countries
  - 13 large industries
  - 1 SME
  - 2 Research
  - 4 Academia

Consortium, another view

- Ind/sme
  - Intecs (I)
  - AKH (I)
  - ADEL (UK)
  - Ikw (D)
  - SYSGO (D)
  - IFAG (D)
  - ESY (D)
  - SYSGO s.r.o. (CZ)
  - SAG (A)

- Research/academia
  - FTW (A)
  - CTU (CZ)
  - DICEA (I)
  - IT-CNR (I)
  - DTU (DK)
  - City (UK)

Solution providers

Problem owners

- Aerospace
  - EADS IW Ge (D)

- Energy Management
  - AKH (I)
  - EDF (F)

- Automotive
  - PSA (F)
  - GM (USA)
  - SAG (A)
  - IFAG (D)

- Metropolitan rail
  - UniControls (CZ)

- Mobile medical
  - IFAG (D)
  - ESY (D)
Why SESAMO?

- SESAMO addresses:
  - ... the root problems arising with the convergence of safety and security in embedded real-time (and therefore time-critical) systems ...  
  - ... subtly and poorly understood interactions between functional safety and security mechanisms ... 
  - ... the absence of a rigorous theoretical and practical understand of safety and security feature interaction ...

Safety versus Security

**Redundancy** in safety-related protocols is a common way to ensure the integrity of communications

- **SECURITY**
- **SAFETY**

But increased redundancy increases the **attack surface** and affects the security characteristics of the communication
Safety / Security: many questions

Safety trumping security: emergency call bypassing PIN

But does safety *always* trump security, in all contexts?

Safety encourages stable software versions. Security sometimes encourages frequent updates – breaking safety certification / qualification

---

SESAMO OBJECTIVES
The SESAMO Objectives

- SESAMO has defined seven objectives
- Each builds upon the last
- Creating a logical, coherent focus for the project

Safety and Security Modelling

- Enabling joint reasoning about safety and security
- Formulate the reasoning in terms of model elements and properties
- Not only “axioms and theorems”
Safety and Security Modelling

Stochastic Activity Networks

Boolean logic driven Markov processes

Essential: Separating Policy from Mechanisms

CHESS Modeling Language

Building Blocks

- This is the constructive aspect of SESAMO
- Identify enabling mechanisms
- Create building blocks, underpinned by models of behavior
- This lays the groundwork for trade-off analysis
Analysis Techniques

- This objective continues the constructive aspect of SESAMO
- Building blocks need contextual analysis elements
  - Qualitative
  - Particularly quantitative
  - Including probabilistic
- Analysis accompanies the enabling mechanisms of SESAMO in the study of certification / accreditation issues

Methodology and Process

- This objective moves the project from piecemeal, individual R&D efforts toward the overall environment
- Seeking a methodology (that is: methods, principles, rules) that integrates safety oriented and security oriented considerations into a process
Methodology and Process

Safety and Security Modeling  Building Blocks  Analysis Techniques  Methodology and Process

Safety Goals

Device Functional Requirements

Device Functional Safety Requirements

Device Functional Security Requirements

Safety Analysis

The SESAMO Tool Chain

- An effective tool chain supporting the integrated safety and security methodology
- The tool chain represents the culmination of the operational aspect of SESAMO
Decision Support

- It is a premise of SESAMO that safety and security cannot always be reconciled in a “win-win” manner
- The elaboration of decision support strategies is a natural consequence
  - Not “Sci-Fi AI personal assistants”
  - Rather, explicit and precise descriptions of trade-offs
- Much of this is within the “Analysis” work

Multiple Domains

- Different domains have developed different approaches to safety and security
- Cross-domain harmonization (approach, tools, accreditation) can bring huge benefits
PROJECT ORGANISATION

Objectives & Workpackages

- User requirements & use case specification
- Mechanisms
- Analysis and assessment
- Methodology and tool chain
- Use case development & evaluation

Management

Integrated safety & security

Dissemination and exploitation
Objectives & Workpackages

WP7
Integrated safety & security

WP1
User requirement & use case specification

WP2
Building Blocks

WP3
Safety and Security Modeling

WP4
Analysis Techniques

WP5
Methodology and Process

WP6
Tool Chain

WP8
All Objectives

WP9
Use case development & evaluation

USE CASES
Use cases

- Avionics – EADS
- Automotive e-motor – Infineon / ikv
- Industrial drive – Siemens
- Car infotainment – Peugeot Citroën
- Medical – Infineon / eesy-id
- Railway – Unicontrols / SYSGO
- Smart grid – EDF / FTW

Observations - requirements

- Priorities for information security:
  - Confidentiality / Integrity > Availability
- Priorities for embedded systems:
  - Availability / Integrity >> Confidentiality
- Additional requirements:
  - Autonomous
  - Timeliness
  - Isolation
  - Safety > Security
Observations - process

- Safety is far better understood than security from both a process and a product perspective.
- Some debate about how best to combine safety and security.
- Not clear that applying separate safety and security processes will converge.
- Hence, desirable to develop an integrated process for building a safe and secure system.

Example – verification tests

Source: ED-202 © EUROCAE
Observations - standards

- Most security standards are concerned with information security:
  - ISO 2700x
- However, some new standards are emerging for control system security:
  - ISA 99 / IEC 62443
  - NIST 800-82
- The Common Criteria deal with security assurance rather than secure development

Security-informed safety

- Security requirements are beginning to appear in safety standards
- Clause 1.2 k) of IEC 61508-1:2010:
  - requires malevolent and unauthorised actions to be considered during hazard and risk analysis. [...]"
- Similarly, draft EN 50126-5:2012 states:
  - “The Safety Case shall demonstrate that [...] misuse-based failures on external interfaces do not adversely impact on the safety integrity of the system”
USE CASE EVALUATION

Example - Car Infotainment

- The use case environment
- Positioning the use case
- Relation to WPs

WP1/4: Requirements & Goals Model
  - Integrity Protection
  - Node Authentication
  - Encryption/Decryption

WP2: Building Blocks
  - Integrity Protection
  - Node Authentication
  - Encryption/Decryption

WP3: BDMP Model
  - Attack scenarios (security)
  - Failure scenarios (safety)
### Use cases and building blocks

<table>
<thead>
<tr>
<th>Use case</th>
<th>Authentication and real-time communication</th>
<th>Encryption</th>
<th>Redundancy and diversity</th>
<th>Monitoring in embedded systems</th>
<th>Partitioning</th>
</tr>
</thead>
<tbody>
<tr>
<td>Railway use case</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Smart Grid use case</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>E-motor use case</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medical use case</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industrial drive use case</td>
<td>●</td>
<td>●</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avionics use case</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>●</td>
</tr>
</tbody>
</table>

Note: SESAMO use cases apply further building blocks

---

### Use cases & analysis methods

<table>
<thead>
<tr>
<th>SESAMO use cases</th>
<th>Avionics</th>
<th>Car Infotainment</th>
<th>Industrial Drive</th>
<th>Automotive E-Motor</th>
<th>Oil &amp; Gas</th>
<th>Medical</th>
<th>Railway Communication</th>
<th>Smart Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Integration of safety and security techniques for preliminary analysis</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security-informed safety case</td>
<td></td>
<td></td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stochastic Modelling of Security and Safety at system level</td>
<td>X X X X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative modelling of Safety and Security for interdependent systems</td>
<td></td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative security analysis with attacker strategy models</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Quantitative trade-offs in Communication Networks</td>
<td>X X</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formal Security Analysis of communication Protocols</td>
<td>X X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formal Analysis of information flow</td>
<td>X X</td>
<td>X X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

black: applied in WP3/WP5

green: being considered / applicable
Generic process definition

- Generic safety and security integrated process containing
  - safety and security activities
  - role definitions
  - work products
  - relations to building blocks and analysis methods
- Adapted to the use case domains
- Supported by an initial tool chain

SESAMO Generic Process

[Diagram showing the SESAMO generic process with phases and activities related to safety and security validation.]
SECURITY-INFORMED SAFETY
IEC 61508-1:2010

- Clause 1.2 k
  - “requires malevolent and unauthorised actions to be considered during hazard and risk analysis. The scope of the analysis includes all relevant safety life cycle phases”

- Clause 7.4.2.3
  - “[...] If the hazard analysis identifies that malevolent or unauthorised action, constituting a security threat, as being reasonably foreseeable, then a security threats analysis should be carried out”

- Clause 7.5.2.2
  - “If security threats have been identified, then a vulnerability analysis should be undertaken in order to specify security requirements”

Safety analysis (Yellow book)

- SYSTEM
- Causal Factor
- Hazard
- Accident
- Accident Trigger
- Barrier

Slide 46  ISSE 2014, 8 September 2014

Slide 47  ISSE 2014, 8 September 2014
Safety and Security analysis

Hazard \rightarrow Compromise \rightarrow Threat

Vulnerability

Causal Factor

Accident Trigger

System

Barrier

Accident

Control

Structured Safety Case

“a documented body of evidence that provides a convincing and valid argument that a system is adequately safe for a given application in a given environment”
Security-informed safety cases

- Express safety case about system behaviour in terms of Claims-Arguments-Evidence
- Review how the claims might be impacted by security
- Review security controls to see if these can be used to provide an argument and evidence for satisfying the claim
- Review impact of deploying controls on architecture and implementation
- Iterative layered approach

Impact of security on safety case

- What impact does security have on the safety case?
- Some observations:
  - Supply chain integrity
  - Malicious events post deployment
  - Design changes to address user interactions, training, configuration, vulnerabilities
  - Additional functional requirements - security controls
  - Possible exploitation of the device/service to attack itself or others
- Evidence for effectiveness of controls hard to find
Mapping safety claims onto NIST security controls

<table>
<thead>
<tr>
<th>Claim</th>
<th>Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>C22 Training OK.</td>
<td>Awareness and Training (AT)</td>
</tr>
<tr>
<td></td>
<td>AT-2 Security Awareness</td>
</tr>
<tr>
<td></td>
<td>AT-3 Security Training</td>
</tr>
<tr>
<td>C42 Supply chain integrity</td>
<td>System and Services Acquisition (SA)</td>
</tr>
<tr>
<td></td>
<td>SA-12 Supply Chain Protection</td>
</tr>
<tr>
<td></td>
<td>SA-12-3 Trusted Shipping</td>
</tr>
<tr>
<td></td>
<td>SA-12-7 Independent Analysis and Penetration Testing</td>
</tr>
<tr>
<td>C52 Vulnerabilities and hazards addressed</td>
<td>System and Services Acquisition (SA)</td>
</tr>
<tr>
<td></td>
<td>SA-10 Developer Configuration Management</td>
</tr>
<tr>
<td></td>
<td>SA-11 Developer Security Testing</td>
</tr>
<tr>
<td></td>
<td>SA-13 Trustworthiness</td>
</tr>
</tbody>
</table>

Layered analysis

- **M0 Policy and requirements** – the highest level where we analyse system requirements, safety and security policies
- **M1 Architectural level** – the intermediate level where we analyse the abstract system components combined according to the abstract architecture
- **M2 Implementation level** – the detailed level where we analyse the implementation of specific components and their integration within the specific architecture
DISCUSSION & OUTLOOK

Discussion

- The impact of Security on Safety is widely accepted
- The debate on how deeply the processes have to be integrated is still ongoing
  - Panel discussion at SESAMO Industrial Day has shown wide spectrum of opinions
- Arguments in favor of integrated process
  - Security attacks have the potential to jeopardize safety – must be considered together
  - Mechanisms for safety and security are sometimes similar but sometimes contradictory – need to be analyzed together (otherwise results or constraints may not hold – e.g. for timing)
  - Security shall be considered from beginning of system development (as safety) not “added” later
  - ...
- Arguments against integrated process
  - Lifecycle are not compatible (e.g. security needs frequent updates after SOP)
  - Different teams (experts with different knowledge, skills) required for safety and security
  - Deep integration will cause additional overhead
  - ...

Slide 58  ISSE 2014, 8 September 2014

Slide 59  ISSE 2014, 8 September 2014
Outlook: the SESAMO Approach

1. Tradeoff analysis (e.g. effect of chosen security mechanism on safety)

2. Combined activities (e.g. joint hazard / threat analysis)

Center Stage BBs & Analysis Techniques

The integrated methodology puts the focus on the interaction points

The use case owners and technology providers are collaborating to deploy the BBs and analytic techniques in their domains
For more information…

- On the SESAMO Website:
  - ♦ Public deliverables:
    - • D2.1 *Specification of Safety and Security Mechanisms*
    - • D3.1 *Specification of Safety and Security Analysis and Assessment Techniques*
  - ♦ And coming soon!
    - • D4.2 *Integrated Design and Evaluation Methodology*
- ■ … and many other articles and papers

---

**THANK YOU!**

https://www.sesamo-project.eu

John Favaro, *Intecs S.p.A.*  
Robert Stroud, *Adelard LLP*