1st International Workshop on the Integration of Safety and Security Engineering (ISSE '14)

Laurent Rioux[1] and John Favaro[2]

[1] THALES Research & Technology
1, av Augustin Fresnel, F-91767 PALAISEAU Cedex
laurent.rioux@thalesgroup.com
[2] Intecs S.p.A.
via Umberto Forti 5, 56121 Pisa, Italy
john.favaro@intecs.it

1 Introduction

The growing complexity of critical systems is creating new challenges for safety and security engineering practices: it is now expected that delivered products implement more and more complex features, while respecting strict requirements on safety and security. For such systems, an ever-increasing portion of design effort is therefore spent on safety and security assessment and verification. Applying safety verification without considering security properties is no longer possible since safety decisions have an impact on system security properties and vice-versa.

The challenge addressed by this workshop relates to the inefficiency and ineffectiveness of combining engineering activities related to safety and security properties of the software or the system. The inefficiency relates to the costs and time required to perform both safety and security engineering. The ineffectiveness relates to the potentially redundant or contradictory solutions elaborated by the safety engineering and security engineering activities. These issues are mainly due to the clustering of these two engineering domain activities.

The purpose of the ISSE'14 workshop was to share ideas, experiences and solutions to concretely combine or integrate safety and security engineering activities. As a result, the ISSE'14 workshop aimed at providing a forum for practitioners and researchers to present contributions and share ideas on combining safety and security process, methods, tools and verification techniques and their applicability to industrial critical systems. It also aimed at promoting discussions, closer interaction, cross-fertilization of ideas, and synergies across the breadth of the safety and security research communities, as well as attracting industrial participants from different domains having a specific interest in safety and security verification.

The workshop was conceived with the intention of becoming a unique place to exchange and discuss ideas about the issues and opportunities associated with combining or integrating safety and security engineering. To that end, a questionnaire was distributed to the participants in order to capture the first elements for a community-building effort that would contribute to a sustainable series of workshops in the future.

A. Bondavalli et al. (Eds.): SAFECOMP 2014 Workshops, LNCS 8696, pp. 267–268, 2014.

2 Workshop Format

According to the stated objectives, the workshop was organized primarily as a discussion forum as opposed to a mini-conference. The morning session included summary presentations of results on safety and security integration by the organizing projects MERGE and SESAMO, followed by two invited talks and presentations of research and experience papers selected for their potential to stimulate discussion and debate, including:

- an application of Failure Mode, Vulnerabilities and Effects Analysis (FMVEA) to safety and security analysis of intelligent and cooperative vehicles;
- an adaptation of models devised for safety assessment of avionics platforms in order to analyse their security, with the aim of developing common models and tools to assess safety and security;
- a uniform approach to risk communication in distributed IT environments combining safety and security aspects.

The afternoon session was dedicated to discussions and interactions on challenges in the integration of safety and security engineering. For this, a panel including research representatives promoting different approaches animated a discussion with participation of the attendees, aiming to identify the scientific and industrial stakes in the integration of both engineering domains. The session concluded with a synthesis report agreed by the attendees. This report will be published at the next workshop.

Acknowledgements. The ISSE ’14 workshop was supported by the following projects:

- **Multi-concerns Interactions System Engineering (MERgE).** The ITEA 2 project MERgE (www.merge-project.eu) aims to develop and demonstrate innovative concepts and design tools to address multi-concerns interactions in systems, targeting the elaboration of effective architectural solutions with a focus on safety and security.
- **Safety and Security Modelling (SESAMO).** The ARTEMIS JU SESAMO project (www.sesamo-project.eu) is addressing the root causes of problems arising with convergence of safety and security in embedded systems at architectural level, where subtle and poorly understood interactions between functional safety and security mechanisms impede system definition, development, certification, and accreditation procedures and standards. The SESAMO approach is to develop a component-oriented design methodology based upon model-driven technology, jointly addressing safety and security aspects and their interrelation for networked embedded systems in multiple domains.