

## SALSA

Living Safety&Security Cases for Cyber-Physical Systems Certification

<b>Programm / Ausschreibung</b>	IKT der Zukunft, IKT der Zukunft, IKT der Zukunft - 4. Ausschreibung (2015)	<b>Status</b>	abgeschlossen
<b>Projektstart</b>	01.10.2016	<b>Projektende</b>	30.09.2019
<b>Zeitraum</b>	2016 - 2019	<b>Projektlaufzeit</b>	36 Monate
<b>Keywords</b>	2_Cyber-Physische_Produktionssysteme		

### Projektbeschreibung

Safety Cases sind eine etablierte Methode in Zertifizierungsprozessen eingebetteter Systeme. Sie dienen dazu, Safety-Ziele mit Safety-Lösungen zu nachverfolgbar zu verbinden, und damit den Nachweis von Sicherheitseigenschaften zu erbringen. Aufgrund ihrer mangelnden Unterstützung von Security-Aspekten und von Änderungen skaliert die Technik der Safety-Cases allerdings nicht für komplexe cyberphysikalische Systeme wie z.B. Plattformen für autonomes Fahren oder Industrie 4.0 Infrastrukturen. Unser Ziel innerhalb des SALSA-Projekts ist es, eine neue werkzeuggestützte Methode „lebendiger“ Safety&Security-Cases zu entwickeln, mit einem Fokus auf effizientes Compliance-Management in Kontexten, die durch Heterogenität, organisationsübergreifenden Strukturen, Zertifizierung mehrerer Standards und kurze Release-Zyklen geprägt sind. Kernkonzepte des SALSA-Frameworks sind eine Knowledge Base mit integriertem Workflow-Framework, die das kooperative Management von Safety/Security-Nachweisketten und die Koordination der damit verbundenen Verantwortlichkeiten in Multi-Standard-Kontexten und im System-Release-Management unterstützt. Das SALSA-Framework wird im Kontext einer Plattform für autonomes Fahren evaluiert.

### Abstract

Safety cases are an established method within certification processes of embedded systems. They trace safety goals down to safety solutions, providing evidence for the fulfilment of a system's safety properties. Albeit, safety cases do not scale up to large-scale cyber-physical systems like platforms for autonomous driving or smart factory infrastructures due to the lacking support of security-specific aspects and system changes. Within SALSA, our goal is to develop a novel tool-supported method of "living" safety&security cases enabling efficient compliance management in settings characterized by heterogeneity, cross-organizational structures, certification with respect to multiple standards and short release cycles. Core concepts within SALSA are a Workflow-enhanced Knowledge Base supporting collaborative maintenance of security/safety evidence chains, coordination of tasks in multi-standard contexts and efficient handling of system releases. The SALSA framework will be evaluated in the context of autonomous driving.

### Projektkoordinator

- Universität Innsbruck

## **Projektpartner**

- ITSEC GmbH
- fortiss GmbH
- TrustMotion Austria GmbH
- TTTech Computertechnik AG