VALU3S

Verification and Validation of Automated Systems' Safety and Security

Programm / Ausschreibung	IKT der Zukunft, ECSEL, ECSEL Call 2019_1 (IA) und 2019_2 (RIA)	**Status**	abgeschlossen
Projektstart	01.05.2020	**Projektende**	31.07.2023
Zeitraum	2020 - 2023	**Projektlaufzeit**	39 Monate
Keywords	4_Industry		

Projektbeschreibung

Die Hersteller von hochautomatisierten Systemen und den in solchen Systemen verwendeten Komponenten haben in den letzten Jahren einen enormen Aufwand für Entwicklung und Forschung betrieben. Die Hersteller dieser Systeme müssen sicherstellen, dass die Systeme bestimmungsgemäß und spezifikationsgerecht funktionieren. Das ist keine einfache Aufgabe, da die Komplexität dramatisch ansteigt, je stärker die Integration und die Vernetzung der Systeme zunimmt. Gerade die zunehmende Vernetzung ist ein aktueller Trend, der sich voraussichtlich weiter fortsetzen und beschleunigen wird.

Mit zunehmender Komplexität der Systeme entstehen, durch die Kombination von in sich unproblematischen Komponenten, vermehrt unerwartete, potentiell unerwünschte Eigenschaften. Eine gründliche Verifizierung und Validierung (V&V) dieser Systeme wird dadurch noch dringender erforderlich, aber auch schwieriger. Durch die V&V von automatisierten Systemen sind die Hersteller dieser Systeme in der Lage, sichere und zuverlässige Systeme für die Gesellschaft zu gewährleisten, da Ausfälle in hochautomatisierten Systemen katastrophal sein können.
Das übergeordnete Ziel von VALU3S ist es, ein über die Grenzen von Anwendungsdomänen hinweg anwendbares Verifikations- und Validierungssystem zu schaffen. Es sollen dazu Methoden, Werkzeuge und Konzepte untersucht werden, die für die V&V von automatisierten Systemen in Bezug auf Betriebssicherheits-, Manipulationssicherheits- und Datenschutzanforderungen geeignet sind. VALU3S soll dazu einen wesentlichen Beitrag liefern, indem es die Möglichkeit bietet, Zeit, Kosten und Aufwand von V&V-Prozessen zu reduzieren. Dadurch wird sichergestellt, dass die europäischen Hersteller von automatisierten Systemen wettbewerbsfähig und weltweit führend bleiben.

VALU3s wird ein neuartiges Framework für die V&V von automatisierten Systemen in Bezug auf Sicherheit, Cybersicherheit und Datenschutzanforderungen entwickeln und evaluieren. Zu diesem Zweck werden 13 Anwendungsfälle mit spezifischen Sicherheits-, Schutz- und Datenschutzanforderungen eingehend
untersucht. Es werden Referenzlisten für (i) V&V-Methoden und (ii) Testszenarien, die mit den definierten Methoden genutzt werden, erarbeitet. Dazu werden sowohl gängige V&V-Methoden angewendet und verbessert als auch neue Methoden entwickelt. Ziel ist, Zeit, Kosten und Aufwand für die Durchführung von V&V von automatisierten Systemen zu reduzieren.

Die beiden Referenzlisten zusammen mit dem V&V-Framework dienen der Gestaltung verbesserter Prozessabläufe für die V&V von automatisierten Systemen. Die verbesserten Prozesse werden durch Qualifizierung und Quantifizierung von Sicherheit, Cybersicherheit und Datenschutz sowie anderer Bewertungskriterien anhand von Demonstratoren zu den 13 Anwendungsfällen bewertet werden. VALU3S wird auch die Entwicklung von Sicherheits-, Cybersicherheits- und Datenschutzstandards durch eine aktive Teilnahme an entsprechenden Normungsgremien beeinflussen. VALU3S wird der Test-Community, Ingenieuren sowie Forschern, Leitlinien zur Verfügung stellen, wie die V&V von automatisierten Systemen verbessert werden kann.

VALU3S vereint ein Konsortium mit Partnern aus 10 verschiedenen Ländern, mit einem Mix aus Industriepartnern aus den Bereichen Automobil, Landwirtschaft, Eisenbahn, Gesundheitswesen, Luft- und Raumfahrt, Industrieautomation und Robotik sowie führenden Forschungseinrichtungen und Universitäten, um das Projektziel zu erreichen.

Abstract

Manufacturers of automated systems and the manufacturers of the components used in these systems have been allocating an enormous amount of time and effort in the past years developing and conducting research on automated systems. The effort spent has resulted in the availability of prototypes demonstrating new capabilities as well as the introduction of such systems to the market within different domains. Manufacturers of these systems need to make sure that the systems function in the intended way and according to specifications. This is not an easy task as system complexity rises dramatically the more integrated and interconnected these systems become with the addition of automated functionality and features to them.

With rising complexity, unknown emerging properties of the system may come to the surface making it necessary to conduct thorough verification and validation (V&V) of these systems. Through the V&V of automated systems, the manufacturers of these systems are able to ensure safe, secure and reliable systems for society to use since failures in highly autonomous systems can be catastrophic.

The high-level goal of VALU3S is to create and evaluate a multi-domain verification and validation framework through an investigation of methods, tools and concepts that are suitable for V&V of automated systems with respect to safety, security and privacy requirements. To do so, VALU3S aims to take an important
step forward in the V&V of automated systems by providing the means to improve the time, cost and effort of V&V processes. This will ensure that European manufacturers of automated systems remain competitive and that they remain world leaders.

VALU3s will design and evaluate a novel framework for V&V of automated systems with respect to safety, cybersecurity and privacy requirements. To this end, 13 use cases with specific safety, security and privacy requirements will be studied in detail. Two reference lists are designed and detailed referring to (i) V&V methods and (ii) test scenarios that will be exploited by the methods defined. VALU3S’s reference method list is created by improving commonly-used V&V methods as well as implementing new methods aiming for reducing the time, cost and effort needed to conduct V&V of automated systems. The two reference lists along with the V&V framework are used to design improved process workflows for V&V of automated systems. Several tools will be implemented supporting the improved processes which are evaluated by qualification and quantification of safety, cybersecurity and privacy as well as other evaluation criteria using demonstrators. VALU3S will also

influence the development of safety, cybersecurity and privacy standards through an active participation in related standardisation groups. VALU3S will provide guidelines to the testing community including engineers and researchers on how the V&V of automated systems could be improved considering the cost, time and effort of conducting the tests.

VALU3S brings together a consortium with partners from 10 different countries, with a mix of industrial partners from automotive, agriculture, railway, healthcare, aerospace and industrial automation and robotics domains as well as leading research institutes and universities to reach the project goal.

Projektpartner

- Siemens Aktiengesellschaft Österreich