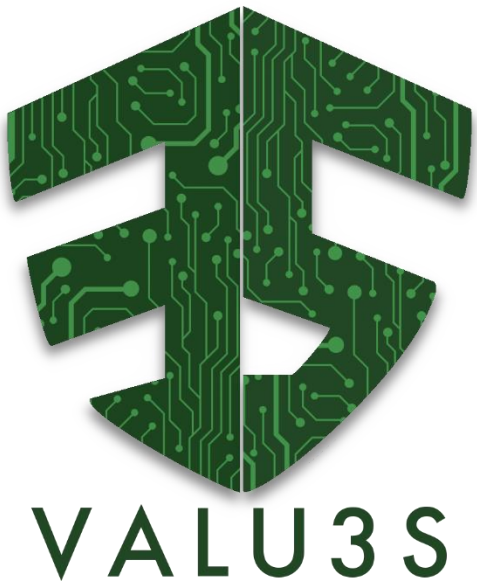


Verification and Validation of Automated Systems' Safety and Security

VALU3S Vocabulary

Document Type	Report
Primary Author(s)	Aleš Smrčka (BUT)
Document Date	2021-11-30
Document Version	1.4 Final
Dissemination Level	Public (PU)
Project Coordinator	Behrooz Sangchoolie, behrooz.sangchoolie@ri.se, RISE Research Institutes of Sweden
Project Homepage	www.valu3s.eu
JU Grant Agreement	876852

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.

Disclaimer

Revision History

Version	Date	Author (Affiliation)	Comment
0.1	2020-09-16	Aleš Smrčka (BUT)	Initial Vocabulary Draft
0.2	2020-10-07	Behrooz Sangchoolie (RISE)	Added some comments on version 0.1
0.3	2020-12-03	Aleš Smrčka (BUT)	Added introduction, modified structure
0.4	2021-01-20	Aleš Smrčka (BUT)	Assigned coordinators for new terms
0.5	2021-05-12	Aleš Smrčka (BUT)	Fixed some of the terms
1.0	2021-09-15	Aleš Smrčka (BUT)	First version
1.1	2021-10-01	Ali Sedaghatbaf (RISE)	Reviewing the first draft.
1.1	2021-11-09	Manuel Schmidt (NXP)	Second Review
1.2	2021-11-11	Aleš Smrčka (BUT)	Accepted recommendations from review
1.3	2021-11-26	Aleš Smrčka (BUT)	Updated references and final modifications
1.4	2021-11-30	Behrooz Sangchoolie (RISE)	First version of the document to be uploaded in the project website.

Chapter 1 Introduction

The systems and software engineering disciplines, techniques, and processes have vastly advanced during past decades. The progress is so rapid that terminology is updated in different domains simultaneously, which allows more definitions representing the same thing or unambiguous definitions leading to misunderstanding and faults in designs. Different standards cope with this problem by identifying terms used in the field of information technology and by providing definitions for these terms. Even though such vocabularies and glossaries include clearly defined terms, they either provide several different but similar meanings for different topics or do not include terms that are newly introduced in current research projects. This document was prepared to collect terms used specifically in the context of the VALU3S project and to unify or narrow down their definitions.

The vocabulary is continuously updated during the development of the VALU3S project. This document is the first version consisting of terms with definitions already agreed by the VALU3S consortium.

Chapter 2 Vocabulary

asset
(with regard to security engineering) is anything of value that should be protected from malicious harm [1].

attack
1. an attempt to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset [2], **2.** a series of steps taken by an attacker to achieve an unauthorized result [3].

authentication
1. the provision of assurance that a claimed characteristic of an entity is correct [2], **2.** the process of verifying a claim that a system entity or system resource has a certain attribute value [4], [5].

automated systems
systems that reduce or eliminate human interventions in processes. In the case of VALU3S, these processes are connected to the project target domains, namely: Automotive, Aerospace, Industrial robotics, Healthcare, Agriculture and Railway.

criteria
specific data items identified as contents of information items for appraising a factor in an evaluation, audit, test or review [6].

critical system
system having the potential for serious impact on the users or environment, due to factors including safety, performance, and security [7].

cybersecurity (and key concepts)
security of cyberspace, where cyberspace itself refers to the set of links and relationships between objects that are accessible through a generalised telecommunications network, and to the set of objects themselves where they present interfaces allowing their remote control, remote access to data, or their participation in control actions within that cyberspace. Cybersecurity shall therefore encompass the CIA paradigm (confidentiality, integrity, and availability) for relationships and objects within cyberspace and extend that same CIA paradigm to address protection of privacy for legal entities (people and corporations), and to address resilience (recovery from attack) [8]. The CIA paradigm refers to the primary cybersecurity attributes. There are also secondary attributes that cybersecurity shall encompass; examples of these attributes are privacy, non-repudiation, authenticity, and freshness [9], [10].

design
1. (process) to define the architecture, system elements, interfaces, and other characteristics of a system or system element, **2.** result of the process as defined in [11], [12].

documentation
written or pictorial information describing, defining, specifying, reporting, or certifying activities, requirements, procedures, or results [13].

error
incorrect state of the system [14], cf. human error.

fault
abnormal condition that can cause an element or an item to fail [15] [9].

failure
termination of the ability of an element or an item to perform a function as required [15] [9].

functional safety
1. part of the overall safety relating to the EUC (Equipment Under Control) and the EUC control system that depends on the correct functioning of the E/E/PE (Electrical/Electronic/Programmable Electronic) safety-related systems [16], **2.** absence of unreasonable risk due to hazards caused by malfunctioning behaviour of E/E (electrical and/or electronic) systems, where hazard is a potential source of harm caused by malfunctioning behaviour of the item [15].

evaluation
action that assesses the value of something [17].

human error
human action that produces an incorrect result [18], cf. error.

incident
a group of faults/attacks that can be distinguished from other faults/attacks because of the distinctiveness of the source of faults/attacks, objectives, sites, and timing [3].

privacy (and key concepts)
degree to which unauthorized parties are prevented from obtaining "personal" sensitive information [1]. Note that, here “personal” is added to the Firesmith’s definition to explicitly address the concern connected to the personal information. Privacy includes the following subfactors:

- Anonymity is the degree to which the users' identities are prevented from unauthorized storage or disclosure.
- Confidentiality is the degree to which sensitive information is not disclosed to unauthorized parties (e.g., individuals, programs, processes, devices, or other systems).

The above definition is also in line with the definition provided in [19], according to which, privacy is guaranteed if the relation between an entity and a set of information is confidential. Thereby, anonymity is the property that the relation between an entity and its identity is confidential.

requirement
condition or capability that must be met or possessed by a system, system component, product, or service to satisfy an agreement, standard, specification, or other formally imposed documents [20].

safety (and key concepts; some are already included, such as error, fault, failure)
1. freedom from unacceptable risk where risk could be defined as a combination of the probability of occurrence of harm and the severity of that harm [16], **2.** absence of catastrophic consequences on the user(s) and the environment [9].

safety/cybersecurity/privacy requirement
requirement that is needed to ensure the safety/cybersecurity/privacy of the product [21].

system
programmable electronic system and electrical/electronic/programmable electronic system: system for control, protection or monitoring based on one or more programmable electronic or electrical/electronic programmable electronic (E/E/PE) devices, including all elements of the system such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices [22].

target domain
targeted industry, where the use cases are selected from. In case of VALU3S, the target domains are Automotive, Aerospace, Industrial robotics, Healthcare, Agriculture and Railway [23].

test case
set of preconditions, inputs (including actions, where applicable), and expected results, developed to drive the execution of a test item to meet test objectives, including correct implementation, error identification, and checking quality and other valued information [24].

testing
quality assurance activity in which systems, subsystems, or components are executed under specified conditions, the results are observed or recorded, and an evaluation is made of some aspect of the system or component [25].

threat
potential cause of an unwanted incident, which can result in harm to a system or organization [2].

user story
simple narrative illustrating the user goals that a software function will satisfy [26], [27].

validation
1. confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled [28], [11], [12], **2.** process of providing evidence that the system, software, or hardware and its associated products satisfy requirements allocated to it at the end of each life cycle activity, solve the right problem (e.g., correctly model physical laws, implement business rules, and use the proper system assumptions), and satisfy intended use and user needs [29].

verification

1. confirmation, through the provision of objective evidence, that specified requirements have been fulfilled [30], [28], [11], [12], **2.** process of evaluating a system or component to determine whether the products of a given development phase satisfy the conditions imposed at the start of that phase [29].

References

[1] D. Firesmith, "Common Concepts Underlying Safety, Security, and Survivability Engineering.," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, CMU/SEI-2003-TN-033., 2003.

[2] "ISO/IEC 27000:2020 — Information technology — Security techniques — Information security management systems — Overview and vocabulary".

[3] J. D. Howard and T. A. Longstaff, "A Common Language for Computer Security Incidents," Sandia National Laboratories, Albuquerque, New Mexico 87185 and Livermore, California 94550, techreport SAND98-8667., 1998.

[4] Network Working Group, "RFC 4949: Internet Security Glossary," https://datatracker.ietf.org/doc/html/rfc4949, 2007.

[5] BUT et al., "Deliverable D5.2 - Final demonstration plan and a list of evaluation criteria," VALU3S Consortium, Oct. 31, 2021..

[6] "ISO/IEC/IEEE 15289:2015 — Systems and software engineering — Content of life-cycle information products (documentation)".

[7] "ISO/IEC 29110-2-1:2015 — Software engineering — Lifecycle profiles for Very Small Entities (VSEs) — Part 2-1: Framework and taxonomy".

[8] C. Brookson, S. Cadzow, R. Eckmaier, J. Eschweiler, B. Gerber, A. Guarino, K. Rannenberg, J. Shamah and S. Gorniak, "Definition of Cybersecurity-Gaps and overlaps in standardisation," Heraklion, ENISA. , 2015.

[9] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," In IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, doi: 10.1109/TDSC.2004.2., 2004.

[10] A. Lautenbach et al., "Deliverable D2.0, Security models," HEAVENS (HEAling Vulnerabilities to ENhance Software Security and Safety). Project deliverable., 2016.

[11] "ISO/IEC TS 24748-1:2016 — Systems and software engineering — Life cycle management — Part 1: Guide for life cycle management".

[12] "ISO/IEC/IEEE 15288:2015 — Systems and software engineering — System life cycle processes".

[13] "ISO 24765-217 — Systems and software engineering — Vocabulary".

[14] "ISO/IEC 15026-1:2013 — Systems and software engineering — Systems and software assurance — Part 1: Concepts and vocabulary".

[15] "ISO 26262-1:2018 — Road vehicles — Functional safety — Part 1: Vocabulary".

[16] "ISO/IEC Guide 51:2014 — Safety aspects — Guidelines for their inclusion in standards".

[17] "ISO/IEC 15414:2015 Information technology — Open distributed processing — Reference model — Enterprise language".

[18] "IEEE 1044-2009 — IEEE Standard Classification for Software Anomalies".

[19] EVITA Project Consortium, "Deliverable D2.3 - Security requirements for automotive on-board networks based on dark-side scenarios," EVITA (E-Safety Vehicle Intrusion Protected Applications), http://www.evita-project.org/., 2009.

[20] "IEEE 730-2014 — IEEE Standard for Software Quality Assurance Processes".

[21] "ISO/IEC TS 15504-10:2011 — Information technology — Process assessment — Part 10: Safety extension".

[22] "IEC 61508-4 — Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems (E/E/PE, or E/E/PES, Part 4: Definitions".

[23] VALU3S Consortium, "Grant Agreement, Project number 876852 — VALU3S," May 2020.

[24] "ISO 29119-1-2013 — Software testing — Concepts and definitions".

[25] "IEEE 610-1990 — IEEE Standard Computer Dictionary: A Compilation of IEEE Standard Computer Glossaries".

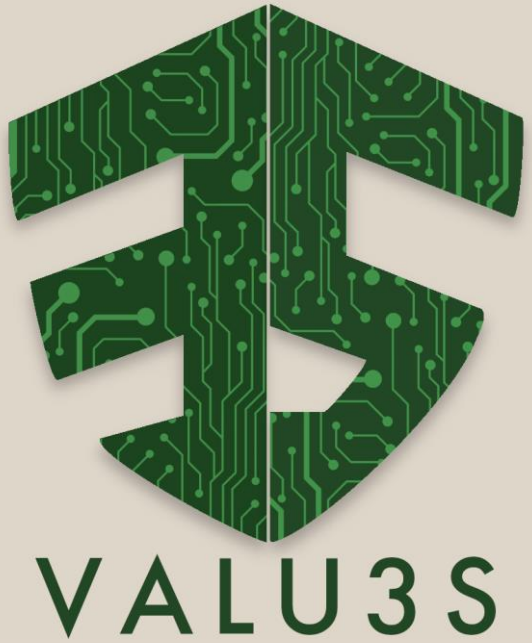
[26] "ISO/IEC/IEEE 26515: 2011 — Systems and software engineering — Developing user documentation in an agile environment".

[27] MGEP et al., "Deliverable D2.2 - Final multi-dimensional layered framework," VALU3S Consortium, Dec. 31, 2020.

[28] "ISO/IEC 25000:2014 — Systems and software Engineering — Systems and software product Quality Requirements and Evaluation (SQuaRE) — Guide to SQuaRE".

[29] "IEEE 1012-2012 — IEEE Standard for System and Software Verification and Validation".

[30] "ISO/IEC 12207:2008 — Systems and software engineering — Software life cycle processes".



www.valu3s.eu

ECSEL Joint Undertaking
Electronic Components and Systems for European Leadership

This project has received funding from the ECSEL Joint Undertaking (JU) under grant agreement No 876852. The JU receives support from the European Union's Horizon 2020 research and innovation programme and Austria, Czech Republic, Germany, Ireland, Italy, Portugal, Spain, Sweden, Turkey.