Defence-related Research Action - DEFRA

ACRONYM: AMC3

Title: Automated Methodology for Common Criteria Certification

Duration of the project: 01/02/2024 - 31/07/2027

Key words: cybersecurity, certification

Budget: 1.673.000 €

of which RHID contribution: 1.590.634€

PROJECT DESCRIPTION

Belgian Defence is increasingly relying on software, both in terms of pure software applications as well as in the form of cyber-physical systems. When this software suffers from defects, vulnerabilities and weaknesses, attackers might exploit its inherent vulnerabilities and tamper with mission critical systems or exfiltrate sensitive information. In order to mitigate this risk and ensure that software is dependable and trustworthy, certification and accreditation activities have traditionally been integrated into the software lifecycle. Software assurance through certification and accreditation suffers from the fact that these processes are extremely resource and time consuming. A structured and to a large extent automated/agile approach that takes into account software updates must therefore be developed. The ARCOS initiative shows that US Defence is rapidly evolving towards higher levels of cybersecurity maturity, which implies a more thorough assessment of all the software and systems that are approved to operate inside one of the classified or unclassified networks within military organisations.

The aim of AMC3 is to realise this vision and apply it to the Belgian Defence sector. AMC3's goals are (1) to modernise Defence cybersecurity certification processes, and (2) to automate the process and drastically decrease human load. Indeed, given the ever-larger number of IT and OT systems that are in use at Belgian Defence, and the always increasing complexity of these systems, a proper management of the inherent cybersecurity risk requires that the internal accreditation process is supported by an approach that is based on automating major parts of the process with trustable powerful techniques. To achieve this, AMC3 offers automatic simulation-based (formal) verification and monitoring that can produce evidence while preserving traceability to facilitate mining and automatically build assurance case argumentation. As a large portion of the input to the accreditation process is to be provided by the manufacturer of the software/ system, it is important to involve the Defence industry as well as Defence itself with its internal developments. The internally developed MASFAD system will serve as an experimentation and validation use case throughout the project. The aim is to validate the AMC3 methodology, and especially the interaction/collaboration between the development team and the military accreditation cell. It is precisely the goal of this project to develop a methodology for performing automated certification and accreditation, assemble a set of tools that support this methodology, and validate the methodology on two typical Defence related use cases.

The first use case is an in-house developed Advanced Persistent Threat (APT) detection tool for protecting government and military networks, while the second is a weapon-system piece of software.

AMC3 will be divided into three phases that cover all the issues related to automatic certification: (1) development of a methodology for automatic certification accompanied by adequate efficient validation techniques, (2) consideration of incrementality and updating to identify new requirements and evidence to be produced, (3) automating runtime certification monitoring, and technical/cost analysis. Two case studies will be used. The first, MASFAD, comes from RMA and is an IDS that is deployed as a digital twin on a simulated but relevant representation of the Defence network. It will mainly be used during phases 1 and 2. The second, FNH SAM, is offered by FN Herstal. This is an armament management software already in production and that will mainly be used in phase 3. These two case studies will respectively make it possible to develop the methodology and to carry out a technical and economic analysis to estimate the cost benefit of implementing the methodology or parts of it into an industrial solution.

Lessons-learned on the MASFAD use-case will have a direct impact on the certification and accreditation processes within Belgian Defence and will reinforce cyber resilience of classified and unclassified military networks. The use case in collaboration with FNH applies the AMC3 methodology to FN® SAM with a potential direct impact on Belgian Defence as FN® SAM has been evaluated with a proof of concept in 2021 and is undergoing a pre- deployment in 2023. The objective is to target a full deployment later to manage the whole fleet of weapons of Belgian Defence. The results of AMC3 will therefore be incrementally deployed to the operational solution of FN® SAM to reinforce the security of the whole solution. To enable uptake of the AMC3 methodology, a cost/benefit analysis will be carried out.

AMC3 will produce the following impactful main outcomes: the AMC3 Methodology and its prototype platform, validated in scalability and cost effectiveness on two industrial case studies. The innovations enable the adoption of more agile DevOps methodologies that are sufficiently rigorous to certify newly developed or updated software for Belgian Defence. The beneficiaries of this new methodology are Defence actors (direct or supply-chain) and their suppliers, as well as the entire socio-economic fabric confronted with automatic certification. To achieve maximum impact, project results will be disseminated towards Belgian (CCB) and international certification bodies, including Horizon Europe projects working on the topic of automated certification.

CONTACT INFORMATION

Coordinator
Axel Legay
UCLOUVAIN/ Pôle en ingénierie informatique
e-mail: axel.legay@uclouvain.be

Partners
Philippe Massonet
CETIC/ Business Research Alignment
e-mail: philippe.massonet@cetic.be

Wim Mees
RMA/ Communications, Information Systems and Sensors (CISS)

e-mail: Wim.Mees@mil.be

Yves Roskam
FN Herstal S.A./ FN Herstal Business Development
e-mail: Yves.Roskam@fnherstal.com

LINK(S)

Temporary link: https://www.cetic.be/AIDE-en