Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats

Sprawozdania

Informacje na temat projektu

certMILS

Identyfikator umowy o grant: 731456

Strona internetowa projektu

DOI
10.3030/731456

Projekt został zamknięty

Data podpisania przez KE
27 Listopada 2016

Data rozpoczęcia
1 Stycznia 2017

Data zakończenia
30 Czerwca 2021

Finansowanie w ramach
INDUSTRIAL LEADERSHIP - Leadership in enabling and industrial technologies - Information and Communication Technologies (ICT)

Koszt całkowity
€ 5 516 543,75

Wkład UE
€ 3 999 055,63

Koordynowany przez
TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH
Austria

Periodic Reporting for period 3 - certMILS (Compositional security certification for medium- to high-assurance COTS-based systems in environments with emerging threats)

Okres sprawozdawczy: 2020-01-01 do 2021-06-30

Podsumowanie kontekstu i ogólnych celów projektu

Previously isolated physical systems have become connected to the Internet, thus becoming cyber-physical systems (CPS). For instance, in transportation, for passenger as well as operator comfort, almost all means (airplanes, trains, cars, and ships) are networked. Due to the potential of a malicious attacker the security of CPS has obtained a lot of interest. However, unlike many other IT systems, CPS usually have been heavily scrutinised for safety for decades. While the safety protection against accidental faults does not address security, there are already established safety methods as well as “safety certification stakeholders”. Securing and certifying CPS therefore must respect the existing safety certification processes.
certMILS developed a security certification methodology for CPS, which are characterised by safety-critical nature, complexity, connectivity and open technology. We aimed to increase the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety and security certification of composable systems. "MILS" in certMILS stands for "Multiple Independent Levels of Safety/Security", indicating that certMILS uses a special kind of operating systems called "separation kernel" (SK). This kind of operating system is highly deterministic and reliable and puts user functionality into the application layer.
certMILS generated interaction between developers, evaluation laboratories and certification authorities in three European countries creating standardised and validated compositional methodology for evaluating and certifying high assurance products; modular protection profile (PP) for SKs, addressing also hardware aspects for Common Criteria (CC) for Information Technology Security standard; evaluation of an SK according to this PP; guidance for developers and evaluators; assurance preservation throughout operational deployment. Our approach was applied to three industrial pilots (smart grids, railway, subway).

Prace wykonane od początku projektu do końca okresu sprawozdawczego oraz najważniejsze dotychczasowe rezultaty

Activity 1: Compositional Methodology for Security Certification
WP1 "Baseline for compositional evaluation": Partners with security and safety backgrounds summarized existing compositional security regulations/interpretations (D1.1) what tools/ techniques exist (D1.2) how to do compositional certification for an SK-based product (D1.3).
WP2 "Standardisation of MILS integration methodology": We drafted the Base MILS Protection Profile (D2.1) using the Security Target (ST) and evaluated that it meets CC content requirements. We identified potential PP Modules that could be of use for the MILS community for additional functionality (D2.2). We edited the Base PP and PP Modules in parallel due to interdependency. We created templates for a security architecture (D2.3) and guidance for using an SK to build secure CPS systems (D2.4).

Activity 2: MILS Platform Certification
WP3 "MILS platform definition" served for the certification of an SK. We studied how the modular PP of WP2, consisting of a base PP and PP modules, represents this ST. We asked for certification body

feedback.
WP4 "MILS platform enhancement" developed a security testing methodology, considering the relevant standards CC and IEC 62443 and fuzzing to discover hard to find vulnerabilities. We implemented a certifiable partitioned network driver with accelerators and described a certifiable MILS design of secure boot and update.
WP5 "MILS platform certification" provided assurance that the MILS SK works as specified in the ST. We reviewed product and development artefacts incl. the ST itself, documentation related to the product life cycle, development and guidance. We did testing and vulnerability analysis and produced evaluation reports for all CC activities.

Activity 3: Certification Pilots
WP6 "Pilot: Smart Grid": For medium-assurance, a pilot was based on Industrial and Automation Control System (IACS) of an electrical substation incl. Remote Terminal Units (RTU). We defined the security scope for the pilot, considering the standards IEC 62443 and CC. A master-slave configuration with control, communication and acquisition RTU devices was implemented. To scale the pilot from medium to high assurance, a compositional security design (with WP2 input) was made. We ported the RTU architecture to PikeOS and evaluated the results according to IEC.
WP7 "Pilot Railway": The use case demonstrator (security gateway) was presented and the railway pilot described. Security requirements based on IEC 62443 for the pilot were defined and the pilot implemented. Evaluation and certification were done for IEC 62443-4-1 and IEC 62443-4-2.
WP8 "Pilot Subway": We specified the HW platform and operational environment of the demonstrator, defined SW components, which must be implemented to create application “T-composition” and defined standards to show the principles and procedures for the implementation, acceptance and subsequent certification, and the pilot was implemented. Evaluation and certification were done for IEC 62443-4-1 and IEC 62443-4-2.

Activity 4: Management, dissemination and exploitation
We created a corporated identity to make certMILS recognisable in conferences, workshops and events. We set up an IT infrastructure, a website, social media and a Zenodo community for public deliverables. We validated our SK protection profile approach by soliciting feedback from SK experts (D9.2). We organized three MILS workshops with proceedings on Zenodo, published several papers incl. joint papers reporting on the consortium’s security certification experience of CPS under CC and IEC 62443 and based on the MILS architecture, and seven newsletters. To compensate for cancelled conferences due to the Covid-19 pandemic in 2020 and 2021, new dissemination activities were carried out. For instance, a podcast series and two videos about certMILS were published. Kick-off, technical and Advisory Board meetings and monthly telcos were held regularly and risk assessment continuously performed.

Innowacyjność oraz oczekiwany potencjalny wpływ (w tym dotychczasowe znaczenie społeczno-gospodarcze i szersze implikacje społeczne projektu)

Our approach to use PP modules for certification (D2.1 D2.2) proved to be a good choice: when we started certMILS, modular PPs only had been proposed; but since April 2017 modular PPs are integrated into mainline CC. certMILS produced 11 additional PP modules for components that can be used as modules, far beyond initial expectations. The approach was validated with SK experts (D9.2). We initiated a CC users forum working group, with SK vendors (4 p.), certification bodies (2 p.), evaluation laboratories (5 p.), hardware vendors (2 p.), Tier-1/2 (3 p.), 1 academic.
certMILS participated in IECEE for IEC 62443. Partners EZU and THA achieved one of the first IEC 62443-4-1 certifications worldwide. We learned that some standards are aware of each other, e.g. early versions of IEC 62443 IsaSecure SDLA explicitly acknowledges validity of CC certification for OS (although this was replaced by more generic wording later).
The certMILS approach to modular design, assurance and certification fosters safe and secure development of heterogeneous systems, increasing security assurance and decreasing costs. We formulated an approach how to use CC assurance for a SK for IEC 62443 (D1.3) security architecture templates (D2.3) and guidance for composed systems using IEC 62443 and CC (D2.4). We worked on system development processes that consider security throughout the development cycle (D1.3 D4.1) and validated this work in three pilots.

certMILS Logo

Ostatnia aktualizacja: 10 Stycznia 2022

Permalink: https://cordis.europa.eu/project/id/731456/reporting/pl