ADMORPH: TOWARDS ADAPTIVELY MORPHING EMBEDDED SYSTEMS

The domain of Cyber-Physical Systems (CPS) is one of the largest information-technology sectors worldwide and a driver for innovation in many other crucial industrial sectors such as health industries, industrial automation, avionics and space. The embedded computer systems in these physically-entangled CPS increasingly rely on complex system architectures. Oftentimes these architectures are heterogeneous multi-core or many-core systems, which are distributed and connected via complex networks. Highly distributed and networked systems entrusted with the control of physical assets are called Cyber-Physical Systems of Systems (CPSoS).

Designers of these CPS(oS) face several daunting challenges as these systems have to meet a range of stringent extra-functional design requirements in terms of e.g. real-time performance and energy efficiency. Mission- and safety-critical CPS(oS), like those in the avionics and space domains, usually also demand ultra-high levels of dependability. This is becoming even more important as the levels of system autonomy rise. With advanced levels of autonomy, more and more systems that were traditionally not considered safety-critical now become safety-critical. Furthermore, as mission- and safety-critical CPS(oS) become increasingly connected, they receive more and more attention from attackers, which may also render these systems unreliable and unavailable and thus potentially cause dangerous situations. To provide a high degree of reliability, availability, and safety, mission- and safety-critical CPS(oS) need to be able to cope with various disruptive events, which could be related to hardware component failures or cyber-attacks aimed at disrupting the system or worse, attacks compromising software components with the goal of taking over critical system functionality.

System adaptivity, foremost in terms of dynamically remapping of application components to processing cores, represents a promising technique to fuse fault- and intrusion tolerance with the increasing performance requirements of these mission- and safety-critical CPS(oS). In the ADMORPH project, we evaluate this hypothesis using a novel, holistic approach to the specification, design, analysis and runtime deployment of adaptive, i.e., dynamically morphing, mission- and safety-critical CPS(oS) that are robust against both component failures and cyber-attacks. To this end, we will address four aspects that are instrumental for the realization of these adaptively morphing systems: (i) the formal specification of adaptive systems, e.g. by means of a coordination language to specify system requirements and adaptivity strategies; (ii) adaptivity methods like strategies for maintaining safe and secure control of CPS(oS); (iii) analysis techniques for adaptive systems to e.g. perform timing verification of adaptive systems to avoid timing violations after system reconfigurations; and (iv) run-time systems for adaptive systems that realize the actual run-time system reconfigurations to achieve fault and intrusion tolerance. The developed technology will be evaluated using three industrial use cases taken from the radar surveillance systems, autonomous operations for aircrafts, and transport management systems domains.

FUNDED UNDER: H2020-EU.2.1.1, Grant agreement ID: 871259
START/END DATE: 1 January 2020 – 31 December 2022
KEY THEMES: Cyber-Physical Systems (of Systems), Fault-tolerance, Intrusion-tolerance, Adaptive systems, Mission- and safety-critical systems, Run-time systems, Analysis of adaptive systems
PARTNERS: University of Amsterdam (NL, Coordinator), Thales Nederland B.V. (NL), SYSGO S.A.S. (FR), University of Luxembourg (LU), Lund University (SE), United Technologies Research Centre Ireland (IE), Q-Media (CZ), FCIENCIAS.ID (PT), University of Augsburg (DE)
BUDGET: € 4.499.468

www.admorph.eu
LinkedIn: https://www.linkedin.com/in/admorph/
Twitter: https://twitter.com/ADMORPH1



Pictures from the kickoff meeting 29 & 30 January 2020