Chapter 6

Runtime Safety Assurance for Adaptive Cyber-Physical Systems:

ConSerts M and Ontology-Based Runtime Reconfiguration Applied to an Automotive Case Study

Tiago Amorim
Fraunhofer IESE, Germany

Daniel Schneider
Fraunhofer IESE, Germany

Denise Ratasich
Vienna University of Technology, Austria

Mario Driussi
Kompetenzzentrum - Das virtuelle Fahrzeug Forschungsgesellschaft mbH, Austria

Georg Macher
AVL List GmbH, Austria

Radu Grosu
Vienna University of Technology, Austria

Alejandra Ruiz
Tecnalia, Spain

ABSTRACT

Cyber-Physical Systems (CPS) provide their functionality by the interaction of various subsystems. CPS usually operate in uncertain environments and are often safety-critical. The constituent systems are developed by different stakeholders, who – in most cases – cannot fully know the composing parts at development time. Furthermore, a CPS may reconfigure itself during runtime, for instance in order to adapt to current needs or to handle failures. The information needed for safety assurance is only available at composition or reconfiguration time. To tackle this assurance issue, the authors propose a set of contracts to describe components' safety attributes. The contracts are used to verify the safety robustness of the parts and build a safety case at runtime. The approach is applied to a use case in the automotive domain to illustrate the concepts. In particular, the authors demonstrate safety assurance at upgrade and reconfiguration on the example of ontology-based runtime reconfiguration (ORR). ORR substitutes a failed service by exploiting the implicit redundancy of a system.

DOI: 10.4018/978-1-5225-2845-6.ch006

INTRODUCTION

For over 20 years, the trend towards more collaboration has been prevalent for rather closed systems, such as communicating ECUs within a vehicle. But roughly since the 2000s, it has been extended towards open systems such as dynamic compositions of different vehicles, traffic infrastructure, and Internet-based services. New computing paradigms have been coined along the way, most notably pervasive computing, ubiquitous computing, ambient intelligence, and cyber-physical systems. At the heart of these paradigms, different types of computer-based systems, from different application domains (of information systems as well as of embedded systems), and from different manufacturers, collaborate with each other to render higher-level services that a single system would be unable to provide. The systems are integrated - more often dynamically, that is during runtime - into so-called Systems of Systems (SoS), which consist of different collaborating systems (i.e., entities encompassing both hardware and software) that might in turn be built upon multi-core technology and host several applications. Moreover, dynamic application updates, reconfigurations or adaptations are most probably a key feature of many future systems to gain in resilience and flexibility. Technologically, this is driven by ever more closely interconnected distributed embedded systems of systems running under the umbrella terms of cyber-physical systems (CPS) and Internet of Things (IoT).

However, whereas CPS offer tremendous potential for new applications, they also impose significant challenges regarding the assurance of safety. In critical domains, nondeterministic reconfiguration and inadequate safety assurance might result in unacceptable system-inherent risks related to (per typical "safety" definition) physical harm to people, but also to financial loss or damage to the environment.

In most critical domains, assurance activities are guided by functional safety standards. Such standards typically provide means for risk identification and classification and, based thereon, give guidance as to how the risk shall be reduced to an acceptable level and how this shall be documented. To this end, current practice requires that the entire system and all system contexts are well defined and understood at design time so that the necessary analyses can be conducted, measures can be introduced and a sound and comprehensive safety argument can be designed. This prerequisite is clearly not fulfilled by *adaptive* CPS due to the uncertainty of dynamic compositions and reconfigurations, which can hardly be foreseen and analyzed before runtime. Thus, for future CPS contexts, established safety engineering approaches and standardization can therefore not be readily applied.

In typical CPS domains, e.g., automotive or railway, there is often no easy way to bring the system into a safe state. This is because we often demand from a CPS to be fail-operational, i.e., the system should preserve a degraded functionality or limited operation in case of failures rather than just switching to a safe mode (fail-safe). This is especially crucial, e.g., when dealing with autonomous vehicles where the driver is no longer the actor who will take control of the system in case of a failure. The system shall make decisions to ensure the safety of its passengers. A fail-operational functionality makes the system go through different states where a failure is detected, the hazard is avoided, and finally the system provides a solution to maintain its functionality without any interruption. While self-adaptation or runtime reconfiguration is already being applied in several domains (e.g., in the Worldwide Web where clients, servers, and gateways continuously change) and with different objectives (e.g., fault tolerance or resource management), the approach is hardly used in CPSs. The reason is mostly because of the aforementioned complexity issues and the fact, that CPSs typically have to provide a temporally correct behavior and need to be predictable to ensure safe operation.