Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 95 (2016) 32 – 39

Procedia
Computer Science

Complex Adaptive Systems, Publication 6
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2016 - Los Angeles, CA

Topology-Based Safety Analysis for Safety Critical CPS

Jean-Yves Choley[a]*,Faïda Mhenni[a], Nga Nguyen[b], Anis Baklouti[a]

[a]*Quartz Laboratory,Supméca, 3 rue Fernand Hainaut, 93400 Saint-Ouen, France*
[b]*Quartz Laboratory, EISTI, Avenue du Parc, 95000 Cergy-Pontoise, France*

Abstract

Since Cyber-Physical Systems (CPS) may exhibit different structures and emergent behaviours during different operational phases, while also being safety critical, it is useful to perform systematic safety analyses tightly relying on the functional and components topologies of such systems. Our proposal is to perform FMEA and FTA analyses as soon as possible in the CPS design process in order to identify and mitigate the risks related to some safety critical structures and behaviours. Thus, these preliminary analyses enable to propose relevant design modifications and improvements such as optional or additional redundancies, components repairability capabilities or relevant control strategies, taking into account the complexity and the potential variability of the structure and the behaviour of the systems. This work derives from previous MBSE (Model-Based System Engineering) and MBSA (Model Based Safety Analysis) integration studies, performed during the early phases of the design of safety critical mechatronic systems, including interconnection components and multi-physical interactions. It relies mainly on M2M (Model to Model) and M2T (Model to Text) transformations and appropriate SysML metamodeling. The proposed CPS safety analysis methodology is illustrated using an aeronautic industrial case study.

Keywords: CPS; mechatronics; systems engineering; MBSE; safety analysis; MBSA; FMEA; FTA; topology

* Corresponding author. Tel.: +33-149452921; fax: +33-149452929.
E-mail address: jean-yves.choley@supmeca.fr

doi:10.1016/j.procs.2016.09.290

1. Introduction

CPS (Cyber-Physical Systems) are cross-domain systems that rely on mechatronics at the interface between the physical world, mainly dealing with energy and material, and the cyber world, mainly dealing with data, information and knowledge. They include actuators and sensors, along with embedded systems for real-time computing, connection to computing resources and human-machine interfaces, as proposed in Fig. 1. Rather than to oppose mechatronics and CPS as usually studied, this scheme highlights the integration of numerous mechatronic devices in a CPS structure, thus implicitly generating CPS related requirements to be taken into account when designing a mechatronic subsystem.

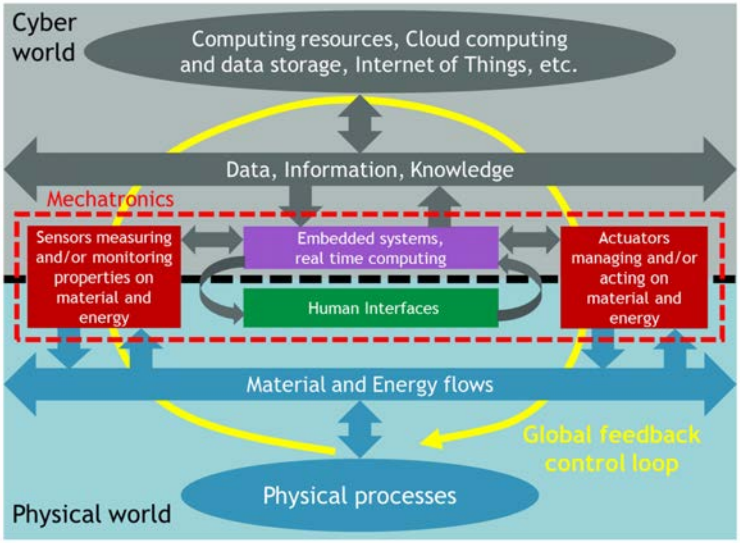
Cyber world
Computing resources, Cloud computing and data storage, Internet of Things, etc.
Data, Information, Knowledge
Mechatronics
Sensors measuring and/or monitoring properties on material and energy
Embedded systems, real time computing
Human Interfaces
Actuators managing and/or acting on material and energy
Material and Energy flows
Global feedback control loop
Physical processes
Physical world

Fig. 1. Partial view of the interface between cyber and physical worlds

Most CPS are also complex systems with potentially dynamically variable topology, meaning that some components, being physical, cyber or interfaces between physical and cyber worlds, may appear or disappear from the structure of the system. Consequently, the system may exhibit new emergent behavior, thus needing some careful safety analyses for safety critical CPS. Our main goal is to deal with safety requirements as soon as possible in the design process of complex systems, with an integrated MBSE-MBSA framework that allows the generation of safety artifacts, such as FMEA and FTA, directly analyzing the topology of the system. Thus, even with a varying topology, it may be possible to perform safety analyses that encompass most of the dysfunctional behavior of CPS.

The paper is organized as follows. First, a short overview of related works about the integration of safety analysis within a SysML-based systems engineering approach is given in section 2. Then, the proposed integrated process, called SafeSysE, is detailed in section 3, and illustrated with a FCS (Flight Control System) use case in section 4. Finally, the paper is concluded in section 5 with a discussion and some future works.

2. Related works

CPS and mechatronic systems similarities and differences are highlighted by Guérineau et al[1], and a metrics-based approach is proposed in order to define the best relevant design methodology. Among existing design methodologies relevant for complex systems, merging MBSE and MBSA processes have been studied in many different ways such as sharing a common SE-SA (Systems Engineering – Safety Analysis) safety data base[2,3], a more simple strategy that consists in only sharing safety information[4], or a more elaborated one in performing direct SE-SA automated models transformations[5,6]. Taking into account the variability of the topology of a CPS when performing safety analysis, even