Mixed Criticality Technology

Subjects: Engineering, Electrical & Electronic

Contributor: José Simó

Embedded systems used in critical systems, such as aeronautics, have undergone continuous evolution in recent years. In this evolution, many of the functionalities offered by these systems have been adapted through the introduction of network services that achieve high levels of interconnectivity. The high availability of access to communications networks has enabled the development of new applications that introduce control functions with higher levels of intelligence and adaptation. In these applications, it is necessary to manage different components of an application according to their levels of criticality. The concept of “Industry 4.0” has recently emerged to describe high levels of automation and flexibility in production. The digitization and extensive use of information technologies has become the key to industrial systems. Due to their growing importance and social impact, industrial systems have become part of the systems that are considered critical. This evolution of industrial systems forces the appearance of new technical requirements for software architectures that enable the consolidation of multiple applications in common hardware platforms—including those of different criticality levels. These enabling technologies, together with use of reference models and standardization facilitate the effective transition to this approach.

Keywords: embedded control systems ; hypervisors ; distributed systems ; mixed-criticality systems ; industry 4.0

1. Introduction

Industry 4.0 expresses a hypothetical fourth stage of the technical-economic evolution of humanity, counting from the First Industrial Revolution. This fourth stage would have started recently, and its development would be projected towards the third decade of the 21st century. Artificial intelligence is pointed out as a central element of this transformation, closely related to the growing accumulation of large amounts of data (“big data”), the use of algorithms to process them, and the massive interconnection of digital systems and devices. From a practical point of view, the evolution towards these new industrial systems is characterized by a large-scale interaction between machines (M2M) and the massive use of data with the aim of achieving flexible production systems, customer-oriented convertible factories, optimization in the use of resources, and circular economy ecosystems.

In this scenario, it is necessary to structure the digitization of means of production so that the management and communication of large amounts of information can coexist with critical automation systems dominated by real-time and security restrictions.

The market for real-time embedded systems has expanded quickly in recent years and is expected to grow for the foreseeable future. This evolution of the technology of embedded systems in terms of computing capacity, connectivity, and performance has been very significant and has enabled the use of more complex control applications that can require more complex design and implementation techniques. Today, all hardware platforms of embedded systems are multicore, and this enables the use of new technologies (e.g., artificial intelligence) [1].

Control activities have traditionally been designed with various tasks that perform the control functions, visualization, and interaction with other devices. All these activities have different levels of criticality due to temporary restrictions or the implication of possible failures and their consequences. The mixed-criticality systems approach seeks to organize in a coherent way the different activities according to their criticality level. Moreover, multi-core computing platforms ideally enable co-hosting applications with different requirements (e.g., high data processing demand and stringent time criticality). Executing non-safety and safety critical applications on a common powerful multi-core processor is of paramount importance in the embedded system market for achieving mixed-criticality systems. This approach enables scheduling a higher number of tasks on a single processor so that the hardware utilization is maximized, while cost, size, weight, and power requirements are reduced. In [2], a survey was presented on mixed criticality in control systems.

In the industrial sector, digital transformation is maintaining and increasing competitiveness. The integration of technologies based on the industrial internet of things (IIOT) and technologies of Industry 4.0 will enable the digital transformation of the latter [3][4]. Intelligent factories, energy systems, and other critical infrastructures are adopting real-time monitoring and analysis capabilities to assess operational efficiency and can incorporate predictive analysis and maintenance to minimize idle time due to system failures. One of the crucial elements in digital transformation is the ability to monitor network control systems in real time. IT solutions attempt to achieve greater efficiency by consolidating common hardware platforms and remote operating capabilities. Recent market trends are forcing industrial manufacturers to look at other software solutions in order to incorporate more non-real-time functionality around crucial real-time tasks in order to accomplish goals, such as cloud connectivity for uploading machine data for server-based predictive maintenance algorithms. Virtualization seems to be a promising path forward, but with the multiple types of virtualization solutions out there, deciding which one to use requires in-depth discussion and thought [5].

Other sectors such as aerospace and defense have used some of these technologies successfully in the design of control systems for avionics components. The integrated modular avionics (IMA) architectures are an evolution of distributed systems to federated systems, and enable integrating multiple applications with different criticality levels in the same hardware platform. The adoption of IMA has resulted in a significant reduction in the cabling, weight, and energy consumption of computer equipment in aircraft, satellites, and drones. The European Space Agency (ESA) has promoted the adaptation of IMA to cover space market needs. The IMA-SP (IMA for Space) project [6] has defined a partitioned architecture with additional services to ARINC-653 standard to deal with new future software developments.

Temporal and space partitioning (TSP) preserve the fault containment properties and “separation of concerns” in development. The functional benefits are related to: The allocation of different criticality/security classes that coexist within the same computer; management of the growth of software functionality; higher degrees of integration as better performing processors becomes available; and easier design for re-use [7].

2. Digitalization and Industry 4.0

The transition to Industry 4.0 will depend on the successful adaptation of a set of technologies that enable interconnecting different levels of control and management in an industrial environment.

Figure 1 shows an overview of the system with the various levels and components.

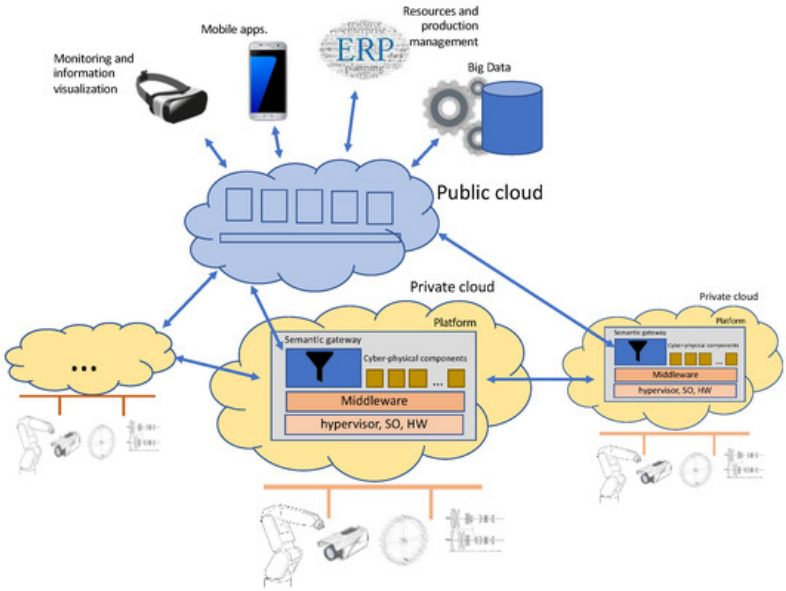

Figure 1. General view of a system for industry digitalization.

The lower level is composed of a set of cyber-physical systems (CPS) each within a private cloud that gathers and combines information from physical systems and provides access to control devices. The CPSs are interconnected through a horizontal communication between private clouds.

The technologies with a strong impact at this level are related to: The control of devices; mechanisms for access and action on devices forming the internet of things; systems based on models to organize and structure information configuring the reference models for industry 4.0; and execution systems that exploit the capacities of the hardware

(multicore systems) and organize applications on a common platform in which real time activities interact with physical devices.

The upper level is structured on the cloud and publishes a set of services that aim to provide certain levels of information to the outside and connect this information with services and processes for the management, planning, and visualization of components and devices at other levels.

2.1. Cyber-Physical System Level

The cyber-physical system is one of the key enablers for the realization of Industry 4.0. It refers to an embedded system with real-time functionalities, control, access to devices, communications, high computing capacity, and user interaction. The CPS level groups the components and services for the real time operation of the physical devices that compose the industrial entity (section). The system, guided by an execution platform based on a multicore system, allows the definition of different execution environments that cover the needs for real time, security, confidentiality, and certifiability of the applications that make up the system in which applications with different levels of criticality can coexist. Figure 2 shows a more detailed vision of the CPS level.

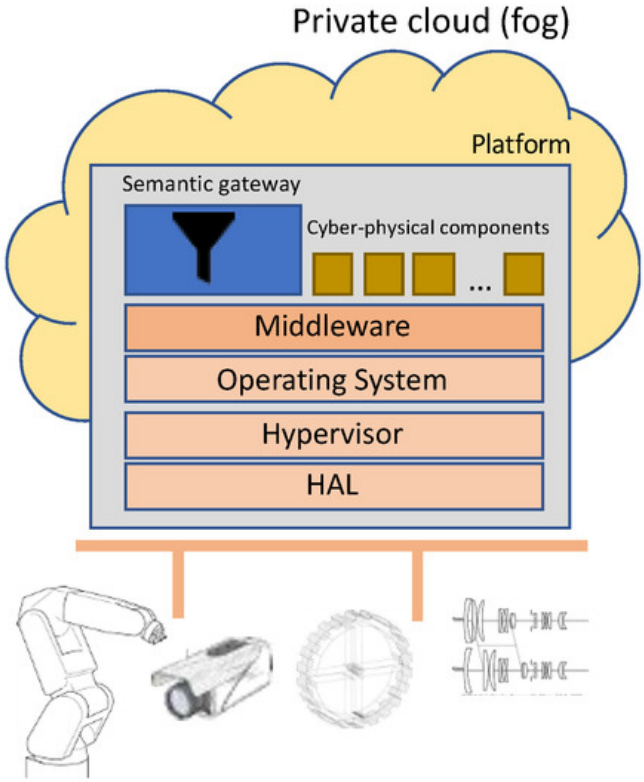

Figure 2. Cyber-physical system level.

At this level, the different CPSs interact with each other through efficient, safe, and predictable horizontal communication. At the same time, these CPSs communicate with the higher level through a vertical communication that enables the development of the strategic and business vision of the company.

The main requirements that are needed at this level can be summarized in the following points.

- Real time capabilities: The embedded system performs control functions by reading sensors and acting on the process with the need to fulfil the time constraints associated with each of the processes or sub-processes that comprise the industrial environment. Real-time activities require real-time operating systems in order to have a predictable behavior and determine system schedulability.

- Support application with different levels of criticality: The evolution from distributed systems to federated systems (in which several applications are executed on the same hardware platform) enables various applications to be executed in isolation with differing time restrictions and levels of certifiability. The ability to handle applications with different levels of criticality on the same platform enables the new multicore hardware platforms to be exploited to the maximum.

- Security and safety: There is an increasing need to securely manage applications. A secure initialization of the platform and verification of integrity is a prerequisite. Secure communications and detection and resistance to cyberattacks are required in operation.

- Application reuse: Applications or components developed in previous projects should be reusable on new embedded computing platforms provided by multi-core processor architectures.
- Communication: At the cyber-physical level, the machines are connected to other machines, material flow management systems, and inspection systems to form a unit that works in a coordinated and highly reconfigurable manner.

The following enabling technologies can be considered basic to the development and operation of this level: Platform virtualization (fault management, temporal, and spatial isolation), industrial internet of things, robotics, cyber-security, fog and edge computing, simulation, and middleware.

As stated in the requirements, many CPS are also mixed-criticality [8]. For example, smart buildings [9] or eHealth IoT systems [10] are works that develop implementations of CPS with mixed criticality systems (MCS) requirements.

2.2. Information Aggregation Level

The machines, robots, and manufacturing resources integrated in Industry 4.0 applications generate an immense volume of communication—both horizontally and vertically.

Vertical integration of automated production is necessary to enable constant process monitoring and integration of additional IoT services. Services such as data analysis, predictive maintenance, or simple access to digital user guides and helpdesks, are customized for the specific machine and integrated directly into the system. Access is granted to all who need it, in a personalized way and, if necessary, through cloud applications. Any external supplier who needs to be integrated into the overall system can obtain specific interfaces for this purpose.

It is important to emphasize that each of the original control tasks of the individual I4.0 components is an essential part of the solution and an important communication task and source of information.

Data and control flows take place in and between the cyber-physical and information integration functional domains. The controls, coordination, and orchestration exercised from each of the functional domains have different granularities and are executed in different time cycles. As it starts in the functional domains, the interactions become coarser, their cycle becomes longer, and the scope of the impact is likely to become larger. Consequently, as information advances in the functional domains, the scope of the information becomes broader and richer, and so new information can be obtained, and new intelligence can emerge in broader contexts. Each functional domain is characterized by the definition of a connectivity model and a computational deployment pattern.

The starting point is the control domain, which is where control tasks are performed, the lowest level information is generated, and time and reliability constraints are more restrictive. The pattern of computational deployment at this level is closely linked to the horizontal connectivity model, and both, working in a coordinated manner, are in charge of the interaction with the physical world composed of machinery and manufacturing resources.

For a satisfactory integration between the cyber-physical level and the information integration level, we propose the development of gateways between levels that make compatible the different quality of service requirements and offer solutions for information management according to the chosen computational deployment pattern—including private cloud and public cloud systems (Figure 1). It is essential to develop information conversion and integration models that, through automatic processing technology, prepare the information according to the context in which it will be used.

Enabling technologies at upper levels include: Big data and analytics, cloud computing, augmented reality, cyber-security monitoring, and deep learning.

3. CPS Platform

Over the last decade, advances in processor technologies have had a strong impact on the architecture of processors with a special emphasis on the processors used in embedded systems. These advances have included the generalization of multicore architectures and support for virtualization at the hardware level.

Virtualization has enabled cloud computing platforms to host applications in the cloud efficiently and on a large scale. Hardware virtualization support in embedded systems has allowed the improvement of hypervisor performance for critical systems offering several isolated execution environments (called partitions with their own operating system and application) on the same hardware platform. Figure 3 shows the architecture of an embedded I4.0 system with hypervisor and partitions.

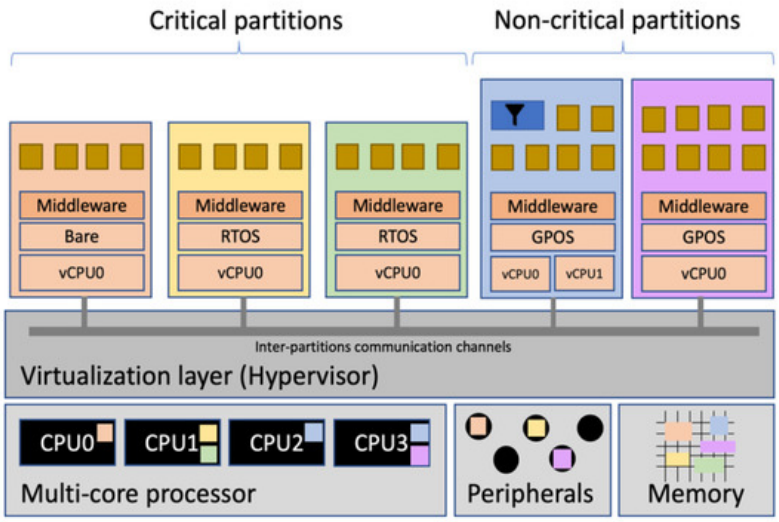

Figure 3. Overview of an embedded I4.0 component in a mixed-criticality context.

Virtualization techniques are the basis for building partitioned software architectures [11]. The virtualization layer is the software layer that virtualizes computing resources. It can be defined and used to manage application or system resources. The hypervisor (also known as a virtual machine monitor (VMM)) implements the virtualization layer of the software and enables several independent operating systems to run their applications on a single hardware platform.

The purpose of the hypervisor is to efficiently virtualize available resources. One of its required features is that it must introduce a low overhead; therefore, the performance of the applications running on the virtualized system must be similar to that of the same applications running on the native system. In the environment of critical systems, the hypervisor is the layer on top of the hardware that has to offer the necessary characteristics for the execution of real-time systems with a high level of integrity and safety.

To run several isolated execution environments, the hypervisor must cover:

- Fault isolation: A fault in one application must not spread to other applications. Any failure must be resolved by the application itself or by the hypervisor.
- Spatial isolation: Applications must run in independent physical memory address spaces. The hypervisor must ensure that the applications cannot access any memory area that has not been specifically assigned to them.
- Temporary isolation: The real-time behavior of an application must be correct independently of the execution of other applications. The allocation of system resources to one application is not influenced by others and can be analyzed independently.

The availability of a platform on which completely independent and isolated partitions such as the one provided by a hypervisor can be executed is the basis for the design and development of mixed criticality systems. Each partition containing an application with its operating system may have a different level of criticality. Criticality level means the level of exigency or safety required by the application that is performing control functions over the processes.

There have been some hypervisors that have been used to implements MCSs since they provide the correct level of isolation to applications of different criticality. The MULTIPARTES and DREAMS architectures [12][13] is one of the approaches for the development of MCS under realistic assumptions.

In [14], RTA-HV is used to provide virtualization support for a multicore hardware platform for the automotive industry. In [15], VOSYS monitor is used as virtualization technology, a multi-core software layer, which allows the co-execution of a safety-critical real-time operating system (RTOS) and a noncritical general purpose operating system (GPOS) on the same hardware ARMv8-A platform. Last release (v2.5.0) is ASIL-C-ISO 26,262 certified [16]. A hypervisor for a mixed criticality on-board satellite software system is discussed by Salazar et al. in [17].

Partitioning is implemented for Components Of The Shelf (COTS) Network On Chip (NoC)-based MultiProcessor System On Chip (MPSoC) for the mixed criticality systems, in the safety critical field in [11]. The proposed technique was developed as a software module to be interred in a certified RTOS for avionics systems.

References

1. ARTEMIS. Embedded Intelligence: Trends and Challenges, a Study by Advancy, Commissioned by ARTEMIS Industry Association. 2019. Available online: https://artemis-ia.eu/publication/download/advancy-report.pdf (accessed on 30 November 2020).
2. Burns, A.; Davis, R. Mixed criticality systems–A review. In Technical Report; Department of Computer Science, University of York: York, UK, 2013.
3. IIC. The Industrial Internet of Things Volume G1: Reference Architecture. 2019. Available online: https://www.iiconsortium.org/IIRA.htm (accessed on 30 November 2020).
4. Kagermann, H.; Helbig, J.; Hellinger, A.; Wahlster, W. Recommendations for implementing the strategic initiative INDUSTRIE 4.0. In Final Report of the Industrie 4.0 Working Group; National Academy of Science and Engineering: München, Germany, 2013.
5. Kou, E. Achieving the Industrial Internet of Things through Virtualization. White paper. Available online: https://www.5gtechnologyworld.com/achieving-the-industrial-internet-of-things-through-virtualization/ (accessed on 30 November 2020).
6. IMA-SP. IMA-SP. IMA-SP Integrated Modular Avionics for Space. In ESA Project; Coordinator: Astrium SAS; Contract ESTEC 4000100764, European Space Agency (ESA): Noordwijk, The Netherlands, 2011.
7. Windsor, J.; Hjortnaes, K. Time and space partitioning in spacecraft avionics. In Space Mission Challenges for Information Technology, Proceeding of the Third IEEE International Conference on Space Mission Challenges for Information Technology, Pasadena, CA, USA, 19–23 July 2009; IEEE: Piscataway Township, NJ, USA, 2009; pp. 13–20.
8. Biondi, A.; Marinoni, M.; Buttazzo, G.; Scordino, C.; Gai, P. Challenges in virtualizing safety-critical cyber-physical systems. In Proceedings of the Embedded World Conference, Nuremberg, Germany, 27 February–1 March 2018; pp. 1–5.
9. Dimopoulos, A.C.; Bravos, G.; Dimitrakopoulos, G.; Nikolaidou, M.; Nikolopoulos, V.; Anagnostopoulos, D. A multi-core context-aware management architecture for mixed- criticality smart building applications. In Proceedings of the System of Systems Engineering Conference (SoSE), Kongsberg, Norway, 12–16 June 2016; pp. 1–6.
10. Kotronis, C.; Nikolaidou, M.; Dimitrakopoulos, G.; Anagnostopoulos, D.; Amira, A.; Ben-saali, F. A model-based approach for managing criticality requirements in e-health iot systems. In Proceedings of the 13th Annual Conference on System of Systems Engineering (SoSE), Paris, France, 19–22 June 2018; pp. 60–67.
11. Avramenko, S.; Violante, M. RTOS solution for noc-based COTS MPSoC usage in mixed- criticality systems. J. Electron. Test. 2019, 35, 29–44.
12. Trujillo, S.; Crespo, A.; Alonso, A. Multi-PARTES: Multicore virtualization for mixed-criticality systems. In Proceedings of the Euromicro Conference on Digital System Design, DSD, Los Alamitos, CA, USA, 4–6 September 2013; pp. 260–265.
13. Obermaisser, R.; Perez, J. Distributed Real-Time Architecture for Mixed-Criticality Systems (English Edition); CRC Press: Boca Raton, FL, USA, 2018.
14. Evripidou, C.; Burns, A. Scheduling for mixed-criticality hypervisor systems in the auto- motive domain. In Proceedings of the WMC 2016 4th International Workshop on Mixed Criticality Systems, Porto, Portugal, 29 November 2016.
15. Lucas, K.P.; Chappuis, M.; Paolino Dagieu, N.; Raho, D. VOSYS monitor, a low latency monitor layer for mixed-criticality systems on ARMv8-A. In Leibniz International Proceedings in Informatics (LIPIcs); Bertogna, M., Ed.; Schloss Dagstuhl Leibniz Zentrum fuer Informatik: Wadern, Germany, 2017; pp. 6:1–6:18.
16. Virtual Open Systems Newsletter. Available online: http://www.virtualopensystems.com/en/company/news/newsletter-2018-09/ (accessed on 30 November 2020).
17. Alonso, A.; de la Puente, J.A.; Zamorano, J.; de Miguel, M.A.; Salazar, E.; Garrido, J. Safety concept for a mixed criticality on-board software system. IFAC-Papers Online 2015, 48, 240–245.
