

Embedded Artificial Intelligence: The ARTEMIS Vision

Dimitrios Serpanos, ISI/ATHENA and University of Patras

Gianluigi Ferrari, University of Parma

George Nikolakopoulos, Lulea University of Technology

Jon Perez, Ikerlan

Markus Tauber, University of Applied Sciences Burgenland

Stefan Van Baelen, IMEC

Advances in embedded and cyberphysical systems have disrupted numerous application domains. We examine the requirements and challenges of these technologies, which present significant opportunities for interdisciplinary research.

Embedded computing has brought significant advances in application domains ranging from home appliances and health systems to environmental monitoring and from smart factories to autonomous

transportation (cars, trains, ships, and airplanes) and smart cities. Embedded computing systems constitute the *cyber* part of cyberphysical systems (CPSs). Autonomous CPSs are commonly used in processes of increasing complexity that are designed and implemented with single-processor systems (for example, a patient's insulin pump) or distributed, interconnected processing nodes (for example, autonomous vehicles). Autonomous CPSs have also become increasingly connected to the Internet of Things (IoT), which includes specialized networks, such as the Industrial IoT, Internet of Vehicles, and others.

Clearly, a hierarchy of CPSs is emerging, where simple autonomous systems are interconnected to create higher-level autonomous systems that, in turn, are interconnected to provide even more complex systems and applications. For example, a CPS for an autonomous car's cruise control is part of an autonomous car—a more complex distributed CPS—that may be a node of a network of

Digital Object Identifier 10.1109/MC.2020.3016104
Date of current version: 21 October 2020

autonomous vehicles (a fleet) managed through a cloud application.

The pervasiveness of embedded systems and the increasing deployment of CPSs lead to an emerging infrastructure that spans globally and

this vision, CPSs need to be efficient, scalable, and extensible in terms of both hardware and software.

The adoption of CPSs in various application domains leads to strong constraints on their design and implemen-

these requirements, the application domains, ranging from manufacturing to transport and from health to power, impose different constraints on each specification. For example, industrial production systems have stricter requirements for real-time constraints and continuous operation than home automation systems, while they have more relaxed stipulations for power consumption relative to autonomous, mobile health-monitoring systems.

Recent developments enable the creation of autonomous systems that are self-aware and adaptive to dynamic environments.

enables the development of new applications and services that were infeasible or inconceivable in the recent past. The immediate availability of operational data as well as computational power in conjunction with artificial intelligence (AI) techniques provides significant opportunities for systems and services worldwide. To achieve

tation. More precisely, CPS technologies are quite demanding for the purpose of satisfying strong application and operational environment requirements, including real-time constraints, safety and security, continuous operation, scalability, extensibility, autonomy, power consumption, and internetworking. Although CPSs typically abide by several of

EMBEDDED INTELLIGENCE

The significant recent technological advances, including the revolution in AI, lead to the increased “intelligence” of computational systems and, especially, of CPSs. This happens during both the design phase and operation in the field. Autonomous and semi-autonomous systems have been a reality for a long time in controlled environments, for example, robots in manufacturing lines, but recent developments enable the creation of autonomous systems that are self-aware and adaptive to dynamic environments, such as efficient and safe self-driving vehicles.

Embedded intelligence requires the development of efficient and effective technologies for embedded systems and CPSs in all application domains. A presentation of the related key technologies appears in the core circle of Figure 1, which presents the vision of the ARTEMIS Industrial Association, the largest European organization focusing on embedded systems, CPSs, and related technologies.¹

The quest for embedded intelligence requires efficient embedded systems and CPSs, with effective processors, coprocessors, memories, network subsystems, special-purpose circuits, operating systems, programming environments, and so forth. Considering that these systems operate in resource-constrained environments, depending on the application domain, efficient tools are necessary for design space exploration that combines hardware and software so as to identify appropriate, effective designs. This is in



FIGURE 1. Embedded intelligence. (Source: <https://artemis-ia.eu/key-technologies.html>; used with permission.) SoS: systems of systems; HPC: high-performance computing.

addition to the technologies required for efficient and cost-effective systems.

The increasing computational capabilities of CPS nodes lead to powerful distributed systems that implement complex processes with high performance and reliability. The traditional model—where edge nodes collect information and transmit the data to centralized systems (or the cloud) for processing and actuation feedback—is rapidly changing to a model of powerful interconnected nodes that execute sophisticated processing locally and send information and event data only as required to central nodes. This augments performance and supports real-time processing, due to increased local node processing and a reduced centralized processing load, and it improves reliability and security, as a result of local storage and less data transmission, while saving bandwidth and reducing network complexity. Edge computing, coupled with AI methods, enables faster processing and decisions near data sources. In particular, it strongly supports the evolution of autonomous CPSs that are self-aware and adaptable to dynamic environments without sacrificing their interconnectivity and orchestration for higher-level complex applications.

The evolution of “smart” edge systems enables highly demanding distributed applications and services in several domains; for example, aerial autonomous vehicles enable services from fleet management to border surveillance. The requirements for increasing functionality and efficiency for hyperconverged infrastructure at the edge and those for smart sensors—for example, smart cameras—lead to a need for high-performance computing (HPC) architectures at the CPS level, where embedded vision systems, virtual reality, data fusion, and AI constraints are representative examples of the need for sophisticated, embedded HPC architectures.

The dramatic penetration of CPSs in increasing domains, from avionics

to agriculture and from manufacturing to health, is disruptive. The rapidly growing number of embedded platforms constitutes a strong enabler of new business opportunities and models that have become feasible. More importantly, such models and opportunities are multiplying, and it is certain that new, unforeseen services will appear in the future. The ability to organize CPSs in domains, develop applications on them, and manage

them effectively requires designs that can efficiently synthesize in large systems, effectively and seamlessly, providing necessary special-purpose computational infrastructures at will. Technologies that integrate systems and enable building systems of systems (SoSs) are fundamental in this direction. Software technologies and appropriate software architectures, such as service-oriented ones, are necessary to address the needs for evolving systems and platforms and for enabling novel services and business models.

Safety is a fundamental property of CPSs, considering their role in multiple processes, including health, manufacturing, and transportation (planes, ships, trains, and vehicles). Safety engineering for CPSs is a cornerstone of the emerging Industry 4.0 and Society 5.0 concepts based on CPSs. Safety requires the mitigation of both accidental failures and cyberattacks on computational and network resources and operations. Security mechanisms are required to protect the data on which safety mechanisms rely. It is imperative to develop methods and mechanisms to build overall safe and secure CPSs, not only individually but in dynamic interconnections when building SoSs, where collective properties need to be attained based on the safety

and security properties of individual systems. Safety is a necessary property not only from the technological point of view but also the social one since it is key to the acceptance and adoption of CPS technologies in society.

Exploiting the preceding technologies, CPSs achieve embedded intelligence employed in all application domains, such as digital industry, transportation, health, and so on. Such application domains are included in

The evolution of “smart” edge systems enables highly demanding distributed applications and services in several domains.

the outer cycle of Figure 1, where the list is not exhaustive but descriptive at a high level of abstraction, indicating priority areas for European industry. Specialized domains include smart agriculture, supply chain management, and border surveillance, to name a few.

RESEARCH CHALLENGES

Embedded intelligence presents several research challenges in its core technologies. In the remainder of this article, we describe several illustrative difficulties. We remark, however, that these are not exhaustive, and, although we organize them according to the core technologies of Figure 1, several of them are cross domain.

The diverse and increasing CPS application domains with strong functional and nonfunctional requirements, such as safety, security, real-time constraints, and low power consumption, drive the new generations of embedded computing systems that exploit multicore devices and advanced virtualization technology. New multicore devices that have novel architectures with effective memory structures (including distributed shared memories), high-performance coprocessors (such as graphics processing units, tensor cores, and programmable cells on field-programmable gate

array components), and on-chip diagnosis and thermal management components provide a continuous challenge that targets the development of low-cost and power-efficient devices that offer the necessary performance and connectivity for increasingly demanding environments.²

The integration of these components, as well as smart sensors, creates significant research obstacles at all fronts, from semiconductor design to dependable system architectures. The challenges extend to the development of integrated development environments (IDEs) and tools that

for digitalization pose major challenges, such as the effective integration of SoSs at the appropriate middleware layer, thus enabling direct interaction among component systems and minimizing complexity while ensuring upgradability, scalability, and extensibility. Appropriate assessment metrics need to be identified to evaluate the performance of integrated systems, especially with respect to single systems. Platform definitions, in terms of functionality and supported (hardware and software) components, are required together with specifications for the cyber-environment where digitalization takes

on that information. Privacy and data integrity form fundamental requirements of these systems to protect information appropriately and secure correct decisions. Safe and secure systems require new security-by-design and safety-by-design approaches that minimize attack and failure surfaces. The difficulties increase when considering CPSs with AI components, where data integrity, as well as algorithmic correctness, is a strong requirement. The inclusion of the cloud with CPS applications and services constitutes a challenge by itself, considering the current open problems of cloud security. The challenge of safe and secure CPSs expands to standardization and certification efforts in view of the legal and social aspects of the emerging CPSs that range from critical infrastructures to autonomous vehicles.

Because CPSs are computing systems with complex software components (in addition to hardware), software engineering and tools for embedded software play an important role in the development of efficient, safe, and reliable systems. Methods for software and system verification, testing for high-level properties (for example, safety and security), runtime verification, software synthesis, and software maintenance and management become increasingly important under the constraints for continuous fail-safe and real-time operation.⁶ Advanced system and software management operations, such as the runtime confirmation of certification compliance due to multiple stakeholders, constitute significant process-dependent challenges.⁷ Virtualization software has become a fundamental requirement for CPSs, leading to a strong need for mechanisms and tools for the efficient virtualization of constrained and heterogeneous microprocessor and multicore platforms.

New languages and tools for safe application development across distributed middleware frameworks and

support the cost-efficient and dependable growth of CPSs, enabling design and design management at the appropriate abstraction levels to manage heterogeneous languages and computing platforms, real-time guarantees, dependability constraints, and so forth. New models of computing, such as approximate, neuromorphic, and AI, provide promising results in several domains, including the cyber-physical interface. The efficient inclusion of AI processing components in embedded devices (for application efficiency and system dependability, among others) poses significant difficulties at both the design and IDE levels. Moreover, the strong progress at all fronts of embedded systems and CPS design creates a significant challenge to standardization and certification efforts, especially for safety-related systems that include AI subsystems.

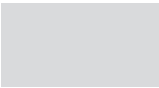
The increasing interconnection and integration of independent, dedicated CPSs to form a higher-level single system while maintaining continuous operation independently of the collaborative system leads to the concept of SoSs.^{3,4} Platforms that integrate SoSs

place; the scalability and interoperability of the platform are key aspects.


In the context of SoS integration, the concepts of the fog, cloud, and IoT, together with the upcoming 5G technology, pose several major difficulties for effective and efficient communication architectures. All these paradigms foster the integration of SoSs in unprecedented ways, supporting a physical and logical network hierarchy of multiple levels of cooperating nodes. Nevertheless, it is necessary to automatically orchestrate different devices and layers, enabling resource sharing and interactions between nodes at the same layer and at different layers in the hierarchy. To meet the specific requirements of integrating SoSs, the combination of heterogeneous communication and application protocols plays a key role. The IoT ecosystem is a perfect illustrative example of the need for communication protocol interoperability.⁵

Safety and security constitute a significant challenge to CPSs. Inherently, intelligent embedded systems and CPSs collect data, which is often sensitive, and make decisions based

Appropriate assessment metrics need to be identified to evaluate the performance of integrated systems, especially with respect to single systems.



virtualized distributed platforms are required. Furthermore, the efficient integration of AI components in systems, especially for non-AI expert developers, is a significant growing challenge that requires fresh approaches to modular design and AI process specification. This is also part of the software lifecycle management, which is especially demanding in CPSs; agile methodologies, continuous integration, DevOps, and reconfigurability in real-time distributed and/or safety-critical systems require novel techniques for the constrained CPS environment. Updating CPS software in the field is a characteristic example that demonstrates the need for methods that guarantee CPS properties, such as safety, security, and real-time operation, in contrast to traditional software updating methods. The new software not only needs to be verified or tested appropriately when developed but inserted in a way that enables real-time updates and nondisruptive continuous operation without violating functional and nonfunctional properties.

The advances in embedded and CPS technologies, coupled with the growth of the IoT, cloud computing, and AI, have led to disruptive growth models in application domains ranging from manufacturing to energy and from transportation to health. The increasing adoption of these systems in everyday operations places significant requirements on these systems, which are application and process dependent, creating significant new opportunities in interdisciplinary research. 

REFERENCES

1. ARTEMIS Industry Association. Accessed: Aug. 10, 2020. [Online]. Available: <https://artemis-ia.eu>
2. J. Perez Cerrolaza et al., "Multi-core devices for safety-critical systems: A survey," *ACM Comput. Surv.*, vol. 53, no. 4, pp. 1–38, July 2020. doi: 10.1145/3398665.
3. M. W. Maier, "Architecting principles for systems-of-systems," *Syst. Eng.*, vol. 1, no. 4, pp. 267–284, 1998. doi: 10.1002/(SICI)1520-6858(1998)1:4<267::AID-SYS3>3.0.CO;2-D.
4. P. Azzoni, "From Internet of Things to System of Systems: Market analysis, achievements, positioning and future vision of the ECS community on IoT and SoS," ARTEMIS-IA, Eindhoven, The Netherlands, White Paper, Apr. 2020. [Online]. Available: <https://artemis-ia.eu/news/artemis-whitepaper-from-the-internet-of-things-to-system-of-systems.html>
5. S. Cirani, G. Ferrari, M. Picone, and L. Veltri, *Internet of Things: Architectures, Protocols and Standards*. Chichester, U.K.: Wiley, 2018.
6. M. T. Khan, D. Serpanos, and H. E. Shrobe, "ARMET: Behavior-based secure and resilient industrial control systems," *Proc. IEEE*, vol. 106, no. 1, pp. 129–143, 2018. doi: 10.1109/JPROC.2017.2725642.
7. A. Bicaku, M. Tauber, and J. Delsing, "Security standard compliance and continuous verification for Industrial Internet of Things," *Int. J. Distrib. Sensor Netw.*, vol. 16, no. 6, 2020. doi: 10.1177/1550147720922731.

DIMITRIOS SERPANOS is director of the Industrial Systems Institute/ATHENA and a professor of electrical and computer engineering at the University of Patras. He is the chair of the ARTEMIS Scientific Council; a Senior Member of IEEE; and a member of the ARTEMIS Scientific Council, ACM, AAAS, and NYAS. Contact him at serpanos@computer.org.

GIANLUIGI FERRARI is an associate professor at the University of Parma, Italy, and a member of the ARTEMIS Scientific Council. Contact him at gianluigi.ferrari@unipr.it.

GEORGE NIKOLAKOPOULOS is a professor at Lulea University of Technology, Sweden, and a member

of the ARTEMIS Scientific Council. Contact him at george.nikolakopoulos@ltu.se.

JON PEREZ is principal researcher at Ikerlan, Spain, and a member of the ARTEMIS Scientific Council. Contact him at jmperez@ikerlan.es.

MARKUS TAUBER is a professor at the University of Applied Sciences Burgenland, Austria, and a member of the ARTEMIS Scientific Council. Contact him at markus.tauber@fh-burgenland.at.

STEFAN VAN BAELEN is project manager at IMEC, Belgium, and a member of the ARTEMIS Scientific Council. Contact him at stefan.vanbaelen@imec.be.