A Systematic Study on Cyber Physical System

M. Revathi, K. Prakash, R. Suguna

Abstract— Cyber-physical systems (CPSs) are physical and engineered systems whose operations are monitored, coordinated, controlled and integrated by a computing and communication core. The economic and societal potential of such systems is vastly greater than what has been realized, and major investments are being made worldwide to develop the technology. There are considerable challenges, particularly because the physical components of such systems introduce safety and reliability requirements qualitatively different from those in general purpose computing. Moreover, physical components are qualitatively different from object-oriented software components. The vision for smart manufacturing is for all aspects of manufacturing to be highly integrated, from plant operation to supply chain. The entire life cycle of a product would be enabled to be tracked, including aspects such as processes and resources, leading to manufacturing environments that are flexible and can optimize performance and efficiency. Advances in CPS can help to reduce the Time-to-market for products and systems, while promoting innovation, competition, and resilience in supply chains. These advances can allow a more flexible optimization of cost and markets since Production could be located near materials, technology skill centers, or consumers. The Future workforce of manufacturing will have core knowledge and skills that can be applied to innovation and research.

Keywords--- Computing, Optimize, Time-to-Market, Resilience.

I. INTRODUCTION

WHAT is a CPS? remains open, widely recognized and accepted attributes of a CPS include timeliness, distributed, reliability, fault-tolerance, security, scalability and autonomous. Many aspects of our lives, including finances, transportation, and emergency services, depend on the reliable production, transfer, and distribution of energy, including electricity, oil, and natural gas. Today’s electric grid is a complex system of systems, with many different stakeholders and customers. The National Academy of Engineers has named the development of electrification, which includes today’s electric system, as the greatest engineering achievement of the twentieth century. The water supply and distribution system is also listed as a great engineering achievement; the supply of safe, clean, and reliable water is important to health, quality of life, and emergency services. Yet even though these systems are great achievements, they need to be modernized in order to increase their efficiency and reliability. Existing infrastructure is aging and control systems can be highly improved. Cyber-physical systems (CPS) stand to have a significant impact on large-scale, computer-mediated physical distributed systems such as the electric grid and water distribution systems. The cyber and physical components integrated in the system have many interactions the can affect the entire operation, but are poorly understood. The electric grid and other utilities can use CPS technologies to help the system become smarter and more efficient.

Figure 1: CPS Security Architecture

The infrastructure for both the electric grid and water distribution systems is aging and face technical and reliability problems. The Environmental Protection Agency reports that there are 240,000 water main breaks per year in the United States, and as a system ages the number of main breaks increases. New technologies, including those in CPS regarding sensors and control, may help to increase the effectiveness of water utility distribution systems.

CPS science and technology can provide many possibilities for innovation in the manufacturing industry through smart products and production and lifecycle design for product safety, security, and sustainability. The scope of areas that benefit from cyber-physical engineering concepts, infrastructure, and tools is broad and includes homes, military logistics and weapons systems, healthcare, clothing, agriculture, food processing and preparation, and automotive and air vehicles. There is a trend towards the demand for products that have safe, dependable, and secure plug and play integration of cyber and physical components thus leading towards the possibility of being highly customizable. Mass customization in manufacturing currently only involves minimal flexibility to alter fixed parameters.
The economic impact of any of these applications would be huge. Computing and networking technologies today, however, may unnecessarily impede progress towards these applications. For example, the lack of temporal semantics and adequate concurrency models in computing and today’s best effort networking technologies make predictable and reliable real-time performance difficult. Software component technologies, including object-oriented design and service-oriented architectures, are built on abstractions that match software better than physical systems. Many applications will not be achievable without substantial changes in the core abstractions.

CPS Definition and Architecture Cyber-Physical Systems are a next-generation network connected collection of loosely coupled distributed cyber systems and physical systems monitored/controlled by user defined semantic laws. Here, cyber systems are collections of control logic and sensor units, while physical systems are collections of actuator units. Prototype architecture of a CPS is shown in Figure. The highlights of this architecture include:

- **Global Reference Time**, which is provided by the next generation network. This should be accepted by all system components, including humans, physical devices, and cyber logic in this architecture.
- **Event/Information Driven**. Just as human society is Event/Information Driven, future CPSs should also use a similar communication mechanism. Moreover, we differentiate between Events and Information. Events are either-raw facts reported by sensor units/humans (called Sensor Events) or-actions made by actuator units/humans (called Actuator Events). Information is the abstraction of the physical world made either by CPS control units or humans through event processing.

- **Quantified Confidence**. This design goal is archived by a Unified Event/Information model. Any event/information in this architecture should contain the following built-in properties. Global reference time—records the event/information occurrence/detected time. Life-span—specifies how long until that event/information’s confidence level drops to zero. Confidence and confidence fading equation—specifies the event/information confidence level and how it fades over time. The confidence level and equation are decided by a particular device and control logic to provide a standard method for the subscriber to calculate the confidence of the subscribed event/information at any point in time. Digital signature and authentication code—specifies who published and who can access the event/information. Trustworthiness—specifies how much the subscriber trusts a particular publisher. Dependability—specifies the subscriber’s dependence on event/information provided by a publisher in order to produce a particular outcome/information. Criticalness—specifies the critical urgency of each event/information so the subscriber can allocate its system resources based on different system design goals.

- **Publish/Subscribe Scheme**. Using this scheme, each CPS Control Unit acts like a human being in that it only subscribes to interesting events/information based on its system goal, and publishes event/information when necessary.

- **Semantic Control Laws**. Usually defined in an Event Condition-Action like form, they form the core of each CPS control unit. With the abstraction of the real-time physical world shown in Figure, we can precisely control system behaviors related to the environment context according to user defined conditions/scenarios. In addition to providing a global reference time, the next-generation network should also provide new event/information routing and data management schemes. Each network node should use a-publish like scheme for passing event/information to its neighbor nodes based on current confidence. Once the confidence of the event/information drops to zero (or below a certain threshold), the value of letting this event/information continue to-live in the network is zero. The Secured Network Knowledge Database Servers only accept the data when it expires, and serves as a knowledge backup.

II. CPS ARCHITECTURE

CPS architecture had a two-layer structure inherently, the physical part and the cyber part. The physical part senses physical environment, collects data, performs commands from the cyber part. The cyber part analyzes and processes the data from the physical part and rise commands.

- Execution layer-Besides a target environment, execution layer consists of various physical devices, such as sensor, actuator, RFID (radio frequency identification) tags, RFID readers, mobile intelligent
terminal and etc., which is in charge of collecting data from physical environment and performing commands.

- **Transport layer**-The next.

![System Architecture Diagram](image)

**Figure 3: System Architecture**

- **Control layer**-Control layer is the key part of the interaction between the cyber part and the physical part Control layer process the data which is collected from sensors and generate commands which will feedback to actuator in execute layer through transport layer. As a part of control layer, application support layer makes use of middleware.

- **Infotainment platform**, cloud computing platform, service support platform and etc. Combining control layer with various industries environmental monitoring smart grid, smart auto, and industry, control come into being generation network supports transport layer, the main technical methods of which contain LAN, Internet, communication network and private network. Transport layer not only realizes real-time transmission, but also has the ability to process and manage amounts of data leakage or damage and security issues during massive data integration. Control layer attacks include the loss of user privacy, incorrect access control policies and inadequate security standards.

**Challenging issues**: The U.S. National Academy of Engineering has compiled a list of grand challenges that are particularly related to CPS. Among the many challenging issues related to society, economy, and environment, CPS research is particularly relevant safety, stability, performance, reliability, robustness, and efficiency, in areas such as transportation, energy, medical and healthcare, defense, manufacturing, and agriculture. Some representative grand challenges for CPS research are as follows:

1. Near-zero automotive traffic fatalities, minimal injuries, and significantly reduced traffic congestion and delays.
2. Sustainable and blackout-free electricity generation and distribution.
3. Clean and energy-aware buildings and cities.
4. Smart, reliable, and flexible medical and healthcare systems.
5. Abstraction and Architecture.
6. Computing and Networking Foundations.
7. Hybrid Systems and Control.
8. Verification, Validation, and Certification.
9. Robustness, Safety, and Security.
10. Stability, Performance, and Safety.
11. Sensing, Computing, and Networking Systems.
12. Modeling, Design, and Development.

**Need for CPS Research**

CPS research is still in its infancy. Professional and institutional barrier have resulted in narrowly defined, discipline-specific research and education venues in academia for the science and engineering disciplines. Research is partitioned into isolated sub disciplines such as sensors, communications and networking, control theory, mathematics, software engineering, and computer science. For example, systems are designed and analyzed using a variety of modeling formalisms and tools. Each representation highlights certain features and disregards others to make analysis tractable. Typically, a particular formalism represents either the cyber or the physical process well, but not both. Whereas differential equations are used for modeling physical processes, frameworks such as Petri nets and automata are used to represent discrete behavior and control flows. Workforce expertise is similarly partitioned, to the detriment of productivity, safety, and efficiency. Although this approach to modeling and formalisms may suffice to support a component-based-divide and conquer approach to CPS development, it poses a serious problem for verifying the overall correctness and safety of designs at the system level and component-to-component physical and behavioral interactions. The broader aeronautics community has identified verification and validation methodologies and concepts as a critical research area. The goals of research in verification and validation of aviation flight-critical systems include providing methods for rigorous and systematic high-level validation of system safety properties and requirements, from initial design through

![Attack and Defense Diagram](image)

**Figure 4: Attack and Defense System**

Based on the CPS architecture attacks are classified into execution layer, transport layer and control layer. The execution layer attacks include security attacks for nodes such as sensors and actuators. Transport layer attacks include data
implementation, maintenance, and modification, as well as understanding tradeoffs between complexity and verification methods for supporting robustness and fault tolerance. Some of the control engineering challenges include:

- Large-scale, real-time, deterministic robust or stochastic optimization.
- Algorithms
- Multiple-objective, multiple-stakeholder optimization frameworks.
- Design of automation with graceful degradation modes.
- Safety diagnosis/health monitoring methods.
- System architectures that facilitate distributed decision making.
- Data fusion from heterogeneous sensors and assessment of the value of the Derived information.

III. CHALLENGES OF CPS

- **Scientific Challenges:** Multi-Paradigm–Multidisciplinary; Socio-Technical Character–Foundational Theories; Multi-domain modeling.
- **Technological Challenges:** Complexity–Interoperability; Autonomy – Privacy; Dependability; Uncertainty
- **Economic Challenges:** Disruption – Service vs. Product; Disruptive dominance.
- **Education Challenges:** Competence–Knowledge Excellence; – Balanced Education; Future Work force.
- **Legal Challenges:** Innovation Barriers – Relatory environment – Certification, Harmonization.
- **Societal Challenges:** Change-Aversion – Public awareness; Public Support.

IV. CONCLUSION

Cyber-physical systems are expected to play a major role in the design and development of future engineering systems with new capabilities that far exceed today’s levels of autonomy, functionality, usability, reliability, and cyber security. Advances in CPS research can be accelerated by close collaborations between academic disciplines in computation, communication, control, and other engineering and computer science disciplines, coupled with grand challenge applications.

REFERENCES

[1] T. Henzinger, E.A. Lee, A. Sangiovanni-Vincentelli, S. Sastry, A. Aiken, D. Auslander and M. Tomizuka, “Center for Hybrid and Embedded Software Systems”, 2008.

[2] R.R. Rajkumar, I. Lee, L. Sha and J. Stankovic, “Cyber-physical systems: the next computing revolution”, In conference on Proceedings of the 47th design automation, Pp. 731-736, 2010.

[3] R. Baheti and H. Gill, “Cyber-physical systems”, The impact of control technology, Pp. 161-166, 2011.

[4] J. Fitzgerald, C. Gamble, P.G. Larsen, K. Pierce and J. Woodcock, “Cyber-physical systems design: formal foundations, methods and integrated tool chains”, Proceedings of the Third FME Workshop on Formal Methods in Software Engineering, Pp. 40-46, 2015.

[5] Martin Törngren, Cyber-Physical Systems: Characteristics, Trends, Opportunities and Challenges, 2015.

[6] R. Kumar, Challenges of Cyberphysical systems, 2012.

[7] L. De Alfaro and T.A. Henzinger, “Interface theories for component-based design”, International Workshop on Embedded Software, Pp. 148-165, 2001.

[8] S.A. Edwards and E.A. Lee, “The case for the precision timed (PRET) machine”, Proceedings of the 44th Conference annual Design Automation, Pp. 264-265, 2007.

[9] S. Johannessen, “Time synchronization in a local area network”, IEEE control systems, Vol. 24, No. 2, Pp. 61-69, 2004.

[10] E.A. Lee, “Model-driven development-from object-oriented design to actor-oriented design”, Workshop on Software Engineering for Embedded Systems: From Requirements to Implementation, 2003.

[11] J.A. Stankovic, “Misconceptions about real-time computing: A serious problem for next-generation systems”, Computer, Vol. 21, No. 10, Pp. 10-19, 1988.