VIRTUAL ROUNDTABLE

Should Cyberphysical Systems and the Internet of Things Get Married?

Joanna F. DeFranco, Penn State Great Valley School of Graduate Professional Studies

This roundtable discussion explores differences between cyberphysical systems and the Internet of Things, including technical challenges and progress toward addressing them. The panel concludes with highlights of cutting-edge and future research areas.

This is a virtual roundtable discussion between seven experts in the cyberphysical system (CPS) and Internet of Things (IoT) communities. It is a valuable conversation to improve community understanding and consensus in an effort to assist in the advancement of both technologies. The panelists were asked a series of emailed questions, thus some of the responses are interactive and will be presented in the order of the email threads. Their answers are thorough, inclusive, and thoughtful. In alphabetical order, the panelists include John Baras, University of Maryland; Oleg Loginov, IoTecha; Stephen Mellor, Industrial IoT Consortium; Janos Sztipanovits, Vanderbilt University; Haydn Thompson, THHINK Group; Martin Törngren, KTH Royal Institute of Technology; and Claire Vishik, Intel.

COMPUTER: Is the IoT a subset, equivalent, or partial overlap of CPSs? Is this conversation worth pursuing? What is your school of thought and why?

HAYDN THOMPSON: This question has been an open debate for many years, and if you are European, the general consensus is that the IoT is a subset of CPSs, and if you are American, the consensus tends to be that CPSs are a subset of the IoT. My view is that a fundamental characteristic of CPSs is the "physical" connection to the world. This is not always the case with the IoT. So, CPSs have an element of interaction with the physical world, usually via sensing, and then an aspect of control via actuation. The IoT, on the other hand, can just be working

Digital Object Identifier 10.1109/MC.2021.3133965
Date of current version: 11 March 2022

ROUNDTABLE PANELISTS

John Baras is a Distinguished University Professor and endowed Lockheed Martin Chair in Systems Engineering, University of Maryland, College Park, Maryland, USA. Contact him at baras@umd.edu.

Oleg Loginov is the president and chief executive officer of IoTecha, Cranbury, New Jersey, USA. IoTecha is a revolutionary technology for electric vehicle smart charging infrastructure and power grid integration. Contact him at Oleg@iotecha.com.

Stephen Mellor is the chief technology officer of the Industry IoT Consortium (IIC), La Jolla, California, USA. The IIC delivers transformative business value to industry, organizations, and society by accelerating the adoption of a trustworthy Internet of Things. Contact him at mellor@iiconsortium.org.

Janos Sztipanovits is the E. Bronson Ingram Distinguished Professor of Engineering, a professor of computer science, a professor of electrical and computer engineering, and the director of the Institute for Software Integrated Systems, Vanderbilt University, Nashville, Tennessee, USA. Contact him at janos.sztipanovits@vanderbilt.edu.

Haydn Thompson is the managing director/owner of THHINK Group, Sheffield, U.K. THHINK specializes in the development of custom platforms for diagnostics, condition/health monitoring, telemetry, and control, with specialist expertise in advanced data analytics, robust ultralow-power embedded wireless sensors, and energy harvesting. Contact him at haydn.thompson@thhink.com.

Martin Törngren is a professor at KTH Royal Institute of Technology, Stockholm, Sweden. Contact him at martint@kth.se.

Claire Vishik is a fellow at Intel, Santa Clara, California, USA. Intel creates emerging technologies, such as data servers, business transformation, memory, and storage, in fields including artificial intelligence, analytics, and cloud to edge. Contact her at claire.vishik@intel.com.

with data, with no control feedback (although the data may well be used for decision making). A good example of this is in diagnostics, for instance, medical/machinery, where data are collected to schedule maintenance and predict impending failures. Over the past few years, however, the world of the IoT has changed toward the IIoT, and there has been a blurring of the domains here, with many CPS and IoT applications now being called *IIoT*. This is a consequence of the cloud and operational technology worlds coming together in the cloud–edge IoT continuum.

MARTIN TÖRNGREN: My take is that CPSs, by definition, emphasize systems and, in particular, system-level properties. The IoT has traditionally been more of a bottom concept of creating opportunities as things are connected. In any case, physicality (energy, timing, reliability, safety, and so on) as well as cyber aspects will be essential for most of the future systems we are building, with similar trends and drivers. Regardless of the name, we are building systems and linking systems that will contain cyber parts (in terms of computers and feedback systems), physical parts, and humans, where the end properties will depend on the properties of the parts/constituent units, their interactions, and interactions with (other entities in) the environment, causing emergence. The distinctions that are more relevant, then, are on what types of systems we design (for example, the level of automation), if they represent systems of systems (no single system integrator), and their specific requirements.

OLEG LOGINOV: We tried answering this question in IEEE 2413-2019[1]:

> *Interconnected and integrated IoT systems can provide new functionalities to improve the quality of life and to enable technological advances in areas such as personalized healthcare, emergency response, traffic-flow management, manufacturing, defense and homeland security, and energy supply and use. The impacts of IoT will be revolutionary and pervasive; this is already evident in emerging technologies such as autonomous vehicles, Smart Transportation, Smart Logistics, intelligent buildings,*

> *Smart Mining, Smart Energy Systems, Smart Manufacturing, multipurpose robots, Smart Agriculture, Smart Forestry, and Smart Medical Devices* (p. 14).

Also from IEEE 2413 (paraphrased): an IoT system is composed of components (or systems) that interact with one another to achieve a set of goals. Cyberphysical devices are technical artifacts/components that compute and interact with the physical via sensing and actuation.[2] Actuation, sensing, and control are fundamental to IoT systems. Examples of other types of cyberphysical mechanisms include dedicated storage devices and networking equipment, such as routers, switches, and transceivers. They can be understood as "information transducers," in that they mediate the translation of physical properties into information by using a function (the intended purpose or characteristic action) and vice versa. Cyberphysical devices are part of a trend of "dematerializing" interactions. These information transducers include sensors for observing the physical world and actuators for changing the physical world.

JANOS SZTIPANOVITS: One of the variants of interpretations of CPSs is the following, from the National Institute of Standards and Technology (NIST) Framework for Cyber-Physical Systems[2]:

> *CPS are often engineered systems. … CPS functionalities are the result of the tight integration of the cyber and physical sides* (p. 50).

The emphasis of this interpretation is that CPSs have functionalities that cannot be implemented only by physical and cyber means. This interpretation clearly has a profound impact on the design processes and required new system science foundations that must be both physical and computational. All in all, CPSs are a category of engineered systems, where certain essential functionalities emerge by the interaction of physical and computational processes. The IoT concept usually emphasizes engineering fine-grained networked systems. They may or may not be CPSs, and CPSs may or may not use IoT platforms. Regarding the common technology elements, I would look to the IoT as a possible platform for creating CPSs. In this sense, I would not equate the two; they are rather complementary.

CLAIRE VISHIK: Indeed, there are a number of views on the relationship between the two concepts, and, as indicated by Haydn, differing approaches to CPSs and the IoT in various geographic regions, for example, the United States and Europe. What is also remarkable is that, in many cases, definitions of the IoT are not provided in documents focusing on the IoT, to avoid controversy. In the United States, CPSs are more frequently considered a subset of the IoT, although, when these definitions are probed, little distinction between CPS and IoT definitions can be detected. To provide an example, the NIST Framework for Cyber-Physical Systems[2] defines CPSs as systems that "integrate computation, communication, sensing, and actuation with physical systems to fulfill time-sensitive functions with varying degrees of interaction with the environment, including human interaction" (p. 18).

On IoT, Voas[4] asked, "What is the IoT?" There are many ways to describe the IoT. More than 20 professional and research groups have worked to characterize the IoT, but so far, there is "no simple, actionable, and universally-accepted definition for IoT." Instead, the NIST "Networks of Things"[4] model focuses on cross-cutting components in the IoT as a way to at least describe what the term may mean: the Network of Things (NoT) model is based on five fundamentals at the heart of the IoT: sensing, computing, communication, e-utility, and actuation.

In other words, the core of the definition for CPSs and the description of the IoT (or NoTs) in the preceding are the same (communication, computation, sensing, e-utility, and actuation with physical systems), but CPSs, per the previous definition, describe those IoT systems that perform time-sensitive functions interacting, to diverse degrees, with the environment, including human interaction. But this behavior is also true of the IoT (or NoT). Thus, it is clear that there is no significant distinction between the two. In practice, electronic systems that have a distinct physical subsystem or electronic processes that have a clear physical element are frequently described as cyberphysical. Examples can be drawn from numerous areas such as autonomous vehicles and smart cities as well as electronically managed supply chains that transport physical goods.

MARTIN TÖRNGREN: Thanks, Claire, for bringing up the NIST IoT characterization and discussion. I would like to add to this. If we contrast this IoT characterization with the NIST CPS definition (raised earlier by Janos), I think we are onto a key difference in scope and emphasis: the IoT (or NoT) involves sensing, computing, communication, e-utility, and actuation. CPSs, or "smart" systems, are coengineered, interacting networks of physical and computational components."[6]

Sensors and actuators represent interfaces to the physical world; see, for example, the classical view of a mechatronic system (Figure 1) in Wikander et al.[5] Thus, given the example that Voas had for the IoT/NoT, an IoT designer would go as far as designing the computer communication system toward sensors and actuators, but not the room (or the car, and so on). However, CPS design, by way of its construction, encompasses the "coengineering" of cyber and physical parts and thus also, for instance, the mechanical engineering aspects of a car. To me, this makes for a clear difference in scope and emphasis. The computer science or automatic control point of view is that the "plant" is given. If we take both the cyber and physical components into account, then we are designing a CPSs. This view appears to resonate with several previous comments, including the ones by Janos and Haydn.

JOHN BARAS: I think of the IoT and CPSs as quite different concepts (even if we consider, as is common today, networked CPSs). In CPSs, the physical part of the system involves multiple heterogeneous physics and plays a key role in system design and operation, which must coordinate the close interactions between the cyber and physical components. Not so for the IoT, which is very loosely defined, as far as I can tell, and primarily focused on the cyber and IT networking parts of systems. One example that emphasizes this important difference is modern and next-generation communication networks that integrate software-defined networks (SDNs), network function virtualization (NFV), and 5G, where everything essentially is software and the hardware components are standardized and de-emphasized. Of course, the two classes of systems overlap, but they are addressing different design and operational challenges. They overlap—one class is not a subset of the other class.

Another important difference is that while in both classes composability and compositionality are key concepts, with appropriate emphasis on component-based architectures and synthesis, it is in CPSs where the interface between the cyber and physical components must be treated as a system and not just as a simple port. For example, in several security challenges, these interfaces must be able to understand the semantics of both sides (the cyber and the physical) and specifically check whether the cyber-commands can be safely executed by the physical part; otherwise, we have catastrophic attacks like some very well-known ones (for example, STUXNET and broken wind turbines). Finally, if we take the view that any iterative algorithm is a dynamical system, most CPSs are hybrid (logic and physical) ones with digital and analog implementations. This is not the case for IoT devices.

STEPHEN MELLOR: There is no useful differentiation. They are equivalent. This is similar to "fog" and "edge." Yes, we can quibble for months about the exact differences (if any), but in the end, the market will decide. Google returns 11.1 million links for *CPS* and 12.13 million for *IoT*. That is not quite as big a difference as I was expecting, but … Also, in response to John's email, there are a lot of similarities to the Industrial IoT (IIoT). In addition, CPSs and the IoT overlap to the point that it's six of one, half a dozen of the other.

***COMPUTER*:** You all contributed amazing responses, especially by referencing one another's statements and relevant documents. In reviewing/interpreting the statements to determine the themes among them, it appears there is consensus in highlighting/distinguishing the focus of each category/class (IoT/CPS) rather than the distinction label (overlap/complementary/subset). As Janos stated, "Interpretation clearly has a profound impact on the design processes and required new system science foundations." This speaks to the importance of this discussion.

Part of the discussion topic for this panel is related to a statement from John. He said that the two classes address "different design and operational challenges." The next two questions are posed with that in mind. Tell me if you agree with the following statement (if not, feel free to edit): the differentiation between the IoT and CPSs can be described by focus/emphasis, where the IoT concerns networked components focusing on sensing/control with one another and CPSs concern the sensing/actuation of a distinct physical world system (or subsystem/electronic process) connection.

VISHIK: In the previous discussion, we talked about the definitions of the IoT and CPSs. The conclusion, at least as far as I could see, was that there are very diverse definitions of the two areas and that each of us uses our own definitions that match specific research areas. This is somewhat similar to the definition of cybersecurity. A broad definition includes everything that may potentially acquire affiliation with cybersecurity. For example, the following is a commonly used extended definition from the National Initiative for Cybersecurity Careers and Studies[7]:

> *Strategy, policy, and standards regarding the security of and operations in cyberspace, and encompass[ing] the full range of threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure.*

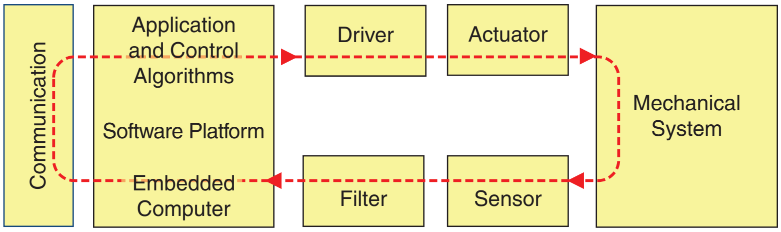

FIGURE 1. The interactions within an integrated mechatronic system (adapted from Wikander et al.[5]).

This breadth was not helpful for the development of cybersecurity as a normal rigorous discipline. Similar breadth has been utilized to define the IoT for a variety of pragmatic reasons. For example, the Global System for Mobile Communications Association stated the following about the IoT in its guidelines on IoT security[8]:

> *Almost all IoT services are built using endpoint device and service platform components that contain similar technologies to many other communications, computing and IT solutions* (p. 5).

If we follow this line of reasoning, as many frameworks and definitions do, the IoT includes everything in information and communications technology, not just endpoint devices. Approaches like this make it easier to use frameworks in traditional IT to examine issues in the IoT. But they make it much harder to focus on cross-cutting issues that characterize what specific research papers consider the IoT.

To react to the previous statement, if we use traditional definitions of the IoT and CPSs that are exceedingly broad, the statement will be incorrect. If we use common sense (and narrower definitions of the IoT and CPS areas), it will be mostly correct but still contain a large number of exceptions for CPSs, especially in areas such as medical devices, where actuation is always mediated. For example, is a contact lens that measures blood sugar levels a CPS or an IoT device? It could actuate an insulin dispenser but only indirectly since it is a separate system. There are many similar examples in other areas. Using the word *focus* provides room for exceptions, but it seems that there are more exceptions than there are rules since only a few fields (for example, automotive, smart grids, and so on) lend themselves easily to this approach.

THOMPSON: In general, there are consequences in terms of physical harm or death if a CPS fails, for example, automotive, aerospace, and so on. If the IoT fails, there may be financial losses and inconvenience but not physical harm (here, the medical IoT may be an exception, but normally there is a human decision maker involved in the loop, as highlighted by Claire). Of course, not all CPSs are safety critical, for example, irrigation control systems in smart farming, but we often see a link via the Internet to a supervisory controller, and this may not require a hard real-time response.

MELLOR: It's a distinction without a difference.

TÖRNGREN: Yes, I agree with this statement. People will often have different understandings of these terms and explicitly or implicitly assume a particular viewpoint, or set of viewpoints, meaning that they have a particular thing in mind (that is, a focus/emphasis).

SZTIPANOVITS: Frankly, I do not completely understand this differentiation. Perhaps for the sake of finding some distinction, I consider the IoT a platform with the usual platform concerns and view the CPS as a design approach with strong emphasis on the codesign of cyber and physical aspects of systems. Clearly, IoT platforms are frequently used for developing systems where CPSs design approaches are needed (for instance, certain categories of networked control systems). However, IoT platforms are also used for creating systems that would be hard to consider CPSs, due to the lack of cross-cutting constraints. Similarly, there are plenty of systems where CPS design approaches are beneficial, but they do not include any IoT elements (not even networking), and, of course, there many IoT-based systems that close control loops over networks and need CPS codesign methods. Since industrial-strength IoT platforms are increasingly available, they accelerate the need for, and increase the complexity of, CPS-like applications. Therefore, it makes sense to maintain links among the respected communities.

BARAS: The statement is ambiguous. As several others have pointed out, we cannot continue calling everything CPSs and everything the IoT. We have been through this discussion several times within both communities. This trend, a few years ago, when Helen Gill was still at the National Science Foundation, came close to "killing" the funding for this program. We sharpened the definition, then, as Janos described. But unfortunately, the trend and bad habits keep creeping in.

So here is my precise answer. I will use networked CPSs and networked human CPSs (H-CPSs) as the reference frame because in this subdomain the IoT and CPSs overlap. The IoT is a platform (actually, a cyber-only platform) that addresses primarily communication (that is, data and information exchanges) between physical and cyber (hardware) devices and system components. CPSs are a framework that focuses primarily on the codesign of the cyber and physical parts of such systems, where there is close interaction between the cyber and physical components. If we consider H-CPSs, this also involves codesign (or better, a co-recommendation) about human behavior and human social aspects.

Now, when we go to networked CPSs and H-CPSs, things get more difficult, as we have to reconsider the network effects [and this needs to be specified precisely, as there are several networks involved (collaboration, information, and communication networks, with some being physical, some cyberlogical, and some mixed)] on the cyberphysical codesign. This has not been properly addressed in CPS research and development efforts. And in this subdomain, some IoT issues and concerns become relevant for CPSs. I cannot find many examples where the opposite is happening, that is, CPS issues becoming relevant for IoT systems. The one area where I have some examples involves constraints on the energy consumption of networked mobile devices communicating wirelessly.

COMPUTER: What do you feel are the major technical challenges (design and operational) of the IoT and CPSs?

VISHIK: There are many challenges at the technical levels. Areas such as security, privacy, integration, safety, and so on are well known. Similarly, there is a significant body of knowledge that is growing at the intersection of physical and cyber areas. I will leave these aside for now. What I think is a significant gap is the ability to develop IoT and CPS devices in ways where requirements are integrated and the integrated risk metrics to evaluate potential outcomes are available. At a very simplified level, how do we define requirements for safety, security, and privacy when they may be orthogonal to one another? How do we recognize misalignment? How do we understand that new tools are needed? For example, are traditional safety metrics sufficient for autonomous vehicles? Or should we switch to model-based approaches?

With regard to the integrated risk picture, how can we define and compute risks for situations where, for example, safety and security need to be integrated? In a simplistic way, even looking at the percentages for allowed failure (which are much more rigorous in safety than in security) reveals a problem that remains unresolved. Without answering these questions, it will not be possible to address more complex environments based on systems of systems (for instance, smart cities). So, what are the major technical challenges in the IoT and CPSs? They are numerous. But they are connected by one foundational consideration: if we don't have stricter definitions of the two areas, we will be able to address these challenges only in a highly fragmented fashion. Similarly, for cybersecurity that became a study of everything under its broad definition, more rigor is required to understand better how to build resilient IoT and CPS platforms and environments.

At a very simplified level, how do we define requirements for safety, security, and privacy when they may be orthogonal to one another?

THOMPSON: Hard real time and safety are the main technical challenges in CPSs. An issue is that the control engineering, software engineering, and networking worlds are quite different. The two types of systems are developed in different ways. CPS engineers use rigorous processes to meet certification for safety. IoT engineers tend to have a less structured method of development, which is more about getting a system to market as quickly as possible (consider sprints and scrums). A key challenge is that the two worlds are colliding, with engineers trying to integrate safety-critical systems via the IoT. This would be OK for nonreal time (for example, the smart irrigation systems), but, of course, connecting a CPS via the Internet will result in delays, so hard real-time control would not be possible, for instance, the autonomous control of a car. Looking to the future, there will need to be new development methods (including certification) that can cope with these new integrated IoT/CPS systems, with more use of autonomous control at the edge to cope with intermittent connectivity and periods of outage.

MELLOR: Not knowing what you don't know ("unknown unknowns" for American readers).

TÖRNGREN: A large amount of effort has been spent on investigating challenges for the IoT and CPSs, as reported in the Electronics Components and Systems for European Leadership strategic research agenda[9] and recommendations from the Platforms4CPS project.[10] I would like to highlight the following:

- using CPSs and the IoT to drive and support sustainability
- making sure that future CPS and IoT systems are trustworthy
- managing the complexity of future CPS and IoT systems.

These topics are naturally interrelated.

SZTIPANOVITS: For the IoT: platforms that provide security, dependability, and at least some safety guarantees. For CPSs: composition, assurance, security, the assurance of CPSs with embedded learning-enabled components, DevOps and DevSecOps for CPSs, and, of course, a number of complex issues related to H-CPSs.

BARAS: There are many challenges, as several others have already pointed out. My brief list of the main ones includes the following:

- *IoT*: security standards, privacy standards, containing security breaches at the edge when unknown devices are linked to edge routers, quantitative evaluation of the impact of 5G and 6G, quantitative evaluation of the impact of network virtualization (SDNs, NFV, and so on), and, most importantly, a systems engineering (composability and compositionality) framework to design/implement/operate IoT systems to provably satisfy given requirements
- *CPSs and H-CPSs*: most importantly, a systems engineering (composability and compositionality) framework to design/implement/operate CPSs, networked CPSs, and networked H-CPSs systems to provably satisfy given requirements, security and trust issues, and standards; integrating machine learning and artificial

intelligence (AI) concepts and methods in such systems in a quantifiable and measurable way; developing a taxonomy of architectures for specific subdomains of CPSs; quantifying the effects that the several networks involved in networked CPSs and networked HCPSs have on one another (which is mostly unexplored territory); and developing credible models of human behavior (including social) and their incorporation into H-CPS investigations.

LOGINOV: The main difficulty is the deployment in brownfield (legacy equipment) scenarios. It is the integration with legacy systems that typically takes the most effort.

Approaches to certification will have to change, as we are moving to systems, for example, autonomous cars, where we cannot predict every risk.

***COMPUTER*:** The challenges presented from the last question were well thought out and will most certainly facilitate progress in the right direction. Claire summed it up with her comment on the importance of stricter definitions in both areas, so we can systemically address all of the challenges. The third and final question (based on themes I pulled from your comments), will be a continuation of Haydn's comment regarding "looking to the future" to cope with new integrated IoT/CPS systems.

What/how much progress is being made with the following challenges:

1. trust standards (for example, security, privacy, integration, and safety)
2. integrated requirements (such as the ability to develop IoT and CPS devices in ways where requirements are integrated)
3. risk metrics/provability guarantees (for instance, integrated, quantifiable, and measurable risk metrics; percentages for allowed failure; and so on)?

LOGINOV: We have made a lot of progress, but a lot is yet to be accomplished. It is important to embrace the constant of evolution. As we learn about trust in the IoT, we realize that a lot more still needs to be developed.

THOMPSON:

1. *Trust standards*: We already have standards for safety in various sectors, such as aerospace and automotive. We also have standards for privacy in Europe, including the General Data Protection Regulation. (Moving processing and data to the edge is also beneficial for privacy.) There are standards for security (and there has been a lot of activity on blockchain), and one thing we need in the future is trusted edge clusters. Integration is still a challenging area, though, as there are so many competing standards in this area, and we continue to have difficulties with semantic interoperability. When considering AI (which is now everywhere), we also need to think about transparency and ethical issues concerning trust.
2. *Integrated requirements*: I am not sure what the question is here, as requirements are always integrated. Do you mean integrating CPS and IoT systems? In this case, there are serious issues with proving safety, such as, latency, security, and so on.
3. *Risk metrics/provability guarantees*: My background is in aerospace, so things are very black and white for me. Risk depends on consequences and the probability that a given event will happen. Fundamentally, it is necessary to quantify risk and prove the appropriate figures to meet safety regulations. If you cannot prove this, the system will not be certified. I am thus a bit confused by the question. What I do believe is that approaches to certification will have to change, as we are moving to systems, for example, autonomous cars, where we cannot predict every risk. Here, we may need new approaches that provide a continuously predicted safety guarantee that is valid for a limited time period.

TÖRNGREN: I will complement Haydn's comment with the following:

1. *Trust standards*: Trust/trustworthiness is starting to be used as a new umbrella term, which incorporates dependability as well as attributes like fairness and transparency. This is, for example, noticeable in the new European Union AI guidelines (and proposed legislation). With the increasing capabilities and complexity of CPS and IoT systems, most trust-related aspects face challenges, and their combined consideration poses even greater challenges with the tradeoffs involved. In, for example, automated driving, a large number of new (and evolving) standards are in progress and related to safety and security, attempting to define the "rules" of the game, operational design domains, risk metrics, safety processes for high levels of automated

driving, and how to handle various vulnerabilities (from hardware/software faults, over insufficient specifications and performance imitations, to attacks).

2. *Integrated requirements*: My comments are similar to Haydn's.
3. *Risk metrics/provability guarantees*: A main aspect for future highly automated CPSs, operating in more unconstrained environments, is that they will need to reason about risk at runtime. They will thus have built-in risk metrics, which will be evaluated at runtime and have to trade performance versus, for example, safety. They will also be highly complex, emphasizing the need for transparency and explainability, presumably with some sort of mandated "black/red" boxes (like aircraft recorders). Formal models and proofs will be important, but their assumptions have to be scrutinized, and the real world will new generations of CPS, which will always pose surprises since they will (at some point) deviate significantly in their behavior from the model. Thus, resilient designs and architectures will be essential.

MELLOR:

1. *Trust standards*: Standards are difficult in the absence of best practices and a principled view of how to reconcile various aspects. So, in respect to standards, they will be some time in coming. For principles and best practices, work is proceeding apace. See "The Industrial Internet of Things Trustworthiness Framework Foundations."[11]
2. *Integrated requirements*: This is backward. Requirements drive development. Besides, the IIoT and CPSs are the same thing, so what does "integrated requirements" even mean?
3. *Risk metrics/provability guarantees*: Again, the Industrial Internet Consortium is working on this, but we have not published anything [though there are some interesting sections in the Trustworthiness Framework[11] regarding how to represent trust numerically (see section 4.7), which will lead, in time, to metrics].

SZTIPANOVITS: I agree with Martin and Haydn, so let me add just a few remarks. Since there are IoT applications that are not CPSs and CPS applications that are not the IoT, let me just comment on those systems where the two overlap: CPSs that are built on IoT platforms. Consider the following:

1. *Trust standards*: I cannot add too much. The term incorporates a number of different properties and interpretations. A particularly interesting area that is evolving rapidly is human–CPS systems, which force us to contrast the anthropomorphic interpretation of "trust" and possible machine-based interpretations. Networked human–AI–machine teams are emerging in areas such as connected autonomous vehicles, and much needs to be done to understand how to formalize "trust" in these hybrid, complex distributed systems.
2. *Integrated requirements*: I cannot add to what Haydn wrote.
3. *Risk metrics/provability guarantees*: This is becoming a tremendously important issue in autonomous systems (whether IoT based or not). As Martin wrote, the fundamentally new challenge is that these systems cannot be assured only at design time, not only because they are complex but because they frequently incorporate learning-enabled components that can evolve during operations and may be created in a completely data-driven manner (without explicit models). A new research direction in assured autonomy (there is an ongoing DARPA program on this) started developing dynamic assurance concepts that can change during operation and runtime methods that produce a sort of "assurance gauge" indicating whether the system (or some of its components) goes out of conformance with training conditions. Regarding provable guarantees, there are viable results to bound system behavior with runtime safety monitors. This area of research is interesting, important, and wide open.

BARAS: I have the following comments:

1. *Trust standards*: As I frequently state, trust is a very frequently used word and equally frequently abused. In the context of our discussions, there are several quite different meanings of trust. There is the standard meaning that we associate with human interactions. This, in itself, has several versions (for example, direct versus indirect trust). There is trust as it is used in telecommunications and computing, that is, devices, links, nodes, and computers that are trustworthy, meaning that after inspection, they have been found not to be compromised or offered stronger resilience to attacks. There is the trusted platform module, a secure chip standard with keys embedded at manufacturing time (a product of the industry Trusted Computing Group) that is now included in almost 75% of computers. Then there is trust in CPSs and autonomous

systems, where the meaning is that a system executes a task or mission within the tolerance of an expected normal behavior.

Trust/trustworthiness is starting to be used as a new umbrella term, which incorporates dependability as well as attributes like fairness and transparency.

Before we can discuss standards, we need to define what trust means in the various problems relevant to our discussion and develop quantitative models of trust and associated specifications so that we can talk about verification and assurance. In addition, we need to develop trust and mistrust dynamics for single as well as networked systems. There is work along these lines in the various meanings and areas I have mentioned. Then we can define standards of trust in each area and most importantly the interoperability of trust across domains [that is, a way to translate and link trust specifications from area to area and across components, akin to security composition (still unsolved)].

2. *Integrated requirements*: I do not quite understand the thrust of this topic. In CPS and IoT systems, we have requirements to start with, which are modified and new ones are added as we step through a system design (that is, derivative requirements and so on). What is lacking in both areas is a framework for requirements that catalyzes and facilitates compositionality—contract-based design is a big step in this direction. We need a framework to combine requirements of physical components [usually given in terms of constraints and metrics involving numerical variables (continuous and sampled)] and requirements of cyber components [usually given in terms of constraints and metrics involving Boolean (integers) variables and via logic].

   There is mathematical unification between optimization and logic that leads to a unified framework via mixed (that is, numerical and integer variables) multicriteria constrained optimization, constraint-based reasoning, and satisfiability modulo theories and algorithms. But we have still a long way to go to have a framework and tools that are practical and easy to learn and use. Another very important challenge is to come up with an integrated modeling framework and tools to combine space and time specifications and their tolerances as needed because several requirements are now given via temporal logic (linear temporal logic, metric temporal logic, metric interval temporal logic, and signal temporal logic). STL is a step in this direction but a very small one.

3. *Risk metrics/provability guarantees*: Risk metrics are very important because they directly link to robustness and sensitivities to perturbations in inputs and models. There is a fundamental theory from robust control that covers many classes of systems problems but not yet temporal specifications well. The same mathematics that can be used for tradeoff analysis and design space exploration can be used (and has been used) in advanced methods and tools for verification and validation. But with learning components and autonomy we need to develop rigorously what I call *trusted autonomy* (the term *assured autonomy* is also used). Trusted autonomy requires systems to self-monitor their behavior and execution of tasks, self-adjust models and execution to correct anomalies and deviations, and self-learn from task execution and monitoring and anomalies. There is active research in this area but we have a long way to go.

VISHIK:

1. *Trust standards*: As pointed out in other responses, the answer depends on the definition of trust. If trust is understood as it is defined in trusted computing (we trust an application when it behaves the same way under the same circumstances), there are a large number of mature standards. The Trusted Computing Group has developed many of them beyond the trusted platform module. There are a number of International Organization for Standardization (ISO)/International Electrotechnical Commission standards (IEC), and there are several trusted execution environment standards, and the list can be continued. If we include the concept of trustworthiness, we will find a number of developing standards for various environments, such as CPSs and AI, for example, in https://www.iso.org/committee/6794475.html under the ISO/IEC. If we take the term *trust* casually, for example, saying that "without

privacy, it is impossible to achieve trust in the digital economy," applying trust to ethics and societal situations, the use of the word is legitimate, but it doesn't have a rigorous definition and is descriptive rather than terminological.

2. *Integrated requirements*: These are not a new area, but the space has been slow to develop. This is due to a variety of factors, including the traditional separation of research areas between privacy and safety, for example, IT systems and CPSs. But this is a field of study that needs to receive a push from researchers and technologists. If we think about fully automated environments, for instance, self-driving cars and smart cities, codeveloping requirements for safety and security, physical subsystems and their cyber components, and so on, is necessary to move forward. I hope the interest in research in this key area will grow.
3. *Risk metrics/provability guarantees*: Risk metrics and metrics in general have always required considerable effort. The transition from calling for metrics and risk base analysis, publishing single-case risk models, and developing metrics/risk models that could be used in a whole field has always been complicated. The probabilities of failure vary significantly between safety and security and between physical subsystems and cyber components, to give an example. The transition from metrics to models (say, in safety) has also been slower than expected. With increased access to real-time and near-real-time data, these models can be constructed in new data-driven ways.

   The slowness is probably due to the fragmentation of the field. If we resolve the integration issues in point 2, building the quantifiable risk models in point 3 will be feasible, and improving them to make them broadly applicable will be a matter of time.

COMPUTER: Thank you all for your participation in this discussion. You provided valuable insights and highlighted key research areas, especially trust (define trust, trusted edge clusters, semantic interoperability, transparency, fairness, vulnerabilities, developing models and standards of trust, developing trust and mistrust dynamics, and ethical issues), requirements (integrating safety/privacy/security, proving safety, proving latency, and a framework and tools), and risk (models, metrics, quantifying and certifying risks, reasoning about risk at runtime, and trusted/assured autonomy). Is there enough concept overlap within these two technologies that the CPS and IoT communities put on rings and start planning their marriage?

REFERENCES

1. *IEEE Standard for an Architectural Framework for the Internet of Things (IoT)*, IEEE Std 2413-2019, May 21, 2019.
2. Framework for Cyber-Physical Systems, release 1.0, NIST, Gaithersburg, MD, USA, May 2016. [Online]. Available: https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf
3. "Cyber-physical systems public working group smart grid and cyber-physical systems program office engineering laboratory," NIST, Gaithersburg, MD, USA, NIST Special Publication 1500-201, Jun. 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf
4. J. Voas, "Networks of 'Things'," NIST, Gaithersburg, MD, USA, NIST Special Publication 800-183, Jul. 2016. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-183.pdf
5. J. Wikander, M. Torngren, and M. Hanson, "The science and education of mechatronics engineering," *IEEE Robot. Autom. Mag.*, vol. 8, no. 2, pp. 20–26, Jun. 2001, doi: 10.1109/100.932753.
6. "Cyber-physical systems," Engineering Laboratory, National Institute of Standards and Technology, Gaithersburg, MD, USA. Accessed: Dec. 30, 2021. [Online]. Available: https://www.nist.gov/el/cyber-physical-systems
7. "Cybersecurity glossary," National Initiative for Cybersecurity Careers and Studies, Gaithersburg, MD, USA. Accessed: Dec. 30, 2021. [Online]. Available: https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#C
8. "IoT security guidelines: Overview document," GMSA. https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf (accessed Dec. 30, 2021).
9. "Strategic research agenda 2020," ECS. https://www.ecsel.eu/sites/default/files/2020-02/ECS%20SRA%202020%20%281%29.pdf (accessed Dec. 30, 2021).
10. "Platforms4CPS key outcomes and recommendations," Platforms4CPS. https://www.platforms4cps.eu/ (accessed Dec. 30, 2021).
11. M. Buchheit *et al.*, "The Industrial Internet of Things trustworthiness framework foundations," Industrial Internet Consortium. https://www.iiconsortium.org/pdf/Trustworthiness_Framework_Foundations.pdf (accessed Dec. 30, 2021).

JOANNA F. DEFRANCO is an associate professor of software engineering at the Penn State Great Valley School of Graduate Professional Studies, Malvern, Pennsylvania, 19355, USA. Contact her at jfd104@psu.edu.