CYBER-PHYSICAL SYSTEMS
2019, VOL. 5, NO. 3, 145–172
https://doi.org/10.1080/23335777.2019.1624619

ARTICLE

Science of design for societal-scale cyber-physical systems: challenges and opportunities

Janos Sztipanovits[a], Xenofon Koutsoukos[a], Gabor Karsai[a], Shankar Sastry[b], Claire Tomlin[b], Werner Damm[c], Martin Fränzle[c], Jochem Rieger[c], Alexander Pretschner[d] and Frank Köster[e]

[a]Institute for Software Integrated Systems, Vanderbilt University, Nashville, TN, USA; [b]Electrical Engineering and Computer Sciences, University of California, Berkeley, CA, USA; [c]Department of Computer Science, University of Oldenburg, Oldenburg, Germany; [d]Computer Science, Technical University of Munich, München, Germany; [e]Institute for Transportation Systems, German Aerospace Center (DLR), Braunschweig, Germany

ABSTRACT

Emerging industrial platforms such as the Internet of Things (IoT), Industrial Internet (II) in the US and Industrie 4.0 in Europe have tremendously accelerated the development of new generations of Cyber-Physical Systems (CPS) that integrate humans and human organizations (H-CPS) with physical and computation processes and extend to societal-scale systems such as traffic networks, electric grids, or networks of autonomous systems where control is dynamically shifted between humans and machines. Although such societal-scale CPS can potentially affect many aspect of our lives, significant societal strains have emerged about the new technology trends and their impact on how we live. Emerging tensions extend to regulations, certification, insurance, and other societal constructs that are necessary for the widespread adoption of new technologies. If these systems evolve independently in different parts of the world, they will 'hardwire' the social context in which they are created, making interoperation hard or impossible, decreasing reusability, and narrowing markets for products and services. While impacts of new technology trends on social policies have received attention, the other side of the coin – to make systems adaptable to social policies – is nearly absent from engineering and computer science design practice. This paper focuses on technologies that can be adapted to varying public policies and presents (1) hard problems and technical challenges and (2) some recent research approaches and opportunities. The central goal of this paper is to discuss the challenges and opportunities for constructing H-CPS that can be parameterized by social context. The focus in on three major application domains: connected vehicles, transactive energy systems, and unmanned aerial vehicles.

Abbreviations: CPS: Cyber-physical systems; H-CPS: Human-cyber-physical systems; CV: Connected vehicle; II: Industrial Internet; IoT: Internet of Things

ARTICLE HISTORY
Received 27 January 2019
Accepted 7 May 2019

KEYWORDS
Cyber-physical systems; social context; incentives; conflict resolution; policy

CONTACT Janos Sztipanovits janos.sztipanovits@vanderbilt.edu Vanderbilt University, VUSE-ISIS building, 1025 16th Ave S, Suite 102, Nashville, TN 37212, USA.

1. Introduction

Cyber-Physical Systems (CPS) are apervasive enabling technology advancement, which is impacting all industrial sectors and almost all aspects of society. Arecent study by McKinsey [1] estimates that the on-going digitisation of industry will potentially add 1.5 trillion US to the GDP of the United States by 2025 and 1 trillion EUR to the GDP in Europe. Emerging industrial platforms such as the Internet of Things (IoT), Industrial Internet (II) in the US [2] and Industrie 4.0 in Europe [3,4] are triggering a‘gold rush’ toward new markets and are creating societal-scale systems, which importantly, in addition to the synergy of computational and physical components, involve human components (H-CPS). H-CPS are at the heart of today's sharing economy and the driver of new industry sectors that involve humans interacting with CPS. These sectors are producing companies which are changing how we live. For example, the future of mobility is being determined by companies like Uber, Lyft, Olla and Didi, which are transforming personal transportation into aservice. In addition, shared use of the third aerial dimension is being used to determine the future of logistics, and how we deliver goods through our urban and rural infrastructures.

It is not surprising that we are beginning to see societal tensions developing because of new technologies with massive social impacts, and, potentially, conflicting social expectations and policies. These tensions are particularly evident in the following areas:

- *Autonomous and Shared Control H-CPS* A new generation of autonomous systems is emerging where the division of control can be dynamically shifted between humans and machines. Addressing the research challenges of modelling human decision making and responses in automation is key for making outcomes provable. Without solving these challenges, the societal acceptability of associated risks and liabilities remains questionable.
- *Privacy* Emerging societal-scale H-CPS creates fundamental conflicts between the utility of services, costs, personal and institutional privacy and social fairness and justice. Without suitable incentive design schemes, we may well be left with either policies that are too restrictive, or the policies may result in accidental compromises of information, adverse selection, or unfair information rents.

The debates about licensing and liability of self-driving cars on roads, unmanned aerial vehicles (UAVs) on aerial highways, the threats of litigation against self-driving features of automobiles like Tesla, and the controversies created by smart city and smart home technologies regarding privacy violations are all indications of the build-up of societal strains about the impact of these new technology trends. These tensions now extend to regulations, certification, insurance and other societal constructs that are necessary for the widespread adoption of these new technologies into our societal-scale systems. In spite of the heterogeneity of the application domains, a common insight has emerged: 'There is an absolute necessity of societal discourse in architecting and constraining the new generations of H-CPS.' We illustrate this imperative via two examples: (1) Dynamic traffic-aware routing and (2) self-driving cars.

- *Dynamic Traffic-Aware Routing* An interesting H-CPS application is Google Maps' dynamic, traffic-aware routing service. Real-time sensing of traffic flow, congestion weighted routing service and drivers decisions on accepting or rejecting the routing recommendation form a complex, closed loop networked control system for the overall traffic flow. Dynamics are emerging from the networked interactions among physical systems (cars), physical processes (traffic flow), routing algorithms, human decisions (drivers) and network delays. The system has societal impact with winners and losers. Drivers are incentivised and rewarded by saving travel time and fuel. The societal interest is satisfied by a more balanced traffic flow and better utilisation of the existing infrastructure. However, the cost is paid by (previously under-utilised) neighbourhoods, to which dynamic routing is diverting the traffic, in terms of the increased threat of accidents, air pollution and noise. Should the trade-off among conflicting interests be decided by the service provider, or should the company, in collaboration with stakeholders (including residents of previously quiet neighbourhoods), build a system that can accommodate local policies emerging at societal forums?
- *Self-Driving Cars* A much more controversial problem where technical solutions lead to major social dilemmas is self-driving cars making life-and-death decisions especially in situations where they have to choose between the 'lesser of two evils'. Currently, for example, there is a sharp contrast between societal norms and laws in the US and Germany. In the US, the issue is, by and large, open for societal discourse, while in Germany it is unconstitutional to leave life-and-death decisions to automation, based on an argumentation of the German Constitutional Court which ruled unconstitutional a proposed law for assuring safety of airspace by allowing automated shooting down of hijacked aircraft [5]. We cannot expect that there will be uniform societal responses to this moral dilemma; however, it is clear that whatever positions are accepted, they will have deep consequences on technical solutions.

As these examples illustrate, societal-scale CPS are motivated by societal needs, and must conform to social norms and respond to expectations. If these systems evolve independently in different parts of the world they will hard-wire the social context in which they are created. That will make interoperation hard or even impossible, decrease reusability and narrow markets for products and services. In fact, for products marketed globally, such as cars, it is imperative that the products are tailored to country-specific regulations. There are complementary but interrelated solution approaches to this challenge: (1) Create public policy that is aware of technologies and technology shifts and (2) develop technologies that adapt to different public policies. The primary emphasis of our work belongs to the second approach. ***The central goal of the paper is to discuss the challenges and opportunities for constructing H-CPS systems that can be parameterised by social context.*** The primary application domains we consider to illustrate the technical challenges and research opportunities are: (1) Connected Vehicles (intelligent transportation systems domain), (2) Transactive Energy Systems (smart grid domain) and (3) Unmanned Air Vehicle Traffic Management (smart city services domain).

In Section 2, the paper briefly defines CPS and presents background and related work that needs to be considered in the context of the proposed research agenda. Section 3 discusses societal aspects for the three major application domains considered in the paper. In Section 4, we outline the main hard problems for designing societal-scale H-CPS and the overarching research challenges. Section 5 proposes four synergistic approaches for parameterising H-CPS with societal context: Incentive engineering, online conflict resolution, policy-aware system synthesis and policy auditing. Finally, Section 6 summarises the main conclusions from our initial work.

2. Background and related research in CPS and H-CPS

According to one of the widely accepted definitions, CPS are smart-engineered systems with functionality that emerges from the networked interaction of computational and physical processes [6]. Most modern products already are or rapidly becoming CPS driven by new requirements and competitive pressures. The tight integration of physical and computational components creates new generations of smart systems whose impacts are revolutionary; this is evident today in emerging autonomous vehicles, military platforms, intelligent buildings, smart energy systems, intelligent transportation systems, robots and smart medical devices. Unparalleled pervasive sensing, actuating and computation, together with real-time networked information are creating a new generation of systems that will be able to execute extraordinary tasks that are barely imagined today transforming transportation, energy, health care, and other sectors of the economy.

In recent years, CPS as a multidimensional and complex system IoT has attracted considerable attention in industry, academia and government [7]. Emerging industrial platforms such as IoT, Industrial Internet (II) in the US and Industrie 4.0 in Europe are triggering a gold rush toward new markets and are creating societal-scale systems, which importantly, in addition to the synergy of computational and physical components, involve humans (H-CPS). H-CPS areat the heart of today's sharing economy and the driver of new kinds of industry sectors that involve humans interacting with CPS. These sectors are now producing companies, products and services in transportation, energy and healthcare which are changing how we live. For example, the future of mobility is being determined by companies which are transforming personal transportation into a service. In addition, shared use of the third aerial dimension is being used to determine the future of logistics, and how we deliver goods through our urban and rural infrastructures.

The past 20 years provided ample evidence that the separation of computing and physical sciences has created a divergence in scientific foundations that has become strongly limiting to achieve progress in CPS [8]. CPS are not just ensemble of systems designed separately and integrated to meet the desired functionality. Their transformative potential stems from the heterogeneity of the constituents parts coupled with tight connectedness and integration which is typically achieved via networking and information technologies. Salient system characteristics are emerging through the interaction of physical and computational objects and it is not possible to identify whether emerging behaviours are the result of computations (computer programs), physical laws, or both working together.

CPS permeate all aspects of modern life, from our infrastructure to our personal use devices ranging from medical devices to automobiles. We depend on CPS to operate not only in a manner that is safe and reliable but also ethical and fair. While typical CPS research addresses the tight interaction between the physical and cyber parts, in-depth consideration of their societal implications and impact on how we live is still in early stages.

The key to building systems which can be integrated into societal-scale infrastructures is an envisioned design methodology and tools that take into account proofs of correctness-by-construction, verification of correct functioning, models of human cognition, societal norms and values and responses of humans to automation systems. These systems need to provide safety and security assurances, resilience guarantees and privacy guarantees at least to the level that makes assessing and quantifying risks acceptable for insuring these systems. To achieve these goals, it is necessary to integrate advances from a broad research agenda in CPS and H-CPS developed over a decade that include: (1) Foundations for design of composable and predictable CPS, (2) security and resilience of CPS against failures and cyber-attacks and (3) interactions among humans, human organisations, and networked CPS. In the following, we overview some of the related work from these areas that provides the foundations for the design of societal-scale CPS.

CPS are best described using hybrid system models of computation. Hybrid system theory lies at the intersection of the fields of engineering control theory and computer science verification. To understand the behaviour of hybrid systems, simulate and control these systems, theoretical advances, analyses and numerical tools are needed. A general model for a hybrid system along with an overview of methods for verifying continuous and hybrid systems is presented in [9]. The proposed verification technique for hybrid systems is based on two-person zero-sum game theory for automata and continuous dynamical systems. The unique challenges in CPS design emerge from the heterogeneity of components and interactions. Composition for heterogeneous systems focusing on stability has been investigated using a passivity-based design approach that decouples stability from timing uncertainties caused by networking and computation in [10]. Cross-domain abstractions that provide effective solution for model-based fully automated software synthesis and high-fidelity performance analysis are also presented. CPS challenge the established boundaries between disciplines, and thus, the software tools available for design. The design and implementation of an experimental design automation tool suite for CPS is described in [11]. The key new components are model integration languages and the mathematical framework and tool for the compositional specification of their semantics. Synthesis of complex systems that consist of multiple-distributed systems is a very hard problem that can benefit from compositional techniques. A compositional approach for synthesis of distributed CPS is presented in [12], and it has dramatically better complexity and is uniformly applicable to all system architectures.

The consequences of successful attacks on control networks can be more damaging than attacks on information networks because control systems are at the core of many critical infrastructures. Safety and security of networked control systems under denial-of-service-attacks have been considered in [13]. Designing incentives for investing in network reliability and security have been studied in [14]. The problem is formulated and analysed as a non-cooperative two-stage game, and it is shown that security and reliability decisions are tightly coupled, and should be considered jointly to improve efficiency. The challenges emerging from heterogeneous systems in the presence of aperiodic sampling and denial-of-service attacks have been studied in [15]. Safety and security have traditionally been distinct problems, but the tight integration of cyber and physical components in CPS has created new problems. A safety/security threat model for CPS various techniques to improve the safety and security of CPS is presented in [16]. The main challenges and a roadmap for building a resilient IoT for CPS are presented in [17].

Security and resilience are system properties emerging from the intersection of system dynamics and the computing architecture. A modelling and simulation integration platform for experimentation and evaluation of resilient CPS is presented using smart transportation systems as the application domain in [18]. Evaluation of resilience is based on attacker-defender games using simulations of sufficient fidelity. Connected vehicles, transactive energy systems and unmanned aerial vehicles share many common characteristics that include security concerns as well as countermeasures for protection [19].

Connected vehicles required substantial new innovations for reliability and security. The benefits and perils of decentralised vehicle-to-vehicle communication for hazard warning are studied in [20]. It is shown that the timely delivery of such crucial information is a safety goal. The results derived by simulation provide valuable insights for the reliability of timely message reception. Beyond simulation, a prototyping platform for investigating the impact of attacks against automotive networks is developed in [21]. The goal of the prototyping platform is to investigate and demonstrate different security aspects and scenarios as while using standardised hardware and software components.

Although research for design of composable, predictable, reliable and secure CPS must continue, investigating the interactions among humans, human organisations and networked CPS is essential in designing societal-scale H-CPS. An overview of the main challenges in the specification, design and verification of human cyber-physical systems, with a special focus on semi-autonomous vehicles is discussed in [22]. Human interaction with the physical world is increasingly mediated by automation. This interaction is characterised by dynamic coupling between cyber and human decision-making agents. Guaranteeing performance of such H-CPS requires predictive mathematical models of this dynamic coupling. A dynamic inverse model for a human operator of a quadrotor is developed in [23]. Modelling the interactions between an autonomous car and a human driver as a dynamical system where the robot's actions have immediate consequences on the state of the car but also on human actions is considered in [24]. The user study presented suggests that the robot is indeed capable of eliciting desired changes in human state by planning using this dynamical system. A simulation model of human driver attention allocation is presented in [25]. The simulation model relates attention directly to a task model and it is able to automatically measure task-dependent event frequencies and adapt its distribution of attention according to these frequencies. The simulation model is used to create a dynamic cognitive driver model that reproduces similar effects. A comprehensive and harmonised method for assessing the effectiveness of advanced driver assistance systems by virtual simulation is presented in [26], with the problem of rare-event coverage being addressed in [27]. A collection of human models in transportation, critical issues in human modelling and assisted transportation, and studies of human behaviour, error and risk assessment are presented in [28].

CPS affect society and human lives in a multitude of ways. Societal strains caused by these emerging technologies give rise to significant questions of policy and regulation [29]. Important research directions are related not only to privacy, security but also to management and regulation of the emerging societal-scale CPS. Although creating public policy that is aware of technologies and technology shifts is a very important research direction, our work focuses on developing technologies that can be adapted to varying public policies. Before presenting promising technology approaches for providing adaptability to societal context, we briefly discuss three major CPS application domains, connected vehicles, transactive energy systems and unmanned aerial vehicles, to illustrate the technical challenges and opportunities.

3. New application domains

3.1. Connected vehicles

Connected Vehicle (CV) technology provides services that are based on vehicles that are equipped with communication and computation resources that enable vehicles to recognise their location and their status, and to communicate with each other and the surrounding Intelligent Transportation System (ITS) infrastructure [30]. An introduction to the history and concepts of connected and automated vehicle systems can be found in [31]. The evolution of the connected car taking into account technology maturity levels, driving factors and business models of connected cars is described in [32]. Today, vehicles are increasingly being connected to the IoT. The benefits of the Internet-of-Vehicles (IoV) and industry standards are discussed in [33]. An examination of the interactions between CV technology and the environment at the levels of vehicle, transportation system, urban system and society is presented in [34]. Although net positive environmental impacts are anticipated at the vehicle, transportation system and urban system levels, greater vehicle utilisation and shifts in travel patterns at the society level are expected to offset some of these benefits.

The primary motivations for CV applications are accident prevention, improved safety and mobility as well as environmental benefits. Safety applications exploit increased situational awareness to reduce or eliminate crashes through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications. Mobility applications include driver advisories and warnings, and vehicle and/or infrastructure controls utilising real-time data from equipment located onboard vehicles and within the transportation infrastructure. CV data are transmitted via a range of communication media and are used by transportation managers in a wide range of dynamic, multi-modal applications to manage the transportation system for optimum performance.

In the US, the US Department of Transportation (USDOT) has established a major program for defining the Connected Vehicle Reference Implementation Architecture (CVRIA) and developing a suite of regional pilot implementations (https://www.standards.its.dot.gov/). CVRIA is a collection of applications (over 100) documented by precisely defined architecture models using enterprise, functional, physical and communication views. The goal of the CVRIA framework is integrating CV technologies and identifying candidate interfaces for standardisation. While not elaborated deeply in the existing CVRIA models, safety and privacy are driving concerns for the proposed technology solutions.

In Europe, the Amsterdam Group (https://amsterdamgroup.mett.nl/) integrates four key umbrella organisations (Car2Car Communication Consortium (C2CC-CC), representing the industrial side (https://www.car-2-car.org/); Polis, representing European Cities including societal aspects (http://www.polisnetwork.eu/); ASECAP, the European Association of Operators of Toll Road Infrastructures (http://www.asecap.com/); and CEDR, the Platform for Cooperation between National Road Authorities (http://www.cedr.eu/)). The goal of the consortium is close cooperation with the European and international standardisation organisations as a key contributor, and in cooperation with infrastructure stakeholders, joint deployment of cooperative ITS. With the publication of the Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committee and the Committee of the Regions: A European strategy on Cooperative Intelligent Transport Systems, a milestone towards cooperative, connected and automated mobility Document COM (2016) 766 final on 30 November 2016, the European Commission has set the scene for C-ITS deployment in Europe.

While CV technology is not necessarily (yet) linked to autonomously driving vehicles, these technologies are mutually supportive. Automated driving benefits from the added electronic horizon provided by CV technology and CV benefit from the capabilities to fully automatically influence the dynamics of cars, in particular for increasing safety and optimising resource usage and decreasing carbon footprint. However, their introduction raises several concerns:

- As long as humans remain in control, drivers use both their intuition and reflexes to deal with extreme situations and there are well-established rules regarding liability. When this task is delegated to automation, current acceptance/certification processes relying on test-driving cannot possibly cope with the complexity of the systems responsible for situational awareness and decision making in autonomous vehicles.
- Autonomy assumes that principles of decision making to resolve extreme situations will be enforced by software, which are otherwise resolved by humans. These challenges have triggered a substantial debate about the ethical dimensions of decision making in autonomous systems [35] and caused the Germany Ministry of Transportation to install a dedicated commission to address ethical, societal and legal dimensions for autonomous driving.
- The inherent reliance on communication makes CV-guided traffic vulnerable to terrorist that could potentially cause drastic traffic disasters and even the complete collapse of large segments of transportation networks.
- Humans in cars are subjected to decision making in traffic optimisation systems, which are unaware of individual high urgency goals of

> individuals, for example, resulting from acute and critical health problems. While the need for societally agreed policies in weighing priorities between societal and individual goals of different traffic participants, the US and German approaches to this differ. For example, in a number of US states, autonomous vehicles are allowed to be used as long as insurance policies are demonstrated that cover damages induced from the autonomous car, while recent German legislation demands that drivers must ultimately always be able to take over control whenever the cars automation system issues a take-over request.

Research in CV must address the impacts of differences in social expectations regarding safety, security and privacy. The introduction of autonomy brings up safety concerns that are represented as conflicting individual, organisational and societal goals. Managing these conflicting goals requires capturing and formally modelling goals and social norms that should influence built in online conflict resolution mechanisms.

3.2. Transactive energy systems

Smart energy and electricity networks are a crucial component in building smart city architectures; their consistent and harmonised inclusion in the smart city design should be carefully considered through a detailed analysis of the impacts (environmental, energy, economic, societal) and the implementation of cost-benefit analysis (CBA), not only in terms of managing the grid itself but also in a wider perspective that includes environmental, security and social aspects. This paper first discusses the main impact that smart grid deployment has, in different respects, in smart cities and then presents a methodology for an extended CBA, able to go beyond the strictly financial aspects. It is based on previous developments at the European level. The methodology conceptually illustrated can naturally be extended to the assessment of proposals for the development of smart cities.

Power grids today are going through a major transformation with the increased use of renewable energy generation technologies and market-based transactive exchanges between energy producers and consumers [36]. Transactive Energy Systems (TES) integrate economic and control mechanisms that allow the dynamic balance of supply and demand across the entire electrical infrastructure using value as a key operational parameter [37]. The motivation for transactive energy comes from the increasing diversity of resources and components in the electric power system and the inability of existing practices to accommodate these changes. Expanded deployment of variable generation on the bulk power side, distributed energy resources throughout the system, and new intelligent load devices and appliances on the consumption side necessitate new approaches to H-CPS, with new business models for how electric power is managed and delivered. Smart energy and electricity networks are a crucial component in smart cities and have significant environmental, energy, economic and societal impacts [38]. Their design and implementation require a broad perspective that includes environmental, security and social aspects.

TES intend to achieve multi-objective optimisation via the combination of distributed control system principles and economic practices such as markets. The economic aspects of the formulation of TES solutions, however, relate to Federal and State policies and regulations that are driven by societal forces. For example, one concern is whether a given TES implementation satisfies the required level of separation between markets and operations. Market mechanisms and the designed incentives should also be flexible and configurable enough to accommodate fair energy policies and motivate the participants' behaviours. These challenges lead to the technical approaches in *Incentive Engineering* discussed in Section 5.

Social context is an essential factor on the level of individual consumers as well. The CPS infrastructure for TES includes smart meters that are replacing manual meter reading. Smart meters offer significant benefits to utilities and end users by providing more detailed information about energy usage via the possibility for disaggregating consumption data. One example of the social conflicts that have emerged is the fear that smart meters would potentially lead to a detailed surveillance of activities in the home. As a significant consequence of this fear in Europe, the Dutch Senate rejected a Smart Metering Bill in April 2009 that would have mandated its use in every home [39]. In the US, we examined some aspects of public acceptance challenges of smart meters and showed a range of consumer concerns with smart meters [40]. These concerns vary across the country and have led to differing regulatory approaches to the use of energy-conserving demand reduction technologies. Another type of conflict involves the negotiation of utility needs for a stable revenue stream with the disruptions associated with distributed generation and the emergence of the prosumer. The adjudication of the conflicts has created enormous opportunities for software systems that can integrate prosumers and micro-grid systems into the transformed utility models.

We believe that the TES application domain – with its very strong relationship to economic policy and regulations, privacy and security policies, and consumer expectations on dependability and trust – is an extremely significant domain to define technology challenges for developing systems that are adaptable to social context.

3.3. *Unmanned aerial vehicles*

Recently, there has been an immense surge of interest in using unmanned and remotely controlled aerial vehicles, also known as drones, for civil applications

[41,42]. Through projects such as Amazon Prime Air, Google Project Wing and Airbuss Project Vahana (a partnership between Airbus and Uber), many companies are investing in drone services such as commercial package delivery, flying taxi service, aerial surveillance, emergency supply delivery, videography, and search and rescue. Furthermore, this transition is happening worldwide, in North America and in Europe, most recently in China, and in the UAE. Because drones are envisioned to fly in the low altitude space, between 200 and 500 feet, the allocation of this airspace must be done carefully to maximise safety, efficiency and ease of human participation while minimising environmental impacts and discomfort, particularly in urban/suburban settings. The use of UAVs in commercial applications has the potential to dramatically alter several industries and impact our daily lives. Safety, security, privacy, ownership, liability and regulation cause significant challenges that must be addressed. Such societal issues and possible recommendations are studied in [43].

We are engaged in developing tools [44] for government agencies to establish low altitude air transport infrastructures, relying on a combination of systems analysis and publicly available data from sources including NASA, FAA, ArcGIS (population density) and NOAA (weather data). We have proposed the concept of air highways or virtual pathways in the airspace. Air highways provide a scalable and intuitive way for managing a large number of drones. These paths can be updated in real-time according to changes in the airspace. Trunks and branches of air highways, similar to ground-based highway systems, naturally emerge. For regional and city-level drone infrastructure, the next step would be to consider multiple levels of air highways, possibly separated by altitude. The goals in the design of these highway networks include connectivity between cities, efficient and safe use of different altitude levels, and flexibility with respect to unknown or changing conditions in the airspace. Many practical details, such as the locations of and rules for intersections and exits, need to be designed. For last-mile drone planning, one potential solution would be to use a priority-based method for reserving space-time for each drone. However, unlike traditional route planning methods which reserve a large block of the airspace for a long period of time, adopting a fine-grain space-time reservation would greatly improve throughput. Last-mile operations will involve drones flying in proximity to humans and other important assets on the ground, necessitating H-CPS research. Data needed by drones and drone operators for planning include city zoning maps which provide priors for human occupancy, cellular traffic data which can be used to infer human occupancy, and road traffic data which for predicting day-to-day human movement.

The intended customers of this innovation and associated software are institutions that need to establish low altitude traffic rules or monitor the status of air traffic, including government agencies as well as companies using the infrastructure. There are many social conflicts that need to be resolved. The US Supreme Court has already ruled that an altitude below 200 feet belongs to property owners (effectively adding a third dimension to property ownership) and that the FAA potentially has jurisdiction of the airspace above 500 feet. In the case of licensed operators, the FAA and NASA are willing to open up the airspace between 500 feet and approximately 2500 feet. It has been proposed to use air corridors above roadways and railways. However, there are still concerns about noise, potential loss of control and liability from accidents.

Privacy concerns about camera-carrying UAVs are also being discussed in the framework of Electronic Communications Privacy Act (ECPA) and EU directive 2002/58/EC. While there are differences between the US and EU rules, we believe that mechanism design research can address data privacy aspects as discussed in Section 5. In addition to data privacy, there are broader public concerns that may be addressed through system design. For example, systems may need to be designed with opt-out rights and opt-in incentives similar to those now in effect for smart meters and connected household appliances.

4. Hard problems and technical challenges

The challenges in developing a science of design for societal-scale H-CPS are compounded due to significant semantic gaps between (1) the scientific methods used in different disciplines (engineering, policy, economics, sociology, psychology) that are needed to investigate the societal impacts as well as (2) the different models and representation across abstraction layers and CPS application domains. These challenges call for a systems science that seeks answers to the following questions:

- What are the key differences in the social context between different parts of the world in the various H-CPS application domains?
- What are the emerging social policy differences and how to represent these policies in a formal, unambiguous way?
- What are the analytical approaches to model and compose system elements, policies and humans at different layers?
- What are the common semantic domains, in which the cross-layer interactions can be described, constrained, and used to compose global properties?
- What are the theoretical foundations to analyse the dynamics of H-CPS that evolve based on policies, constraints and complex interactions?
- How can the technical approaches be integrated into domain-specific H-CPS system architectures and how do they contribute to policy-based customisation?

- What is the operational framework to simulate multi-model interoperation of individual elements across different layers and how simulations can be used for evaluation of system properties?
- How to validate the proposed solutions in selected application domains on experimental test beds?

Transforming design of societal-scale CPS from a high-risk management practice into an engineering discipline based on science is a significant challenge that requires a collaborative and integrative effort. To achieve progress toward this goal, we must address the following overarching research challenges:

- Understanding the nature, scope and evolution of policies and societal expectations in the operation of societal-scale H-CPS as well as their comparative analysis. The purpose of the analysis is not only for shaping of social policies, but also for the exploration and identification of those factors that have the greatest influence on technical solutions.
- Investigating methods for the explicit and formal representation of societal context that include: (1) Incentives, pricing and market policies; (2) operational policies (resource priorities, levels of autonomy); and (3) privacy, security and safety policies. In this context, policies are on the one hand, expressions of societal expectations, and on the other hand formal, machine-interpretable constructs that have potentially deep impact on the structure and operation of H-CPS.
- Developing architectures that guarantee the enforcement of policy requirements in the operation of a new generation of H-CPS in the various application domains.

The dominant trend in societal-scale H-CPS is that technology becomes more human-centric, more contextual and adaptable. Our main hypothesis is that technically impactful differences in social context can be expressed formally, and these representations can be used for adapting technology solutions. The primary challenge is to validate this hypothesis by (1) showing examples for essential differences in social context in the selected three application domains, (2) developing methods for formally representing elements of the social context (values, policies, regulations) and (3) convincingly demonstrating solutions for using these representations as parameters of H-CPS architectures that can significantly influence system properties and behaviours.

Admittedly, the differences in social context would be significantly larger if we expand our scope to additional application domains. However, we believe that even this restricted scope that is synergistic with available resources is sufficient to demonstrate the central tenet of this research: ***Future generations***

of societal-scale H-CPS need to consider social context as an essential parameter for deployed systems.

5. Research approaches and opportunities

The selected domains have strong societal implications and exemplify requirements for safety, privacy, security and dependability policy compliance that are sufficiently different for testing a range of technology solutions. We present four complementary technology approaches for developing H-CPS that are promising for providing adaptability to social context: (1) Incentive engineering, (2) online conflict resolution, (3) policy aware architecture synthesis and (4) policy auditing. These approaches have different characteristics in terms of the scope and required formalism for policy representation and the assurances required for satisfying different policies during operation.

Parameterising H-CPS architectures with social context requires (1) formal modelling of relevant aspects of social contexts and (2) mechanisms that modify the architecture and/or behaviour of H-CPS by means of these models. Incentive engineering, online conflict resolution, policy-aware architecture synthesis and policy auditing utilise different mechanisms and have complementary roles in the adaptation process. We can differentiate these roles and clarify their relationship using a simplified conceptualisation of H-CPS as a layered architecture as shown in Figure 1. The H-CPS application domains are being transformed, or are poised to be transformed, with a wealth of data about the physical systems themselves, as well as how they are being used and valued by people. Sometimes this is termed as putting an 'Internet of Things (IoT)' or Network Layer on top of the physical infrastructure systems, whether it is ground or air transportation, or transactive energy. Travel advisory systems, ridesharing services, automated package delivery and energy aggregation services, are all examples of existing field-tested services (Service Platform Layer) and applications (Application Layer) where real-time operational data, as well as peoples preferences, decisions and use (Human Layer) are in the critical control path.

An issue at the heart of the proposed technology solution is a fundamental co-design problem: ***We need to design distributed control mechanisms that are adaptable to social context and policies in parallel with incentivisation schemes for users to achieve desirable operation of the system as a whole.*** The technology approaches that we investigate are associated with different architectural layers and provide customisation options for different elements of social contexts.

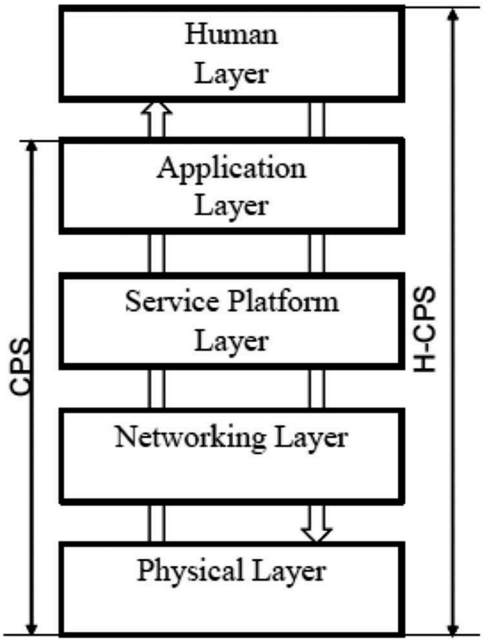

Figure 1. H-CPS architecture layers.

5.1. Incentive engineering

Incentives are a way of inducing modifications of human behaviour by appealing to economic, moral, social and altruistic motivations. Game theory approaches model incentives through the addition of extra terms into player utilities. Incentive engineering is increasingly viewed as the core of modern economic analysis, and has two roles in modern H-CPS design:

(1) In H-CPS where humans are indirectly involved in system operation (by selecting architectures, weighting optimisation criteria, making investment decisions), incentives are used to invest in such a way as to improve the composite properties of the CPS system both at the strategic and tactical levels. For example, incentives expressed in public policies and regulations are used to establish design criteria for the layout of low altitude air highways.

(2) In H-CPS where human behaviour is directly involved in the properties of the overall system dynamics (both the connected vehicle and transactive energy domains are good examples for this), incentive engineering is used to modulate the decision loop of individual players (drivers, customers) such that the overall system behaviour converges toward a societal optimum.

The mathematical foundation for incentive engineering is mechanism design [45], a field in game theory that uses an engineering approach to find the modified game (i.e., the game induced by the specific mechanism), in which Nash equilibria is improved relative to the original game, i.e., equilibrium allocations of the modified game will be closer to (or even coincide with) socially optimal allocation of the original game, to close the gap between the competitive Nash equilibrium of multiple users and the societal good equilibrium (sometimes referred to as the price of anarchy). While this idea has been at the heart of several recent Nobel prizes in Economics, the details of so-called dynamic mechanism design for heterogeneous users are quite subtle and very much in their infancy. Research in this direction must focus on utilising data analysis for the development of new services which include mechanisms of resilience to faults as well as to physical and cyber-attacks. Already, in the connected vehicle and transactive energy domains, commoditisation of data has led to the creation, distribution and monetisation of new products and services at unprecedented levels. At the same time, inefficiencies arise naturally due to asymmetric information and selfishness, such as severe traffic jams as an unintended consequence of routing advisories [46], and vulnerabilities arising from cyberattacks that can cripple traffic networks [47].

Understanding and shaping the incentive structure and motivations of entities including the end user, third-party solution providers, service providers, adversarial agents and regulators of the data market will be necessary for quantifying and identifying inefficiencies, including issues of fairness across different sectors of the population, as well as security and privacy [48]. We have developed models for rational, strategic interactions that lead to novel, computationally tractable representations of Nash equilibria [49]. While we show even myopic players will converge to these equilibria, there is a need to move beyond the traditional-expected utility maximisation framework as it is well known that humans are not perfectly rational. Drawing from non-expected utility [50] and prospect theory [51], an important goal is to create new equilibrium concepts, understand how users arrive at these equilibria, and analyse the outcomes (e.g., measures of societal good versus fairness to the individual). Using experimentation on actual test beds, it is also important to reconcile the beliefs that people have and the decisions they make from the beliefs and decisions assumed in traditional economic models.

In designing incentive mechanisms, progress will depend on user opt-in; however, excess demand can cripple infrastructure. Building on previous work aimed at shifting Nash equilibria to social optima [48], the objective is to design scalable, real-time incentive mechanisms that are responsive to social context (such as perceived notion of fairness, social welfare and social norms), capitalise on access to streaming data in order to improve efficiency, fairness and social welfare while accounting for degrees of bounded rationality in user decision making. Once again as in the case of the road traffic management, the effects of loop closure around the human decision making on the composite system are an open question. The recently emerging field of Mean Field Games (see [52,53]) is relevant in this regard, but it needs to be modified to allow for inhomogeneous user types.

5.2. Online conflict resolution

Societal scale H-CPS increasingly incorporate autonomy complementing the Human Layer (see Figure 1) with capabilities that may dynamically shift control authority between humans and machines. Autonomous operations bring up a different dimension of potential conflicts with social context. While human decisions are motivated by ethics, morality, incentives and deterrence, autonomy needs to include explicit mechanisms for online conflict resolution to resolve partially conflicting goals in situation dependent manner. Progress in the area requires investigating H-CPS architectures that encapsulate online conflict resolution between individual, organisational and societal goals. Mapping societal norms and expectations to some formal constructs (such context-dependent priorities expressed as partial orders) is a very hard problem and require collaboration among social, cognitive and computer scientists.

Suitable and necessarily multi-valued and non-standard logics [54–57] that are expressive enough are needed to capture a broad variety of goals:

(1) Time-bounded probabilistic reachability properties (e.g., to reach a highway exit) [58];
(2) Performance measures such as optimal resource usage and minimal energy consumption [59,60];
(3) Aggregated goals requiring Pareto-optima between their sub-goals [61];
(4) Situational varying strength levels of goals [62], where situations may involve states of human actors [63–65] or state of the controlled physical system;
(5) State-dependent goals, such as goals dependent on beliefs [66] on states, accumulated measures, or goals of other systems [67].

As we capture different strength levels by assuming goals to be partially ordered; hence, strategies are only allowed to sacrifice a lower level goal if no strategy exists achieving both this goal and all higher level goals [12,68]. To capture state dependence, we can assume that a system's current own priorities between goals can be captured by goal-labelled probabilistic hybrid automata [59,60], where transitions reflect changes in the mental state of the human, the physical state of the system, timers, or any combination of these. Each mode of such an automaton is labelled by the partial order of aggregated goals prevalent in this mode. We call such automata the goal automata of the system. Building on [62], we are developing a meta-model of Societal Scale H-CPS that associates with each system at all levels of the hierarchy a goal automaton, and addresses two categories of situations for conflict resolution:

(1) Whenever a system *S* (human and/or technical) enters the scope of an encompassing system *ES* which has capabilities of influencing *S*, then

a negotiation between S and ES takes place which partially resolves possible conflicts between the goals of S and the goals of ES. This resolution may include the denial of entry of S into ES. ES may be an organisational entity (such as a country, a company) or a technical system (such as an air-traffic control system). Whenever S leaves ES, the original goals of S are restored, and all obligations agreed to when entering ES are nullified.

(2) Whenever S and ES dynamically encounter situations in which goals of S and ES and possibly other subsystems $S_1, \ldots, S_n$ are conflicting, the systems $S,\ ES,$ and $S_1, \ldots, S_n$ negotiate dynamically a time-bounded contract [69] for jointly resolving the currently encountered conflicts [57]. The metamodel offers support for efficiently and successfully pursuing such negotiations. Any conflict resolution strategy can be abstractly characterised in this setting as defining a new partial order for S (resp S_j), which then reflects the current prioritisation of the relative importance of the goals of $S, ES,$ and S_j. Note that state changes in the involved system may trigger the need for a renegotiation. An onine conflict resolution strategy can thus be captured mathematically as an operator which takes the current partial orders of goals of $S, ES,$ and all S_j and defines for S (for S_j) a new partial order as well as the duration of this contract.

Existing frameworks for online conflict resolution can be expressed in this setting. A promising research direction is to consider a subset of regulatory goals, which may differ in different countries to demonstrate the parameterisability of this setting to country-specific sets of regulations.

5.3. Policy-aware system synthesis

Security concerns play a significant role in the implementation of H-CPS. A fundamental concern of system design is to introduce and enforce end-to-end security policies that are essential for safety and privacy. Putting policies in place from the beginning will ensure that services are end-to-end secure and provide citizens with real knowledge about the data collection and usage. Well-accepted guidelines for data and information management to empower citizens to manage their own data while maintaining privacy considerations are being developed. Formalising such guidelines is necessary, especially given that access to different forms of data from numerous services allows applications that may have not been considered, and it is paramount that citizens know how to take advantage of these services as well as how their data are being used and how they can control its use.

We briefly demonstrate the challenges using the Connected Vehicle Reference Implementation Architecture (CVRIA) model repository of the US Department of

Transportation (http://local.iteris.com/cvria/) that now includes over 100 complex CV application models with over 8500 data flows, complex mappings to physical objects, organisational entities and communication links. As an example, the top-level dataflow for Electronic Toll payment that carries confidential information between two principles, Driver and the Payment Administrator, while passing through devices, services, communication channels (further decomposed in the model suite) with different security properties. To prevent leakage of sensitive information (such as credit card details), all services, equipment and communication channels involved in the information flow need to have security properties and satisfy privacy policies guaranteed for drivers using electronic toll payment. Similarly to privacy/confidentiality requirements where owners specify reading rights for data in information flows, integrity requirements can be expressed by owners as writing (or modification) rights for information flows. Because these socio-technical systems involve multiple parties, it is important to establish secure collaboration policies based on well-defined models and workflows that can be analysed to determine if the policies comply with the normative requirements and used to enforce secure collaboration [18]. In order to develop and analyse these policies, we must capture the relationships between various parties in the test bed communities and reason about consistency and compliance of the security and privacy policies.

An important research effort is to investigate the formal representation of privacy/confidentiality and integrity policies and their incorporation in system-level synthesis. The key points in this approach are:

(1) Utilise the Myers and Liskov Decentralised Label Model (DLM) [70,71] to introduce security labels for expressing confidentiality/privacy and integrity policies as security types for information flows. Labels identify owners and their restrictions on which other principles can have read or write access to data.

(2) Incorporate DLM into Domain-Specific Modelling Languages (such as the CVRIA modelling languages) as security types over information flows. In DLM, the security type lattice establishes constraints over information flows. We can formally represent all models and security type constraints in FORMULA [72] or the Obligation Specification Language (OSL) [73] with extensions for information flow tracking [74] as formal frameworks. FORMULA is a constraint logic programming tool that represents models as algebraic data type, constraints in first-order logic with fixed point and connected to the Z3 SMT solver to find or complete partial models that satisfy all constraints [75].

(3) Model security properties of services, equipment and communication channels involved as resources in implementing information flows using DLM and use the FORMULA framework to synthesise type-secure mapping of information flows to resources or generate security controls for resources to ensure satisfaction of information flow constraints.

5.4. Policy auditing

Traditionally, safety and security analyses for CPS start by defining the boundaries of the system under analysis. Because most modern H-CPS can be assembled, augmented and modified at runtime by using information technology, this notion of fixed boundaries does not exist any more. This does not lessen the benefits of careful design-time analyses. And yet, as a consequence, we expect pure-embedded, pure business IT and hybrid-combined cyber-physical systems to fail at runtime. Such failures that relate to safety and security but also to privacy must be observed, detected, documented and analysed with respect to likely root causes.

As a complement of the activities that relate to the specification of requirements and their deployment, we hence suggest to incorporate activities that relate to runtime mechanisms that are concerned with failures and cyber-attacks both, and allow analysis both at runtime and post-mortem. The assumption is that because of open interfaces and unknown and potentially ever-changing operation contexts, it is not possible to perform conclusive safety, security and privacy [12] assessments of open and adaptive H-CPS. Instead, potential issues need to be detected, analysed and resolved at runtime. If this is not possible, post-mortem analysis must be supported. This process of (possibly distributed worldwide) learning enables the continuous improvement of products, production facilities and development processes. Certainly not less importantly, it also forms the basis for legal consequences of a systems failures: Understanding what went wrong is a first step towards understanding who is liable.

H-CPS are required to be equipped with data-gathering devices and computational capabilities for data-intensive online or off-line analysis. These functionalities are also focal points for conflicting social expectations and norms. Continuous monitoring to detect anomalies [76] and malicious intruders is a prominent requirement for smart operations, but at the same time, it is a major concern for privacy violations [77]. Legal requirements for monitoring frequently conflict with privacy expectations not only in terms of what kind of data can be collected, but also how the data can be used. Monitoring systems are also primary targets for attackers, who strive to maximise the damage inflicted to the system while remaining covert and not getting detected for an extended duration of time. Due to this exposure, data collection facilities are subject to security policies.

This research direction can be based on a substantial body of results on policy driven monitoring and distributed data usage control where the problem is to enforce policies on the future usage of data in distributed systems. This problem immediately generalises from privacy and security properties to the enforcement of general safety properties in H-CPS, e.g., for the Internet of Things. This existing body of results constitutes the core methodology and technology for accountability [78,79]. Policies for describing requirements on data usage and, more generally, system behaviour (preconditions for contracts) has been studied in [80,81]. The more difficult problem of the enforcement of such policies has, for different infrastructures and various degrees of distribution, been studied also in combination with information flows [79,82]. Previous results are documented specifically for automotive [83] and security policy architectures for smart grids [84].

There are many important questions that need to be addressed. Do we need new legislation that requires logging and analysis mechanisms to be built in? Do we require producers of CPS to continuously analyse logs of system failures and immediately improve their products once the root causes have been detected? How can we perform analyses that make it possible to not only understand root causes but also to assign responsibility and liabilities? Promising research directions in this area include: (1) Understanding and implementation of causality theories for well-defined classes of CPS on the grounds of existing theories by [85,86], (2) The combination of runtime safety and security (and, in a second step, also privacy) analyses into one holistic analysis framework [87,88], and how this impacts design-time analyses, (3) The domain-specific study of trustworthy logs [89,90] and (4) Legal implications and/or prerequisites [91].

6. Conclusions

With the increasingly deeper fusion of the digital world with the world of machines and human society we are in the midst of a profound transformation to society, many aspects of daily life and the global industry. The most visible manifestations of this revolution are the rapid appearance of societal-scale H-CPS, taking the forms of Connected Vehicles, Transactive Energy Systems, commercial applications of Unmanned Air Vehicles, Smart Cities, Smart Health and more. We believe that these systems have such a deep impact on society that their designers cannot and should not expect that they can be developed without deep understanding of the social context within which they are deployed. H-CPS need to become adaptive and contextual.

To accelerate impact, it is necessary to: (1) Understand and compare the nature, scope and evolution of policies and societal expectations in the operation of societal-scale H-CPS. The purpose of the analysis is not to shape social policies, but to determine which factors have the greatest influence on technical solutions. (2) Investigate methods for the explicit and formal representation of societal context (operational, privacy, safety, security policies, incentives, pricing and market policies) that are machine interpretable and impact the structure and behaviour of H-CPS. (3) Develop policy-aware architectures that guarantee the enforcement of policy requirements during the operation of a new generation of H-CPS. The expected outcome of such research is H-CPS architecture specifications that can be 'parameterised' by operational, safety and security policies, and by constraints emerging from societal expectations.

Disclosure statement

No potential conflict of interest was reported by the authors.

Funding

This work was supported in part by the US National Science Foundation (NSF) under the Partnerships for International Research and Education (PIRE) award 1743772 and the Cyber-Physical Systems (CPS) award 1521617 and by the German Science Foundation under Grants DA 206/11-1, FR 2715/4-1, KO 1990/5-1, LE 3131/7-1, LU 1880/2-1, PR 1266/3-1 and RI 1511/2-1.

ORCID

Xenofon Koutsoukos http://orcid.org/0000-0002-0923-6293

References

[1] Manyika J. The internet of things: mapping the value beyond the hype. Orlando (FL): McKinsey Global Institute; 2015.

[2] Annunziata M, Evans PC. Industrial internet: pushing the boundaries of minds and machines. Gen Electr. 2012.

[3] Geisberger E, Broy M. Living in a networked world: integrated research agenda cyber-physical systems. München (Germany): Herbert Utz Verlag; 2015.

[4] Kagermann H, Helbig J, Hellinger A, et al. Recommendations for implementing the strategic initiative industrie 4.0: securing the future of german manufacturing industry; final report of the industrie 4.0 working group. Forschungsunion; 2013.

[5] Cacilo A, Schmidt S, Wittlinger P, et al. Hochautomatisiertes Fahren auf Autobahnen–industriepolitische Schlussfolgerungen. Stuttgart: Fraunhofer-Institut für Arbeitswirtschaft und Organisation IAO; 2015.

[6] Griffor ER, Greer C, Wollman DA, et al. Framework for cyber-physical systems: volume 1, overview. Gaithersburg (MD): National Institute of Standards and Technology (NIST); 2017. (NIST SP)-1500-201.

[7] Lv Z, Song H, Lloret J, et al. IEEE access special section editorial: big data analytics in the internet-of-things and cyber-physical systems. IEEE Access. 2019;7:18070–18075.

[8] Lee EA Cyber physical systems: design challenges. In: 2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC); Orlando (FL): IEEE; 2008. p. 363–369.

[9] Tomlin CJ, Mitchell I, Bayen AM, et al. Computational techniques for the verification of hybrid systems. Proc IEEE. 2003;91(7):986–1001.

[10] Sztipanovits J, Koutsoukos X, Karsai G, et al. Toward a science of cyber–physical system integration. Proc IEEE. 2012;100(1):29–44.

[11] Sztipanovits J, Bapty T, Koutsoukos X, et al. Model and tool integration platforms for cyber-physical system design. Proc IEEE. 2018;99:1–26.

[12] Damm W, Finkbeiner B Automatic compositional synthesis of distributed systems. In: International symposium on formal methods; Singapore: Springer; 2014. p. 179–193.

[13] Amin S, Cárdenas AA, Sastry SS Safe and secure networked control systems under denial-of-service attacks. In: International workshop on hybrid systems: computation and control; San Francisco (CA): Springer; 2009. p. 31–45.

[14] Amin S, Schwartz GA, Sastry SS On the interdependence of reliability and security in networked control systems. In: Decision and control and european control conference (CDC-ECC), 2011 50th IEEE Conference on; Orlando (FL): IEEE; 2011. p. 4078–4083.

[15] Zhang D, Liu L, Feng G. Consensus of heterogeneous linear multiagent systems subject to aperiodic sampled-data and dos attack. IEEE Trans Cybern. 2019 April;49 (4):1501–1511.

[16] Wolf M, Serpanos D. Safety and security in cyber-physical systems and internet-of-things systems. Proc IEEE. 2018;106(1):9–20.

[17] Ratasich D, Khalid F, Geissler F, et al. A roadmap toward the resilient internet of things for cyber-physical systems. IEEE Access. 2019;7:13260–13283.

[18] Koutsoukos X, Karsai G, Laszka A, et al. Sure: amodeling and simulation integration platform for evaluation of secure and resilient cyber–physical systems. Proc IEEE. 2018;106(1):93–112.

[19] Narayanan SN, Khanna K, Panigrahi BK, et al. Security in smart cyber-physical systems: a case study on smart grids and smart cars. In: Rawat DB, Ghagoor KZ, editors. Smart cities cybersecurity and privacy. Elsevier; 2019. p. 147–163.

[20] Müllner N, Fränzle M, Fröschle S. Estimating the probability of a timely traffic-hazard warning via simulation. In: Proceedings of the 48th annual simulation symposium; Society for computer simulation international; Alexandria, VA; 2015. p. 130–137.

[21] Stühring A, Ehmen G, Fröschle S. Building a prototyping platform for investigating the impact of attacks against automotive networks. In: Design, Automation, and Test in Europe (DATE'14); Dresden, Germany; 2014.

[22] Seshia SA, Sadigh D, Sastry SS Formal methods for semi-autonomous driving. In: Proceedings of the 52nd annual design automation conference; San Francisco, CA. ACM; 2015. p. 148.

[23] Robinson RM, Scobee DR, Burden SA, et al. Dynamic inverse models in human-cyber-physical systems. In: Micro-and nanotechnology sensors, systems, and applications VIII. Vol. 9836. International Society for Optics and Photonics; Baltimore, MD; 2016. p. 98361X.

[24] Sadigh D, Sastry S, Seshia SA, et al. Planning for autonomous cars that leverage effects on human actions. In: Robotics: science and systems; Vol. 2; Ann Arbor, MI; 2016. doi:10.15607/RSS.2016.XII.029

[25] Wortelen B, Baumann M, Lüdtke A. Dynamic simulation and prediction of drivers attention distribution. Transp Res Part F Traffic Psychol Behav. 2013;21:278–294.

[26] Yves P, Felix F, Anita F, et al. A comprehensive and harmonized method for assessing the effectiveness of advanced driver assistance systems by virtual simulation: the pears initiative. In: The 24th international technical conference on the enhanced safety of vehicles (ESV); Gothenburg, Sweden; 2015.

[27] Puch S, Wortelen B, Fränzle M, et al. Evaluation of drivers interaction with assistant systems using criticality driven guided simulation. In: Duffy VG, editor. Digital human modeling and applications in health, safety, ergonomics, and risk management. health-care and safety of the environment and transport - 4th international conference, DHM 2013; (Lecture Notes in Computer Science; Vol. 8025); Las Vegas, NV. Springer; 2013. p. 108–117.

[28] Cacciabue C, Riccioli C, Luedtke A, et al. Human modelling in assisted transportation. Milano: Springer; 2014.

[29] Martonosi M. Science, policy, and service. Commun ACM. 2018;61(5):46–48.

[30] Lu N, Cheng N, Zhang N, et al. Connected vehicles: solutions and challenges. IEEE Int Things J. 2014;1(4):289–299.

[31] Shladover SE. Connected and automated vehicle systems: introduction and overview. J Intell Transp Syst. 2018;22(3):190–200.

[32] Möller DP, Haas RE. The connected car. In: Guide to automotive connectivity and cybersecurity. Springer; 2019. p. 171–264.

[33] Contreras-Castillo J, Zeadally S, Guerrero-Ibañez JA. Internet of vehicles: architecture, protocols, and security. IEEE Int Things J. 2018;5(5):3701–3709.

[34] Taiebat M, Brown AL, Safford HR, et al. A review on energy, environmental, and sustainability implications of connected and automated vehicles. Environ Sci Technol. 2018;52(20):11449–11465.

[35] Bonnefon JF, Shariff A, Rahwan I. The social dilemma of autonomous vehicles. Science. 2016;352(6293):1573–1576.

[36] Santacana E, Rackliffe G, Tang L, et al. Getting smart. IEEE Power Energy Mag. 2010;8 (2):41–48.

[37] Council GA. Gridwise transactive energy framework: version 1.0. Pacific northwest national laboratory, PNNL-22946 Ver1 0. 2015.

[38] Masera M, Bompard EF, Profumo F, et al. Smart (electricity) grids for smart cities: assessing roles and societal impacts. Proc IEEE. 2018;106(4):613–625.

[39] McKenna E, Richardson I, Thomson M. Smart meter data: balancing consumer privacy concerns with legitimate applications. Energy Policy. 2012;41:807–814.

[40] Hess DJ. Smart meters and public acceptance: comparative analysis and governance implications. Health Risk Soc. 2014;16(3):243–258.

[41] Finn RL, Wright D. Unmanned aircraft systems: surveillance, ethics and privacy in civil applications. Comput Law Secur Rev. 2012;28(2):184–194.

[42] Floreano D, Wood RJ. Science, technology and the future of small autonomous drones. Nature. 2015;521(7553):460.

[43] Rao B, Gopi AG, Maione R. The societal impact of commercial drones. Technol Soc. 2016;45:83–90.

[44] Chen M, Hu Q, Mackin C, et al. Safe platooning of unmanned aerial vehicles via reachability. In: Decision and control (CDC), 2015 IEEE 54th annual conference on; Osaka, Japan. IEEE; 2015. p. 4695–4701.

[45] Williams SR. Communication in mechanism design: adifferential approach. Cambridge: Cambridge University Press; 2008.

[46] Dong R, Krichene W, Bayen AM, et al. Differential privacy of populations in routing games. In: Decision and control (CDC), 2015 IEEE 54th annual conference on; Osaka, Japan. IEEE; 2015. p. 2798–2803.

[47] Canepa ES, Claudel CG Spoofing cyber attack detection in probe-based traffic monitoring systems using mixed integer linear programming. In: Computing, networking and communications (ICNC), 2013 international conference on; San Diego, CA. IEEE; 2013. p. 327–333.

[48] Ratliff LJ Incentivizing efficiency in societal-scale cyber-physical systems [dissertation]. UC Berkeley; 2015.

[49] Ratliff LJ, Burden SA, Sastry SS. On the characterization of local Nash equilibria in continuous games. IEEE Trans Autom Control. 2016;61(8):2301–2307.

[50] Kahneman D. A perspective on judgment and choice: mapping bounded rationality. Am Psychologist. 2003;58(9):697.

[51] Kahneman D. Prospect theory: an analysis of decisions under risk. Econometrica. 1979;47:278.

[52] Balandat M, Oldewurtel F, Chen M, et al. Contract design for frequency regulation by aggregations of commercial buildings. In: Communication, control, and computing (allerton), 2014 52nd annual allerton conference on; Allerton, IL. IEEE; 2014. p. 38–45.

[53] Balandat M, Tomlin CJ On efficiency in mean field differential games. In: 2013 American control conference; Washington, DC. IEEE; 2013. p. 2527–2532.

[54] Fränzle M, Teige T, Eggers A. Engineering constraint solvers for automatic analysis of probabilistic hybrid automata. J Log Algebra Program. 2010;79(7):436–466.

[55] Teige T, Fränzle M. Generalized Craig interpolation for stochastic boolean satisfiability problems with applications to probabilistic state reachability and region stability. Logical Methods Comput Sci. 2012;8(2).

[56] Gao Y, Fränzle M A solving procedure for stochastic satisfiability modulo theories with continuous domain. In: Campos J, Haverkort BR, editors. Quantitative evaluation of systems, 12th international conference, QEST 2015; (Lecture Notes in Computer Science; Vol. 9259); Madrid, Spain. Springer; 2015. p. 295–311.

[57] Damm W, Peter HJ, Rakow J, et al. Can we build it: formal synthesis of control strategies for cooperative driver assistance systems. Math Struct Comput Sci. 2013;23(4):676–725.

[58] Fränzle M, Hermanns H, Teige T Stochastic satisfiability modulo theory: A novel technique for the analysis of probabilistic hybrid systems. In: Egerstedt M, Mishra B, editors. Hybrid systems: computation and control, 11th international workshop, HSCC 2008; (Lecture Notes in Computer Science; Vol. 4981); St. Louis, MO. Springer; 2008. p. 172–186.

[59] Fränzle M, Teige T, Eggers A Satisfaction meets expectations - computing expected values of probabilistic hybrid systems with SMT. In: Méry D, Merz S, editors. Integrated formal methods - 8th international conference, IFM 2010; (Lecture Notes in Computer Science; Vol. 6396); Nancy, France. Springer; 2010. p. 168–182.

[60] Fränzle M, Gerwinn S, Kröger P, et al. Multi-objective parameter synthesis in probabilistic hybrid systems. In: Sankaranarayanan S, Vicario Eeditors. Formal modeling and analysis of timed systems - 13th international conference, FORMATS 2015; (Lecture Notes in Computer Science; Vol. 9268); Madrid, Spain. Springer; 2015. p. 93–107.

[61] Fränzle M, Shirmohammadi M, Swaminathan M, et al. Costs and rewards in priced timed automata. In: Chatzigiannakis I, Kaklamanis C, Marx D, et al., editors. 45th International colloquium on automata, languages, and programming, ICALP 2018; (LIPIcs; Vol. 107). Schloss Dagstuhl - Leibniz-Zentrum für Informatik; Prague, Czech Republic; 2018. p. 125: 1–125:14.

[62] Damm W, Vincentelli AS A conceptual model of system of systems. In: Proceedings of the second international workshop on the swarm at the edge of the cloud; Seattle, WA. ACM; 2015. p. 19–27.

[63] Friedrichs T, Lüdtke A Modeling situation awareness: the impact of ecological interface design on drivers response times. In: COGNITIVE 2015: The seventh international conference on advanced cognitive technologies and applications; Nice, France; 2015.

[64] Hollmann M, Rieger JW, Baecke S, et al. Predicting decisions in human social interactions using real-time fmri and pattern classification. PLoS One. 2011;6(10):e25304.

[65] Wortelen B, Unni A, Rieger JW, et al. Towards the integration and evaluation of online workload measures in a cognitive architecture. In: Cognitive Infocommunications (CogInfoCom), 2016 7th IEEE international conference on; Wroclaw, Poland. IEEE; 2016. p. 000011–000016.

[66] Van Ditmarsch H, Labuschagne W. My beliefs about your beliefs: a case study in theory of mind and epistemic logic. Synthese. 2007;155(2):191–209.

[67] Damm W, Finkbeiner B, Rakow A What you really need to know about your neighbor. In: Proceedings at 5th Workshop on Synthesis (SYNT 2016); Toronto, Canada; 2016.

[68] Damm W, Finkbeiner B Does it pay to extend the perimeter of a world model? In: International symposium on formal methods; Limerick, Ireland. Springer; 2011. p. 12–26.

[69] Sangiovanni-Vincentelli A, Damm W, Passerone R. Taming dr. Frankenstein: contract-based design for cyber-physical systems. Eur J Control. 2012;18(3):217–238.

[70] Myers AC, Liskov B. Protecting privacy using the decentralized label model. ACM Trans Software Eng Methodol. 2000;9(4):410–442.

[71] Myers AC, Liskov B. A decentralized model for information flow control. In: Waite WM, editor. Proceedings of the sixteenth ACM symposium on Operating systems principles (SOSP '97). Vol. 31. New York (NY): ACM; 1997. p. 129–142.

[72] Jackson E, Sztipanovits J. Formalizing the structural semantics of domain-specific modeling languages. Software Syst Model. 2009;8(4):451–478.

[73] Hilty M, Pretschner A, Basin D, et al. A policy language for distributed usage control. In: European symposium on research in computer security; Dresden, Germany. Springer; 2007. p. 531–546.

[74] Pretschner A, Lovat E, Büchler M. Representation-independent data usage control. In: Garcia-Alfaro J, Navarro-Arribas G, Cuppens-Boulahia N, de Capitani di Vimercati S, editors. Data privacy management and autonomous spontaneus security. DPM 2011, SETOP 2011. Lecture Notes in Computer Science, vol 7122. Berlin: Springer; 2012. p. 122–140.

[75] Jackson EK, Schulte W, Bjørner N Detecting specification errors in declarative languages with constraints. In: International conference on model driven engineering languages and systems; Innsbruck, Austria. Springer; 2012. p. 399–414.

[76] Chandola V, Banerjee A, Kumar V. Anomaly detection: a survey. ACM Comput Surveys. 2009;41(3):15.

[77] Hilty M, Pretschner A, Basin D, et al. Monitors for usage control. In: IFIP international conference on trust management; New Brunswick, NB. Springer; 2007. p. 411–414.

[78] Kumari P, Pretschner A Model-based usage control policy derivation. In: International symposium on engineering secure software and systems; Paris, France. Springer; 2013. p. 58–74.

[79] Kelbert F, Pretschner A Data usage control enforcement in distributed systems. In: Proceedings of the third ACM conference on data and application security and privacy; San Antonio, TX. ACM; 2013. p. 71–82.

[80] Kumari P, Pretschner A Deriving implementation-level policies for usage control enforcement. In: Proceedings of the second ACM conference on data and application security and privacy; San Antonio, TX. ACM; 2012. p. 83–94.

[81] Kumari P, Kelbert F, Pretschner A. Data protection in heterogeneous distributed systems: a smart meter example. In: Heiß H-U, Pepper P, Schlingloff H, Schneider J, editors. INFORMATIK 2011 – Informatik schafft Communities. Bonn: Gesellschaft für Informatik e.V.; 2011.

[82] Kelbert F, Pretschner A A fully decentralized data usage control enforcement infrastructure. In: International conference on applied cryptography and network security; New York, NY. Springer; 2015. p. 409–430.

[83] Broy M, Pretschner A, Salzmann C, et al. Software-intensive systems in the automotive domain: challenges for research and education. SAE Technical Paper; 2006.

[84] Fromm A, Kelbert F, Pretschner A Data protection in a cloud-enabled smart grid. In: International workshop on smart grid security; Berlin, Germany. Springer; 2012. p. 96–107.

[85] Halpern JY. Actual causality. Cambridge (MA): MiT Press; 2016.

[86] Gössler G, Le Métayer D A general trace-based framework of logical causality. In: International Workshop on Formal Aspects of Component Software; Nanchang, China. Springer; 2013. p. 157–173.

[87] Kacianka S, Kelbert F, Pretschner A Towards a unified model of accountability infrastructures. In: Proceedings of causal reasoning for embedded and safety-critical systems technologies (CREST@ETAPS); Eindhoven, The Netherlands. 2016. p. 40–54.

[88] Beckers K, Landthaler J, Matthes F, et al. Data accountability in socio-technical systems. In: Schmidt R, Guédria W, Bider I, Guerreiro S, editors. Enterprise, business-process and information systems modeling. BPMDS 2016, EMMSAD 2016. Lecture Notes in Business Information Processing, vol. 248. Cham: Springer; 2016. p. 335–348.

[89] Banescu S, Ahmadvand M, Pretschner A, et al. Detecting patching of executables without system calls. In: Proceedings of the seventh ACM on conference on data and application security and privacy; Scottsdale, AZ. ACM; 2017. p. 185–196.

[90] Banescu S, Pretschner A, Battré D, et al. Software-based protection against changeware. In: Proceedings of the 5th ACM conference on data and application security and privacy; San Antonio, TX. ACM; 2015. p. 231–242.

[91] Bertolini A. Robots as products: the case for a realistic analysis of robotic applications and liability rules. Law Innovation Technol. 2013;5(2):214–247.