Capturing Autonomy in its Multiple Facets: A Digital Twin Approach

Richard Heininger

Johannes Kepler University Linz
Institute of Business Informatics
Linz, Austria
richard.heininger@jku.at

Chris Stary

Johannes Kepler University Linz
Institute of Business Informatics
Linz, Austria
christian.stary@jku.at

ABSTRACT

Autonomy has been touted to be a major asset of Cyber-Physical Systems (CPS) and its components. By intertwining non-physical and physical processes they seamlessly integrate interdependent computational and physical components. In this contribution we take a closer look on structural constellations of CPS and their components that refer to autonomy. We also take into account development aspects and demonstrate encoding autonomy aspects into a behavior-centered representation scheme for digital twins. It features encapsulation on various layers of abstraction in the course of design and choreography for self-contained while networked operation of CPS as System-of-Systems. As digital twin models created in the course of CPS design activities can be executed automatically, the implementation and adaptation of CPS (components) is intertwined with design activities. Consequently, users can act as designers and experience CPS behavior through digital twin execution interactively. Critical elements, such as managing private data in healthcare, can be monitored and adapted to individual needs.

CCS CONCEPTS

• **General and reference** → Design; • **Computer systems organization** → Embedded and cyber-physical systems; • **Information systems**; • **Security and privacy** → Usability in security and privacy;

KEYWORDS

autonomy; digital twin; socio-technical systems design; subject-orientation; cyber-physical systems

ACM Reference Format:

Richard Heininger and Chris Stary. 2021. Capturing Autonomy in its Multiple Facets: A Digital Twin Approach. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-physical Systems (SAT-CPS '21)*, April 28, 2021, Virtual Event, USA. ACM, New York, NY, USA, 10 pages. <https://doi.org/10.1145/3445969.3450422>

This work is licensed under a Creative Commons Attribution International 4.0 License.

SAT-CPS '21, April 28, 2021, Virtual Event, USA
© 2021 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8319-6/21/04.
<https://doi.org/10.1145/3445969.3450422>

1 INTRODUCTION

Embedded systems, named as Cyber-Physical Systems (CPS) gained attention for supporting the organization and coordination of networking systems between its physical infrastructure and computational capabilities [32]. The operation of CPS should be based on decentralized action while various physical and digital components are coordinated to achieve a common goal. Processing and exchanging data targets computational intelligence to monitor, utilize and control the physical infrastructure through its digital services. Intelligence should include decision-making and reasoning to better achieve production and business results (see also Fig. 1).

Figure 1: Basic capabilities of CPS according to [9]

“CPS are engineered systems that are built from, and depend upon, the seamless integration of computation and physical components. Advances in CPS will enable capability, adaptability, scalability, resiliency, safety, security, and usability that will expand the horizons of these critical systems. CPS technologies are transforming the way people interact with engineered systems, just as the Internet has transformed the way people interact with information. New, smart CPS drive innovation and competition in a range of application domains including agriculture, aeronautics, building design, civil infrastructure, energy, environmental quality, healthcare and personalized medicine, manufacturing, and transportation. CPS are becoming data-rich enabling new and higher degrees of automation and autonomy. Traditional ideas in CPS research are being challenged by new concepts emerging from artificial intelligence and machine learning. The integration of artificial intelligence with CPS especially for real-time operation creates new research opportunities with major societal implications” [27].

We deal with CPS such as a smart phone every day. A Cyber-Physical System then needs to be considered as a socio-technical system intertwining non-physical and physical processes [3]. It consists of seamlessly integrated and interdependent computational

and physical components [27]. Home automation systems, medical monitoring, and industrial control systems are well-known application domains of CPS [22].

The mentioned fields of application indicate the diversity of possible uses of CPS. CPS design must consider this diversity [27]. Furthermore, the design must take into account that CPS can be dynamically changed during its operation. This requires proper specification and development methods and tools. All (digital, mechanical, physical) processes can be managed in an integrated way through model-based behavior specifications termed digital twins. Therefore, digital twins are an executable behavior model of a CPS based on specifications of each component and its exchange of data with other CPS components [5].

The individual system components can change at run time as long as the flow of interaction is maintained. It is part of the specification for the digital twin, which encapsulates the behavior of the components as a basis for design, control and simulation: The vision of the digital twin itself refers to a comprehensive physical and functional description of a component, product or system that contains more or less all information that could be useful in all phases of the current and subsequent life cycle [5].

Of particular importance for CPS development is the variety of applications of CPS which leads to their heterogeneous composition. This high heterogeneity results from the many different autonomously operating components that make up a CPS, depending on the tasks and application. Hence, the design of CPS, and finally, run time has to allow diversity and master heterogeneity in terms of mutually adjusted components. What are the consequences for autonomy, both in terms of architecture and behavior? Becoming aware of conflicts stemming from integrating heterogeneous components keeping their ‘self-containedness’, we want to take a closer look to the autonomy of CPS.

Rather than aiming to determining ‘the optimal level of autonomy’ [16] we aim to highlight various facets of autonomy and how to deal with them when design is integrated with engineering. Engineering considers all activities putting a CPS design to operation and supporting it at run time. Design and engineering activities operate on a digital twins of a CPS. It should contain all physical and functional items that are required for all phases of a CPS life cycle and encapsulates the behavior of the components as a basis for design, control and execution (see also above and [5]).

In section 2 we give an overview of related work starting with the nature of CPS design and current approaches to CPS design and autonomy of CPS (components). We then review the concept of digital twins and their use in CPS design. In section 3, we present a case to demonstrate the different constellations related to autonomy. Stemming from healthcare, it includes critical design issues, such as privacy and security. In section 4, digital twins are introduced as enablers for changing requirements, in particular affecting various CPS components. Subject-oriented modeling of digital twins is then introduced in section 5 as a formally justified representation approach to implement CPS.

Subsequently, autonomy is recognized as a driver of change in CPS development, which is discussed in Section 6 using the case introduced earlier. Digital twin models serve as carrier for existing implementation and further design the same time. Section 7 structures the findings and discusses current approaches to

the design and engineering of digital twins in terms of autonomy specification and socio-technical system development. The latter is of utmost importance when handling heterogeneous components with a unifying modeling approach and implementing overarching requirements, such as individualized privacy management. The digital twin models provide the proof-of-concept, as they can be executed after validation. Section 8 concludes the paper with a discussion on the potential of this approach and further research directions.

2 RELATED WORK

In this section we review the requirements for CPS design techniques and the current approach to design, before detailing the concept of digital twins and their relation to CPS design (processes).

2.1 CPS Design

CPS design involves a variety of disciplines, leading to contributions of various teams of engineers with diverse backgrounds [10]. Many system properties influence the design in more than one discipline, while the lack of clearly defined interfaces between disciplines is likely to hinder collaboration of the involved developers [10].

According to Hehenberger et al.’s survey study [17], CPS-design requires high-level integrated design methods. They should enable designers to take into account all involved engineering disciplines simultaneously (see also Fig. 2). Thereby, conceptual design and system modelling are start activities. They lay ground for the structure and operation of finally developed CPS. The CPS design process requires to focus on (i) physical components, (ii) digital ones, and (iii) on their integration. Physical components are those CPS parts that are present in the physical world. According to their capabilities they recognize events and can set actions physically. Digital components represent all computation-relevant CPS parts. Design is finally about integrating these components in a way that the required CPS functionality can be accomplished through their interplay in a socio-technical system.

From existing case studies Hehenberger et al. concluded that CPS designers directly start working on functional and architecture issues, rather than developing a conceptual model [17]. However, “three main challenges exist in the conceptual design phase as follows: Firstly, how to generate solution concepts based on customer requirements or market survey results? ...the process from requirements specification to solution concepts should be defined. Different solution concepts can be proposed by individual designers, or design groups, according to their background knowledge and professional experience. Secondly, how to evaluate the different solution concepts proposed. Finally, because of the complexity of a CPS, it is impossible to find the optimum solution concepts without iteration and there is a requirement to optimise solution concepts during the early part of the design process” [17, p. 277]. They also conclude from existing work that modeling languages should allow for dynamically modeling architectures with specific reference to CPS. CPS design should lead to a CPS representation “as an assembly of components and the associated interfaces between them”, that allow “to model to determine the important functional and system parameters and hence realise the potential optimization” [17].

Figure 2: Disciplinary integration during early design process of CPS (taken from [17])

The latter, however, also includes human-centered requirements, e.g., stemming from identity, security or privacy management [2].

Latest research claim [18], in order to improve enterprise performance including quality of operation, “currently it is neither feasible nor reasonable to equip any machine with full autonomy when networking with other machines or people. It is necessary to specify rules for machine behavior that also determine an adequate degree of autonomy to realize the potential benefits of the IoT. Yet, there is a lack of methodologies and guidelines to support the design and implementation of machines as explicit autonomous agents such that many designs only consider autonomy implicitly” [18].

Khaitan et al. refer to a CPS as “System-of-Systems”, as autonomous components can run in a federated way, on the one hand as isolated component, and on the other hand, controlled by others through interactions. In the latter case, heterogeneous component can be coordinated for complex system design. Such an understanding should help throughout design to model domain specific, continuous interaction and adaptation according to changing configurations. Their list of modeling techniques and programming tools for designing CPS include formal semantics approaches and architecture styles, such as (multi-)agent and event-based semantic models. For capturing heterogeneity a mixtures of models of computation are advised, whereas the concurrent and dynamic nature seems to favor actor- or agent-based design. Since simulation is a major concern, the automated execution of models is of benefit [20].

Merlo et al. have addressed design engineering methods that integrate the user/consumer into design processes and affect modeling. The proposed integrated approach contains the ordered phases ‘exploration’ as divergent top-down design, ‘synthesis’ as selection and unit tests, and ‘development’ as convergent bottom-up design. This system’s engineering approach recognizes the role ‘customer’ managing the CPS, and ‘user’. Since there are distinct types of users

the user-centered approach ensures their specific requirements for design [25].

Figure 3: CPS Design according to [25]

2.2 Digital Twin Representations for Design

We follow the recently consolidated conceptualization of digital twins proposed by Wagner et al. It reflects the nature of CPS, as a digital twin consists of respective parts physical and digital product, and “connected data that tie and indissolubly connect the physical and virtual product”. It is considered an integrated simulation for optimizing a CPS while mirroring the lifecycle of its actual system pendant. Mirroring means to fully capture the potential or actual physical manufactured product from its micro or atomic level to the macro level through models. Beyond referring to the product a digital twin can contain a production system itself [36].

However, digital twins are mainly used in the product design stages to gain quantitative data for efficient and optimal product generation – see also value chain for product life cycles in Fig. 4. Digital twins increasingly contain digital production information, so that production systems can be simulated. Besides manufacturing steps (machine) tools, and process parameters are handled in the course of optimization. Linking product and production twins into digital production twins affects product engineering process, even addressing human control and interaction issues. Wagner et al. envision enriched use of digital twins along product engineering to ensure coherent and efficient flow of information. They also recognize the lack of a consistent framework for holistic application scenarios, particularly addressing the integration of product designers’ work and production planner concepts [36].

The latter has already been addressed recently by Papacharalamopoulos et al. They propose to study what-if scenarios through experimenting with varying process parameters. They are handled by real time digital twins, thus requiring executable models representing relevant design parameters. “The implementation of a digital twin of a manufacturing process in a real production line should take into consideration, besides the actual development of the consisting model, its validation in terms of very specific concepts and functionalities” [29, p. 111]. Since real-time estimation

Figure 4: Development context of digital twins, according to [36]. Space Shuttle images kindly taken from <https://pixy.org/4621350/> and <https://pixy.org/5946424/>

distinguishes a physics model of a product from a digital twin, a digital twin facility should have additional capabilities for real-time decision making. In the course of optimization, human interventions when experimenting with different designs become transparent and traceable [29].

Consequently, a digital twin becomes a virtual instance of a physical system (twin) that is not only continually updated with the latter's operation data on performance and status throughout the entire physical system's life cycle, but could control the system's behavior [23]. The models representing the digital twin could address CPS from different perspectives and on different layers, based on networked micro and macro elements.

Figure 5: The relationship between digital twin, CPS and IoT according to [24]. Icons kindly taken from <https://www.svgrepo.com>

A CPS is finally characterized by a physical asset and its digital twin [24] – see also Fig. 5. “In contrast, a digital twin is limited to the digital model, not the twinning physical asset, though a digital twin cannot live without its twinning asset in the physical space. In other words, digital twin represents the prerequisite for the development of a CPS” [24, p. 2]. As such, it can serve as an accurate representation of the CPS design process.

3 AUTONOMY CONSTELLATIONS

In this section we first present our scenario to exemplify the various constellations of autonomy that are introduced subsequently. It addresses a case in home health care (HHC) comprising a CPS. HHC includes a wide range of services provided at home of patients, networked with health care professionals [21].

Our basic scenario is shown in Fig. 6. We are dealing with a blood glucose meter (BGM), a heart rate monitor (HRM), a stress monitoring device (SMD) and a home health care information system (IS), all located in the same HHC environment. All devices are CPS and the IS is provided on site. The relationship of the devices to the IS is hierarchical. All sensor data is sent to the IS. It is the central coordinating point for all activities and contains the entire operational logic, which consists of rules of conduct. The latter could be, e.g., the triggering of an emergency call if the heart rate of the monitored patient falls below a certain threshold, or when the combination of two or more monitored values indicates an emergency situation and action needs to be taken.

Figure 6: Home Health Care environment

All sensor devices are connected to WiFi and have a communication interface. This enables them to communicate with the IS, whereby both the devices and the IS can initiate communication. However, the devices are not designed to communicate with each other.

CONSTELLATION 1: OPERATIONAL COMPONENT AUTONOMY.

CPS are designed in a way that operation has to be coordinated by a control component.

The basic scenario represents the autonomy constellation 1: The CPS involved are designed in such a way that they can provide data on demand and fulfill their purpose when connected to WiFi. When they are disconnected from the network, they continue to monitor data, but no action is taken because the operating logic is interrupted. From the point of view of the patients monitored, the HHC is not autonomous at all at run time because the purpose - which is ultimately to call for help in an emergency - cannot be fulfilled.

The HHC environment can adapt over time. All devices are CPS and can assume the role of IS. Therefore, we can imagine that the operational logic is applied at the device level and completely removed from the IS. The IS would then no longer be needed, or it would take on a different role, such as visualizing the data. Fig. 7 represents the customized HHC environment. All devices in the

scenario are now connected to each other because their roles have changed. They may therefore need to communicate with each other to implement all previous and new or novel rules.

Figure 7: Adapted Home Health Care environment

CONSTELLATION 2: FEDERATED SYSTEMS AUTONOMY.

CPS are designed in a way that operational autonomy of components remains while operating as a network node.

We can define the autonomy constellation 2 based on the adapted HHC scenario. The CPS devices are designed to communicate with each other, including the IS, though its role has changed. The status of network connectivity does not reduce the functionality of the devices. However, only interactions known at design time can be implemented within the devices. Thus, if a device or system unknown to a particular CPS requests data from that same CPS, that CPS can only respond as implemented at design time. From the perspective of the monitored patient, the HHC environment is again perceived as a closed system, unlike a network of autonomous devices.

At some point in our scenario, the doctors are granted access to the HHC environment, as shown in Fig. 8. The IS has been removed, and the data is now stored in a special cloud-based health information system (CIS). This transformation of the scenario not only implies a change in the behavior of the devices, but also means that suddenly other dimensions, such as the privacy of patients, are of crucial importance.

Figure 8: Doctor's access to Home Health Care environment

CONSTELLATION 3: AUTONOMY ADAPTATION.

CPS are designed in a way that their operation can be extended.

The autonomy constellation 3 can be derived from the HHC environment shown in Fig. 8. The HHC environment is connected to systems outside the site where it is operated. Therefore, other parties involved, such as physicians and doctors, can retrieve the data of the monitored patient. Although the CPS devices have an interface to send data to other, potentially unknown systems, the behavior of the devices is still hard coded. If, for example, a monitored patient wants to stop sharing his or her health data for privacy reasons, he or she cannot change the implemented behavior. The patient must hope that a configuration option was planned at design time and implemented during the development of the CPS.

Fig. 9 outlines another necessity in the HHC environment of our scenario. The devices need to be maintained regularly. Therefore the CPS software and hardware must be checked on site with again different interfaces.

Figure 9: Maintenance is a necessity in the Home Health Care environment

CONSTELLATION 4: UPDATE/UPGRADE AUTONOMY.

CPS components can be updated dynamically.

CPS manufacturers can decide at design time whether to provide future upgrades to the CPS. Upgrades could be, for example, additional functionality or simply troubleshooting. This can be identified as autonomy constellation 4, as shown in Fig. 9. From the perspective of the monitored patients, the devices of the HHC environment will appear as autonomous as the respective manufacturer allows.

CONSTELLATION 5: IMPLEMENTATION AUTONOMY.

Validation of CPS specification can be performed at design time, while actors and systems can be assigned to components dynamically at run time.

Validation of CPS specification enables developers and operation staff to check semantic correctness, i.e. evaluation whether any implementation of the specified behavior meets the required behavior. Once this kind of validity has been checked, either humans, physical or digital CPS entities can be assigned to each component for final operation.

4 DIGITAL TWINS AS ENABLERS FOR HANDLING AUTONOMY

The scenario described in Section 3 contains several adjustments and changes. We introduce digital twins as enablers. Fig. 10 shows the transformation of the initial state of our scenario from Fig. 6 to

the second state from Fig. 7. The red arrows mark the bidirectional connection between the physical devices and their respective digital twin. In the scenario, the changes are implemented on the side of the digital twin and mirrored by its physical counterpart. The new role of the IS has to be configured manually as there is no support from digital twins in this respect.

Figure 10: HHC environment transformation

In the following we refer to the mirroring character of digital twins as introduced originally in [28]: “An integrated multi-physics, multi-scale, probabilistic simulation of a vehicle or system that uses the best available physical models, sensor updates, fleet history, etc., to mirror the life of its flying twin. The digital twin is ultra-realistic and may consider one or more important and interdependent vehicle systems.” However, we enrich the focus on the object itself with the simulation of the CPS to demonstrate its run time and moving beyond production context, as proposed by [30]. The concept of the digital twin according to three categories enables stakeholders to take different roles and thus to generate greatest possible benefits:

Virtual Twin: A virtual representation is created using a physical asset (in the cloud).

Predictive Twin: Physical, data or hybrid models based on a virtual twin to predict the behavior of a physical asset

Twin projection: In order to gain insights into the underlying operations and processes, the insights gained by the predictive twin are evaluated.

When utilizing IoT devices for improved monitoring they can be conceptualized as nodes of a CPS, with digital twins as behavior models. For handling the latter we use subject-oriented modeling and execution capabilities [13, 14], considering CPS as a network of interacting subjects. Subjects are defined as behavior encapsulations describing the generation of value. They address tasks, machine operations, organizational units, or roles people have in business which generate value. From an operational perspective, subjects operate in parallel and can exchange messages asynchronously or synchronously. Consequently, business or CPS transactions forming value streams can be interpreted as the exchange of messages between subjects.

5 SUBJECT-ORIENTED REPRESENTATION FOR EXECUTION

CPS specified in subject-oriented models, and thus digital twins operate as autonomous, concurrent behavior entities representing distributed elements. Every entity (subject) is capable of performing (local) actions that do not involve interacting with other subjects, e.g., calculating a threshold value of blood pressure for a measurement device. Subjects can also perform communicative actions dealing with the transmission of messages to other subjects, namely sending and receiving messages. Subjects are specified in two separate types of diagrams: Subject Interaction Diagrams (SIDs) and Subject Behavior Diagrams (SBDs).

Figure 11: Subject Interaction Diagram for an ordering process

The SID provides an integrated view of CPS, comprising the subjects involved (rectangles) and the messages (directed links) they exchange. Fig. 11 shows a simple example of a SID. The subject named *Purchaser* initiates an ordering process by sending a message named *Order Request* to the subject named *Approver*. The latter responds with either an *Approval* or *Rejection* message.

Figure 12: Subject Behavior Diagram for subject *Approver*

Subject Behavior Diagrams (SBDs) provide a local view of the process from the perspective of individual subjects. They include

sequences of states representing local actions (called ‘functions’) and communicative actions including sending and receiving messages as specified in the SBD. State transitions are represented using arrows, with labels indicating the outcome of the preceding state. Fig. 12 provides a very simple example of a SBD. It contains a sequence of states, starting with a receive state (green), followed by a function state (yellow), which then splits into two branches, each with a send state (red), each finally ending in a function state. Basically, receive states wait for messages, send states initiate the sending of messages, and function states represent the actual doing. In Fig. 12, the subject *Approver* waits for an *Order Request*, then makes a decision on the request and sends the decision back, finally arriving at a final state.

Figure 13: Executed Subject of *Approver* in run time environment of Metasonic Suite www.metasonic.de

Subjects can be executed by human or computer actors [12, 19], the latter including CPS. The well-defined semantics of S-BPM models (based on Abstract State Machines [4]) enables automated translation into executable code, including PLC code represented with IEC 61131-3 [26]. For example, for the simple ordering process illustrated in Fig. 11 and Fig. 12, Fig. 13 shows a representation for execution for users of a workflow system, which was automatically generated from the modeled behavior. Thus, behavioral changes of the digital twin can be automatically translated and executed by the physical twin.

6 AUTONOMY AS DRIVER FOR CHANGE IN THE HOME HEALTH CARE SCENARIO

In Section 3, we defined five constellations of autonomy based on a home health care scenario. Our results shed light on the fact that autonomy can be considered from different perspectives and can change over time, not only during the run time of a CPS, but also during the design time of a CPS.

Since our ultimate goal is to support the design of socio-technical systems with autonomy in mind, we want to show the respective capabilities of our approach. To this end, we have introduced digital twins as enablers and subject-oriented representation as a modeling approach. Fig. 14 illustrates the transformation scenario shown in Fig. 10. It consists of two SIDs, in the upper part of the figure the initial situation of the HHC system, and in the lower part the transformed HHC system. On the model level, we can thus already

Figure 14: Subject Interaction Diagrams for transformation scenario shown in Fig. 10

capture and implement changing requirements for the autonomy of CPS.

At the run time level, we refer to the capabilities of S-BPM in terms of execution. Thus, behavioral changes of digital twins can be directly translated into machine-executable code and executed on the physical twin, i.e., a CPS. However, the changed behavior may not meet the autonomy requirements or may not function properly. It is therefore imperative to validate the changes before transferring the behavior to the physical twin. Fig. 15 shows this process in relation to the outlined models on the right side of Fig. 10. The process step of testing including autonomy requirements is displayed between the two models, with respect to the actual situation and the target situation of the digital twins. It is sketched as a funnel to indicate the quality improvement of the models that go through this process step. We assume that there will be a larger number of models to be reviewed than models that are actually applied to the physical twin. This allows stakeholders to digitally review the autonomy requirements at design time without applying them to

Figure 15: Checking autonomy and implementing behavioral changes (two-step-process of transformation displayed in Fig. 10)

the physical twin. The validated, modified behavior is implemented at the CPS level in the second step and thus applied to the physical twin. As stakeholders can participate in the development process, autonomy of CPS becomes part of socio-technical design issues.

Figure 16: Implementing privacy management as example for enabling privacy-by-design in a System-of-Systems

A typical example of such a design issue concerns privacy management. Following the (de)centralized identity management architecture discussed in [1], privacy management can be designed on the level of digital twin models. Thereby, users and designers

need to be supported in their efforts to select, provide, and use the required trustworthy digital services through explicit data localization and transfer control [6]. Using subject-oriented twin representations, privacy management can be implemented through (i) privacy-relevant data matching of CPS components, (ii) matching user requirements with provided privacy data, and (iii) execution of privacy requirements, e.g., specified in a dedicated privacy management component (i.e. subject). In line with privacy-by-design principles it enables control which and how data are shared. For instance, health service providers receive only personal information they need for administrative procedures and requested treatments from patients (data minimization). Attribute-based credentials allow users to disclose only a subset of their personal properties such as age, and citizenship [7, 8]. As shown in Fig. 16, explicit consent mechanisms prior to data usage can be implemented to enforce privacy requirements.

Once dedicated communication links between CPS components are established with respect to privacy management CPS adaptation during run time is enabled for upcoming extensions and further use. Fig. 16 shows the respective request - permission-response pairs for privacy-critical components. The System-of-Systems approach not only structures the access to privacy-critical CPS components, but also to adapt it according to individual privacy needs of users (cf. [34, 35]). Thus, a self-referent alignment of the provided services can be instantiated based on privacy-relevant message flows. A cumulative privacy knowledge base storing privacy management data can be used for statistical disclosure control methods and disclosure risk assessment to preserve user privacy on the collected data [11].

Explicit privacy management capabilities in terms of System-of-Systems as shown above go beyond most existing tools, such as SAI Global Risk (www.saiglobal.com) or Onetrust (www.onetrust.com), as they focus on data compliance or user requests rather than complex system (re-)design. For instance, when aiming to achieve and maintain compliance with GDPR, and other privacy laws and regulations, users managing privacy data need support of system developers on data access, portability, or deletion. Although some tools leverage reporting to manage privacy needs via a centralized dashboard, there is no behavior modeling related to the business logic of a CPS component. The presented subject-oriented digital twin approach features digital behavior representation of each CPS component as well as dedicated privacy management components. They can be adapted during run time due to the unifying modeling approach and the automated execution of digital twin models. Key thereby is the data-driven message passing between CPS components.

7 STRUCTURING THE FINDINGS

We have discussed various types of autonomy in this contribution. As a result, autonomy was identified as driver for behavioral changes in socio-technical systems. Table 1 and Table 2 sum up the findings regarding autonomy and capabilities of subject-oriented digital twins.

As already noted by [15] CPS 'do not simply pop into existence'. It is the creation phase to recognize undesirable behavior sequences and the emergence of unpredictable behavior. Behavior set in place

Table 1: Autonomy constellations and associated aspects of digital twins at design time

Autonomy Constellation	Representational Capacity of Subject-oriented Digital Twin (at Design Time)
Operational Component Autonomy	<ul style="list-style-type: none"> • Unified behavior encapsulation (subject specification) • Message passing between subjects
Federated Systems Autonomy	<ul style="list-style-type: none"> • Unified behavior encapsulation (subject specification) • Message passing between subjects
Autonomy Adaptation	<ul style="list-style-type: none"> • Adaptability of set of behavior encapsulations (subject specifications) - concerned subjects need to be modified • Adaptability of message passing between behavior elements (subjects) – concerned interfaces need to be modified
Update/Upgrade Autonomy	<ul style="list-style-type: none"> • Adaptability of set of behavior encapsulations (subject specifications) for design updates of concerned subjects • Adaptability of message passing between behavior elements (subjects) in case interaction changes of concerned subjects
Implementation Autonomy	<ul style="list-style-type: none"> • Adaptability of behavior encapsulations (subject specifications) ensuring semantic correctness • Adaptability of message passing between behavior elements (subjects) ensuring semantic correctness • Completeness of specification for automated execution of models

during the phases of creation and production is finally put to practice during the operational phase. The latter brings in interaction with operating humans, thus establishing CPS as socio-technical system. It is the digital twin, which links the physical system with its virtual equivalent that can serve as socio-technical baseline for reflecting on design before putting a CPS to actual operation. Moreover, behavior encapsulated in models represent how autonomy of CPS is specified and understanding in concrete CPS behavior. Behavior-encapsulating digital twins that can be executed enable probing and evaluating autonomy constellations before moving to actual operation. This validation is the most supportive asset of design-integrated engineering.

Current work discussing how digital twin representations relating to CPS design and engineering needs to consider and embody executable behavior encapsulations for autonomous socio-technical system development. For instance, [31], in the field of energy management, communication and control processes involving digital twins of CPS are key for reliable operation of power systems. Modeling the implementation focuses on high-bandwidth and low-bandwidth applications for oversight decision making.

Table 2: Autonomy constellations and associated aspects of digital twins at run time

Autonomy Constellation	Operational Capacity of Subject-oriented Digital Twin (at Run Time)
Operational Component Autonomy	<ul style="list-style-type: none"> • Assignment of control to behavior element (subject) • Each component can be addressed by control component through message passing protocol between subjects
Federated Systems Autonomy	<ul style="list-style-type: none"> • Choreography – instances of a subject belong to different settings • Unified message passing protocol between subjects
Autonomy Adaptation	<ul style="list-style-type: none"> • Choreography • Dynamic adaptability of instances at run time – only concerned subject instances are affected
Update/Upgrade Autonomy	<ul style="list-style-type: none"> • Choreography • Dynamic adaptability of instances at run time, replacing executable units
Implementation Autonomy	<ul style="list-style-type: none"> • Automated execution of models (in case of subject orientation choreographic run time engine, e.g., Akka-based)

Data-centric models capture physical and digital data streams for real-time measurements. According to the developed methodology, (decision making) behavior is triggered by interpreting incoming values.

Simulation has been considered by [33] addressing processes in production systems for factory planning. Thereby, digital twin representations represent existing factory systems and monitoring processes. Digital twins are generated from environmental information reducing the effort setting up models - shop floor elements are scanned and recognized as objects. The recognized objects serve as baseline for simulating CPS components as behavior encapsulations.

Both sample cases reveal the current focus in CPS development. The flow of data should be non-disruptive – which can be represented in digital twin models. It serves real-time decision making and cost reduction and optimization through live monitoring, as e.g., required for privacy management. So far, these models do neither refer to understanding and representing autonomy for the CPS under development, nor refer to socio-technical interaction. As such, current developments do not utilize digital twins as design representation to explore and validate the different variants of autonomy we have presented in the context of our home health care use case.

8 CONCLUSION

The present paper reviews the efficacy and efficiency gains associated with digital twins for integrating design and implementation of autonomy along CPS development. The feasibility of adopting

digital twin representations has been demonstrated in perspective of the design and execution capabilities of subject-oriented behavior models stemming from Business Process Management. These representations are argued as driving agents for creating and maintaining autonomous CPS through dynamic adaptation of CPS elements. Importance of encapsulated behavior models featuring run time validation of digital twin representations as a key supporter for CPS implementation could be demonstrated. We also have put forth to discuss the various topological constellations of autonomy with respect to CPS and the importance of the socio-technical design validation resulting into successful implementations of CPS.

REFERENCES

- [1] Mahdi Akil, Lejla Islami, Simone Fischer-Hubner, Leonardo A. Martucci, and Albin Zuccato. 2020. Privacy-Preserving Identifiers for IoT: A Systematic Literature Review. *IEEE Access* 8 (9 2020), 168470–168485. <https://doi.org/10.1109/ACCESS.2020.3023659>
- [2] Barbara Rita Barricelli, Elena Casiraghi, and Daniela Fogli. 2019. A Survey on Digital Twin: Definitions, Characteristics, Applications, and Design Implications. *IEEE Access* 7 (2019), 167653–167671. <https://doi.org/10.1109/ACCESS.2019.2953499>
- [3] Borja Bordon, Ramón Alcarria, Tomás Robles, and Diego Martín. 2017. Cyber-physical systems: Extending pervasive sensing from control theory to the Internet of Things. *Pervasive and Mobile Computing* 40 (2017), 156–184. <https://doi.org/10.1016/j.pmcj.2017.06.011>
- [4] Egon Börger and Robert Stärk. 2003. *Abstract State Machines*. Springer, Berlin, Heidelberg. <https://doi.org/10.1007/978-3-642-18216-7>
- [5] Stefan Boschert and Roland Rosen. 2016. Digital Twin—The Simulation Aspect. In *Mechatronic Futures*, Peter Hehenberger and David Bradley (Eds.). Springer International Publishing, Cham, 59–74. https://doi.org/10.1007/978-3-319-32156-1_5
- [6] Kai Bösefeldt. 2020. Holen wir uns das Web zurück! *Informatik Spektrum* 43, 3 (6 2020), 197–202. <https://doi.org/10.1007/s00287-020-01274-3>
- [7] Jan Camenisch, Manu Drijvers, Petr Dzurenda, and Jan Hajny. 2019. Fast key-verification anonymous credentials on standard smart cards. In *IFIP Advances in Information and Communication Technology*, Vol. 562. Springer, Cham, 286–298. https://doi.org/10.1007/978-3-030-22312-0_20
- [8] Jan Camenisch, Manu Drijvers, and Jan Hajny. 2016. Scalable Revocation Scheme for Anonymous Credentials Based on n-times Unlinkable Proofs. In *Proceedings of the 2016 ACM on Workshop on Privacy in the Electronic Society*. ACM, New York, NY, USA, 123–133. <https://doi.org/10.1145/2994620.2994625>
- [9] Olivier Cardin. 2019. Classification of cyber-physical production systems applications: Proposition of an analysis framework. *Computers in Industry* 104 (1 2019), 11–21. <https://doi.org/10.1016/j.compind.2018.10.002>
- [10] Patricia Derler, Edward A. Lee, Stavros Tripakis, and Martin Törngren. 2013. Cyber-physical system design contracts. In *Proceedings of the ACM/IEEE 4th International Conference on Cyber-Physical Systems - ICCPS '13*. ACM Press, New York, New York, USA, 109. <https://doi.org/10.1145/2502524.2502540>
- [11] Josep Domingo-Ferrer, Sara Ricci, and Jordi Soria-Comas. 2017. A Methodology to Compare Anonymization Methods Regarding Their Risk-Utility Trade-off. In *Modeling Decisions for Artificial Intelligence. Proceedings of the 14th International Conference, MDAI 2017, Kitakyushu, Japan, October 18-20, 2017*, Vicenç Torra, Yasuo Narukawa, Aoi Honda, and Sozo Inoue (Eds.). Springer, Cham, 132–143. https://doi.org/10.1007/978-3-319-67422-3_12
- [12] Albert Fleischmann, Udo Kannengiesser, Werner Schmidt, and Christian Stary. 2013. Subject-Oriented Modeling and Execution of Multi-agent Business Processes. In *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*. IEEE, Atlanta, GA, 138–145. <https://doi.org/10.1109/WI-IAT.2013.102>
- [13] Albert Fleischmann, Werner Schmidt, and Christian Stary (Eds.). 2015. *S-BPM in the Wild*. Springer International Publishing, Cham. <https://doi.org/10.1007/978-3-319-17542-3>
- [14] Albert Fleischmann, Werner Schmidt, Christian Stary, Stefan Obermeier, and Egon Börger. 2012. *Subject-Oriented Business Process Management*. Springer, Berlin, Heidelberg. 1–375 pages. <https://doi.org/10.1007/978-3-642-32392-8>
- [15] Michael Grieves and John Vickers. 2017. Digital Twin: Mitigating Unpredictable, Undesirable Emergent Behavior in Complex Systems. In *Transdisciplinary Perspectives on Complex Systems*. Springer International Publishing, Cham, 85–113. https://doi.org/10.1007/978-3-319-38756-7_4
- [16] Norbert Gronau, Marcus Grum, and Benedict Bender. 2016. Determining the optimal level of autonomy in cyber-physical production systems. In *2016 IEEE 14th International Conference on Industrial Informatics (INDIN)*, Vol. 0. IEEE, Poitiers, France, 1293–1299. <https://doi.org/10.1109/INDIN.2016.7819367>
- [17] Peter Hehenberger, Birgit Vogel-Heuser, David Bradley, Benoît Eynard, Tetsuo Tomiyama, and Sofiane Achiche. 2016. Design, modelling, simulation and integration of cyber physical systems: Methods and applications. *Computers in Industry* 82 (10 2016), 273–289. <https://doi.org/10.1016/j.compind.2016.05.006>
- [18] Christian Janiesch, Marcus Fischer, Axel Winkelmann, and Valentin Nentwich. 2019. Specifying autonomy in the Internet of Things: the autonomy model and notation. *Information Systems and e-Business Management* 17, 1 (3 2019), 159–194. <https://doi.org/10.1007/s10257-018-0379-x>
- [19] Udo Kannengiesser and Harald Muller. 2013. Towards Agent-Based Smart Factories: A Subject-Oriented Modeling Approach. In *2013 IEEE/WIC/ACM International Joint Conferences on Web Intelligence (WI) and Intelligent Agent Technologies (IAT)*. IEEE, Atlanta, GA, 83–86. <https://doi.org/10.1109/WI-IAT.2013.155>
- [20] Siddhartha Kumar Khaitan and James D. McCalley. 2015. Design techniques and applications of cyberphysical systems: A survey. *IEEE Systems Journal* 9, 2 (6 2015), 350–365. <https://doi.org/10.1109/JSYST.2014.2322503>
- [21] Steven Landers, Elizabeth Madigan, Bruce Leff, Robert J. Rosati, Barbara A. McCann, Rodney Hornbake, Richard MacMillan, Kate Jones, Kathryn Bowles, Dawn Dowding, Teresa Lee, Tracey Moorhead, Sally Rodriguez, and Erica Breese. 2016. The Future of Home Health Care: A Strategic Framework for Optimizing Value. *Home Health Care Management and Practice* 28, 4 (11 2016), 262–278. <https://doi.org/10.1177/1084822316666368>
- [22] Edward A. Lee. 2015. The past, present and future of cyber-physical systems: A focus on models. *Sensors (Switzerland)* 15, 3 (2 2015), 4837–4869. <https://doi.org/10.3390/s150304837>
- [23] Chao Liu, Pingyu Jiang, and Wenlei Jiang. 2020. Web-based digital twin modeling and remote control of cyber-physical production systems. *Robotics and Computer-Integrated Manufacturing* 64 (8 2020), 101956. <https://doi.org/10.1016/j.rcim.2020.101956>
- [24] Yuqian Lu, Chao Liu, Kevin LKai Wang, Huiyue Huang, and Xun Xu. 2020. Digital Twin-driven smart manufacturing: Connotation, reference model, applications and research issues. *Robotics and Computer-Integrated Manufacturing* 61 (2 2020), 101837. <https://doi.org/10.1016/j.rcim.2019.101837>
- [25] C. Merlo, A. Abi Akle, A. Llarra, G. Terrasson, E. Villeneuve, and V. Pilnière. 2019. Proposal of a user-centred approach for CPS design: pillbox case study. *IFAC-PapersOnLine* 51, 34 (2019), 196–201. <https://doi.org/10.1016/j.ifacol.2019.01.065>
- [26] Harald Müller. 2012. Using S-BPM for PLC Code Generation and Extension of Subject-Oriented Methodology to All Layers of Modern Control Systems. In *S-BPM ONE – Scientific Research. Proceedings of the 4th International Conference, S-BPM ONE 2012, Vienna, Austria, April 4-5, 2012*, Christian Stary (Ed.). Springer, Berlin, Heidelberg, 182–204. https://doi.org/10.1007/978-3-642-29133-3_12
- [27] National Science Foundation. 2020. Cyber-Physical Systems (CPS) (nsf20563) | NSF - National Science Foundation. <https://www.nsf.gov/pubs/2020/nsf20563/nsf20563.htm>
- [28] Elisa Negri, Luca Fumagalli, and Marco Macchi. 2017. A Review of the Roles of Digital Twin in CPS-based Production Systems. *Procedia Manufacturing* 11 (2017), 939–948. <https://doi.org/10.1016/j.promfg.2017.07.198>
- [29] Alexios Papacharalampopoulos, Panagiotis Stavropoulos, and Demetris Petrides. 2020. Towards a digital twin for manufacturing processes: Applicability on laser welding. *Procedia CIRP* 88 (2020), 110–115. <https://doi.org/10.1016/j.procir.2020.05.020>
- [30] Adil Rasheed, Omer San, and Trond Kvamsdal. 2020. Digital twin: Values, challenges and enablers from a modeling perspective. *IEEE Access* 8 (2020), 21980–22012. <https://doi.org/10.1109/ACCESS.2020.2970143>
- [31] Ahmed Saad, Samy Faddel, and Osama Mohammed. 2020. IoT-Based Digital Twin for Energy Cyber-Physical Systems: Design and Implementation. *Energies* 13, 18 (9 2020), 4762. <https://doi.org/10.3390/en13184762>
- [32] Ceren Salkin, Mahir Oner, Alp Ustundag, and Emre Cevikcan. 2018. A Conceptual Framework for Industry 4.0. In *Industry 4.0: Managing The Digital Transformation*. Springer, Cham, 3–23. https://doi.org/10.1007/978-3-319-57870-5_1
- [33] Markus Sommer, Josip Stjepandic, Sebastian Stobra, and Moritz Von Soden. 2020. Improvement of factory planning by automated generation of a digital twin. In *Advances in Transdisciplinary Engineering*, Jerzy Pokojski, Maciej Gil, Linda Newnes, Josip Stjepandic, and Nel Wognum (Eds.). Vol. 12. IOS Press, Amsterdam, 453–462. <https://doi.org/10.3233/ATDE200105>
- [34] Chris Stary and Dominik Wachholder. 2016. System-of-systems support — A bi-graph approach to interoperability and emergent behavior. *Data and Knowledge Engineering* 105 (2016), 155–172. <https://doi.org/10.1016/j.datak.2015.12.001>
- [35] Dominik Wachholder and Chris Stary. 2015. Enabling emergent behavior in systems-of-systems through bi-graph-based modeling. In *2015 10th System of Systems Engineering Conference, SoSE 2015*. IEEE, San Antonio, TX, USA, 334–339. <https://doi.org/10.1109/SYSE.2015.7151954>
- [36] Raphael Wagner, Benjamin Schleich, Benjamin Haefner, Andreas Kuhnle, Sandro Wartzack, and Gisela Lanza. 2019. Challenges and potentials of digital twins and industry 4.0 in product design and production for high performance products. *Procedia CIRP* 84 (2019), 88–93. <https://doi.org/10.1016/j.procir.2019.04.219>