Enhancing Dependability and Security of Cyber-Physical Production Systems

Hessamedin Bayanifar, Hermann Kühnle

Otto Von Guericke Universität Magdeburg, Germany
hessamedin.bayanifar@ovgu.de, hermann.kuehnle@ovgu.de

Abstract. Despite all its potentials, new industrial revolution enabled by cyber-physical systems (CPS), still has major concerns and obstacles to overcome with regards to dependability and security on its way to be fully appreciated. This study targets these concerns by proposing a generic model for intelligent distributed dependability and security supervision and control mechanisms to enable components to autonomously meet their own security and dependability objectives through real-time distributed improvement cycles, using multi-agent systems approach to enable full exploitation of the model's evolution capabilities.

Keywords: Cyber-Physical Production Systems, Smart Manufacturing Unit, Dependability and Security, Multi-Agent Systems.

1 Introduction

Smart distributed manufacturing systems consist of a large number of widely dispersed loosely-coupled yet collaborating heterogeneous components that are vastly connected to and communicate with cyber space. To enhance their capabilities, these systems try to exploit smart properties through enhancing their own intelligence and processing power, or via accessing the internet and its vast options to enhance these properties. On the one hand, using these properties and enhancing capabilities can offer manufacturing enterprises a plethora of opportunities and strategic advantages, on the other hand, however, such vast diversity and total exposure to cyber space, as well as versatility of processes and structures, raise major vulnerabilities as dependability and data security issues that may lower the motivation to rely on these enormous capabilities. In order to increase acceptance, three research hypotheses are posited:

H1: Additional properties and enhanced capabilities increase risks in playing manufacturing on the base of smart manufacturing units. Multi-agent software module patterns are most appropriate for supporting and optimising smart manufacturing units' applications and risks may be lowered by continuously monitoring and analysing the readiness (maturity) of properties and the cleanness of data flows (failure probabilities multiply).

H2: A powerful tool for monitoring and analysing dependability as well as maturities of properties and units can be established on the base of dynamic modelling. The model architecture may be specified by expected contributions and resulting requirements. The desired features for tool implementations may be provided by Multi-agent design pattern.

H3: A decision table for failure risks, disturbance cases, decisions for actions and inputs for learning may be established. Using agents, adequate architecture may be implemented into a learning experimentation environment for simulation or manufacturing scenarios and evaluations of risks.

Following the proposed three hypotheses the research question is formed as weather an agent-based distributed dependability and security supervision and control that has inherited smart system properties, can enhance overall dependability and security of the system. The corresponding factor to analyse the performance of the adopted approach is to see to what extent it promotes or enable flexibility, responsiveness, learning capability, scalability, level of autonomy, reconfigurability, and reusability of the model's modules. To assure maximum dependability throughout an enterprise, the adopted approach must be able to deal with all incorporated components, information flows among them as well as the cyber areas, networks, databases and servers. To this goal, a distributed Dependability and Security Model (Fig. 1) is introduced for covering the entire system, every units and components down to all levels of detail (LoD). The model includes a core model, a control loop, and a connection to the virtual world.

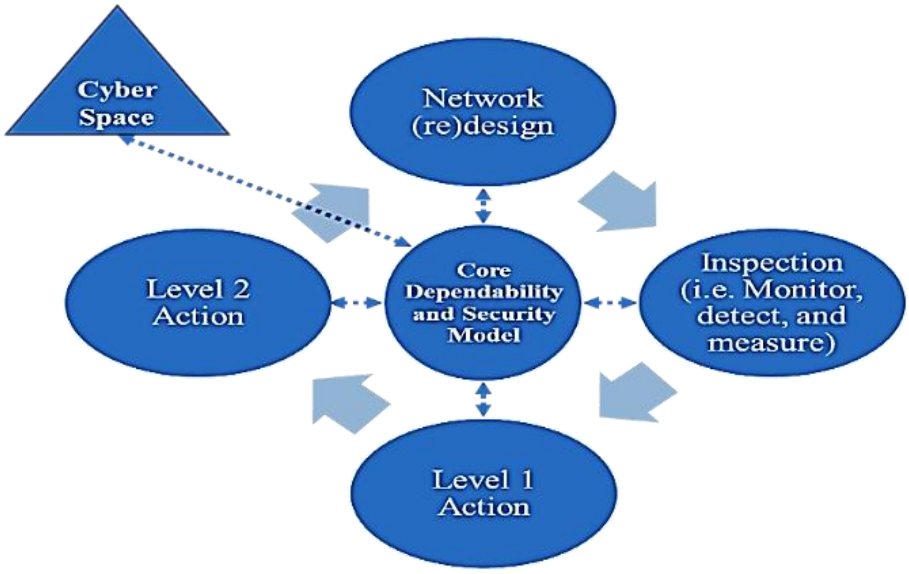

Fig. 1. Smart Dependability and Security architecture

The **core model** consists of two main parts: *object description*, and *risk model*, where the former focuses more on objects' context and self-awareness, and imports data about object's environment, collaborations, functions and modules, objectives, application and task description, etc. that are needed to develop risk model, and the latter covers accordingly all Dependability and Security parameters, vulnerabilities and risks, and the ways of measuring and dealing with them. The *core model*, in other words, feeds the improvement process to be done by the *control loop*. The relevant data for object description section are imported from the cloud or sensed as a part of the object's self-/context-awareness. The risk model contains a scalable feature for considering possible risks, assessing their criticality and their possible effects on the object or the system in total (e.g. Failure Mode, Effect and Criticality Analysis (FMECA)/Fault Tree Analysis (FTA)). Self-optimizing occur via sharing knowledge with all other smart units, and updating its own structure and database through continuous feedbacks (control loops).

The Control Loop invokes the process of Inspection (i.e. *Monitoring*, *Detecting*, and Identifying and *Measuring*), and Reaction (i.e. giving *Alarms*, taking *Action*, and doing the *Reconfiguration* afterwards) in real-time. All steps can be carried out fully- or semi-autonomously by smart objects through this attached core model, which is located in the cyber space and is in collaboration with all other models. This gives the components all abilities to collaborate with the common objective of raising and maintaining the dependability and security of the total system.

2 Relationship to Smart Systems

The suggested solution aims at improving the dependability and security of smart systems with its focus on (but not limited to) cyber physical production systems (CPPS). To this aim, we introduce a generic dependability model and architecture that tries to harness the capabilities and properties of smart systems, that are elaborated in [1] (i.e. interoperability, autonomy, scalability, modularity, heterogeneity, reconfigurability, and context-awareness), for maximising its performance and versatility. In other word, it aims to be mechanism equipped with smart systems' properties, to ensure the dependability and security of smart systems. In order to enable these properties, Intelligent Agents are to be summoned as the implementation toolset for our model.

3 Review of Literature

Smart Distributed Manufacturing systems, enabled by Cyber-Physical Systems, have major structural similarities, as they both address three main layers: physical layer, cyber layer, and data communication and integration layer. Each of these layers has its own concerns with regards to dependability and security. Accordingly, many studies tried to point out these issues or suggest countermeasures [2-6], or to point out and to evaluate the cyber-physical vulnerabilities and their impacts on manufacturing systems [7]. In [8], the approach tries to design and to implement a robust cyber

physical system, and [9] attempts to model ontology-based dependability in CPSs using FMEA techniques are outlined. Mathematical approaches were used in [10] to model security risks of CPSs and to quantitatively evaluate their risks. Dependability of self-optimizing systems was studied and analysed in [11], where various methods covering conceptual design, and development phases were introduced. Authors in [12] used systems' context awareness to increase security in information access, by asking questions like: *who* wants *what* information, *how*, from *where*, and *when*? This study, on the other hand, tries to propose a generic model, and an agent-based structure for developing an intelligent and autonomous distributed dependability and security supervision, and control in CPPS. The model, given its structure, and enabled by intelligent agents, is expected to bring more flexibility and responsiveness. Also, higher autonomy and scalability is predicted through context-awareness and summoning the capabilities of intelligent agents. Moreover, due its decentralized real-time monitoring and control, higher coverage and improved stability is likely to be achieved.

4 Research Contribution and Innovation

This section describes the multi-agent based architecture of the dependability and security mechanism explained in the introduction, and elaborates on the way smart systems properties are manifested and practised in this model. In the end an example shows how the model can function in a given condition using its capabilities enabled by the properties it possesses.

4.1 Multi-Agent Systems (MAS) for Model Architecture

The dependability and security model as described, with the potential properties mentioned, requires a toolset to enable such properties. Accordingly, Multi-Agents Systems (MAS) can be a decent candidate, since intrinsically, intelligent agents (IA) demonstrate responsiveness, proactiveness, goal-orientation, social-ability, scalability, flexibility, robustness, self-configuration, adaptability/ re-configurability, along with their decentralized architecture and learning capabilities [13]. After determining the tool, the model is to be translated into an architecture composed of interacting agents. The first step would split the model task-wise onto single agents. Doing so, the following table 1 and figure 2 demonstrate how to introduce agents and their task descriptions, as well as their overall structure and collaborations' relations.

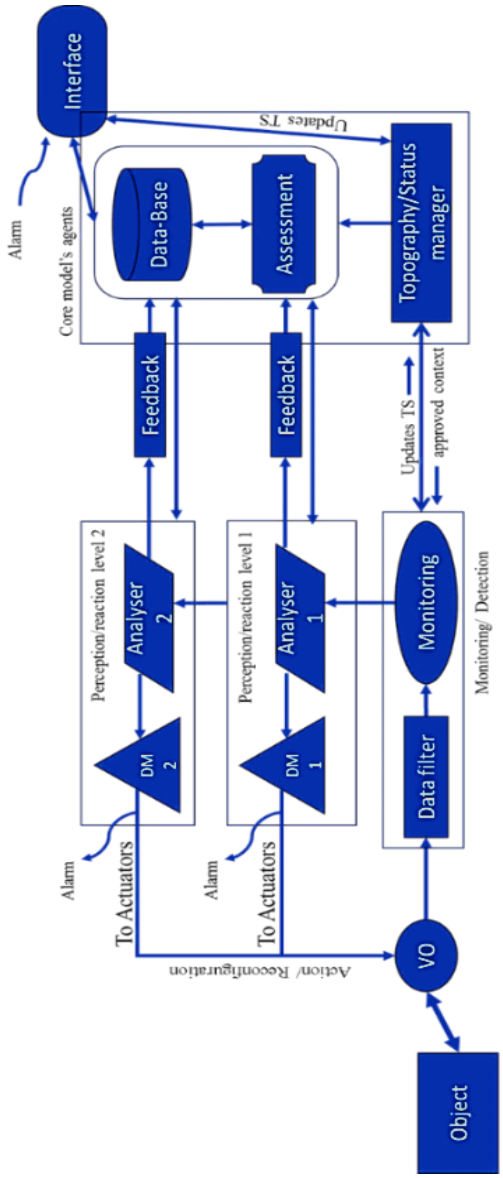

Fig. 2. Proposed Agent Architecture for components' intelligent dependability and security

Table 1. Applied agents and their task description

	Agents	Task Description
Core model	Status manager	Updates the status of components. The main part of context-awareness. Knows the approved context, authorities, topography of the system, etc.
	Database	Stores components models and risk data. Data are stored here in modules for each type of risk to be accessed by analysers and assessment agent. Other components when authorized, can have access to some of the data during negotiation or when they are new to the system, to get updated with vulnerabilities and measures, etc.
	Assessment agent	Receives data from analyser and assesses the risk through negotiating with other components' assessors, receiving context data from TS manager, and having access to the database and the object model
	Interface	For negotiations between agents of other components. Updating the topography and context information, more accurate and global risk assessment, providing access to databases of other components.
Monitoring / detection	Data filter	Filtering out redundancies. Looking for useful data among loads of data
	Monitoring	Looking for anomalies and risks, by comparing the current-state sensed data with current-state approved context. Then sends the detected cases to level one analyser.
Measurement	Data analyser lvl 1	For simpler problems/quicker responses. Data analyser does the identification and measurement of risks. Lvl 1 analyser does the simple analysis and communicates with assessment agent to provide proper input for DM level one. It then provides feedback to the core model.
	Data analyser lvl 2	For more complicated problems, analyser level 1 sends the case to analyser level two with more abilities. If needed this analyser practises negotiations with other components agents to provide best global data of the risk to feed the DM level 2.
Alarm/ Action/ Reconfiguration	Decision-Making lvl 1	For simpler reactions/ quicker responses. After supplied with proper risk information, releases alarm to right entities and send proper commands to actuators to apply right corrective actions, and reconfiguration when needed. Feedback is then being provided to the core model
	Decision-Making lvl 2	Provides higher lever reactions, and reconfigurations, and more advanced alarms for more complicated issues. If needed asks for collaboration of other agents and components resources to solve a problem. Feedback is then being provided to the core model.

Data captured by sensors are sent to the VO (virtual object), which is the cyber representative or digital twin of the component (e.g. industry 4.0 component). Then, these data are filtered (to omit unnecessary data), monitored, and at the same time this stage is being fed into a status/topology manager to gain the approved context for comparing the filtered sensed data to detect anomalies. When detected, info is sent to the level one analyser, where in collaboration with assessment agent and database, the risk will be identified, and its severity will be measured as the sum of possible losses it can cause to other components or parts of the system. Risk data will be sent to the

decision-making agent (DM level one) for making decisions on the appropriate actions, e.g. alarms, and send the command to actuators. However, if the problem requires more advanced analysis, it will be sent to the analyser level two, where harder problems can be analysed, and negotiations with other agents might be necessary to make the right measurements and analyses to provide accurate data for DM level 2. In decision making level two, more complex actions, and if required, negotiations with agents of other components (e.g. for sharing resources in fixing an issue), take place. After the actions are carried out, and issues are confirmed to be solved, the result is fed into the core model to update the risk assessor.

4.2 Properties, as Seen in the Model, and an Agent-Based Example

Table 2 shows the expected contribution of the smart systems properties and accordingly the resulting requirements.

An example can consider a job-shop unit with several automated machines and conveyors, using multi-agent systems to control their production system. Simultaneously, along with data form sensors, machines and controllers' interactions will be checked via "monitoring agents", receiving all information being send and captured by controller units and machines. Two of the possible risks can be either one of the controller agents itself be compromised by an adversary, or something unintentionally occurs to one of the machines. Some cyber security risks associated with the former might be cloning, repudiation, MITM attack, DDoS, eavesdropping, and some risks concerning the machines (can be partial or full breakdowns, connectivity loss, etc.). Taking the breakdown of one of the machines as an example, the monitoring agent will notice the change in the system in real-time (e.g. the number of parts passing across a specific sensor), the analyser will identify the issue (i.e. in this case breakdown of a machine (machine B, in figure 3)) and will measure the impact on the system and its components it collaborates with, and will send the data to decision the maker agent: Alarms will be published to the right entities (e.g. controllers, maintenance centre, spare part inventory, etc.). The machine will be stopped and called unavailable. The request will be sent to other agents for availability of another machines to do the task instead of the broken-down machine and after locating the alternative machine, ways (e.g. conveyors, AVGs, etc.), will be found to send the parts to the new alternative machine. And finally, a feedback will be sent to the core model for updating the data base and the assessment model, and for generating reports.

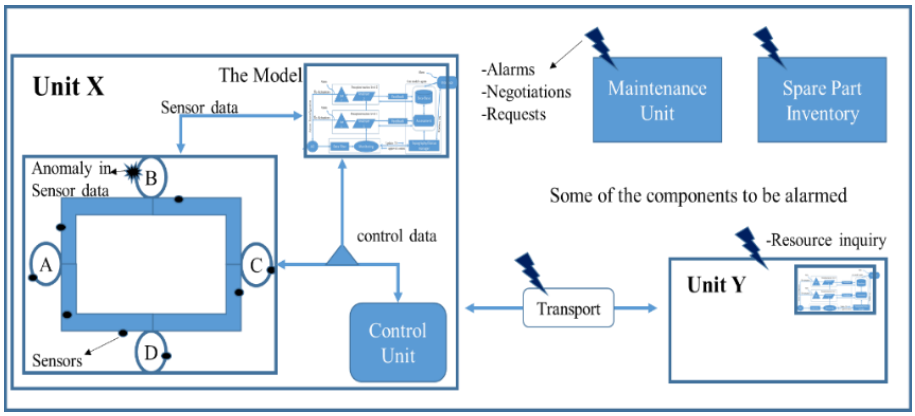

Fig. 3. experiment setup and scheme in a smart manufacturing unit breaks down

Table 2. Control loop steps and the relationship with smart manufacturing systems' properties

	Contribution	Requirements / method
Monitoring: constantly checking the related parameters defined in the core model to find risks		
Context-awareness	Parameters are derived from the context	Via sensors/ cloud
Interoperability	Hierarchical/heterarchical collaboration	Shared semantic/ ontology
Autonomy	Autonomously done by Intelligent Agents	Core model/ sensors
Modularity	Resources to be used in various setups	Modular resources
Scalability	Resources to be added or removed	Registering mechanism
Heterogeneity	Mechanism differs based on object type	Via core model
Detecting: Finding anomalies/risks by comparing real-time status with approved parameters		
Context-awareness	Current vs Approved context comparison	Via sensors/ core model
Interoperability	Hierarchical/heterarchical collaboration	Shared semantic/ ontology
Autonomy	Done by agents, and aided by core model	Agents/ data base
Modularity	Data-base and model to be re-useable	Modular risk Data-base
Scalability	To be seen data-base / detection methods	Updateable core model
Heterogeneity	Methods differs based on object type	Set in core model
Measuring: When detected, identifying the risk type, its severity, impacts, occurrence frequency, using assessments methods such as FMEA/FTA		
Context-awareness	Finding global measure based on context	Updating context data
Interoperability	Objects negotiating to find global measure	Via agents/ model
Autonomy	Done by agents and by using risk model	Risk model in the core
Modularity	Measurement resources to be shared reused in various setups	Risk categories to be modularly saved
Scalability	Criteria/ data-base to be changed/ updated	Scalable risk model
Heterogeneity	Criteria and risk model differ object-wise	Risk model definition
Alarm: Alarming right entities, i.e. people, or components that may be affected by the risk		
Context-awareness	Right entities are known through context	Context update in model
Interoperability	In carrying alarm to various entities	Semantic definition
Autonomy	Done by agents after measuring risks	Agent collaboration
Modularity	Agents/functions to be used in new setups	Modular alarm resource
Scalability	methods/agents to be added or removed	Scalable alarm resource
Heterogeneity	Mechanism tries to stay the same for all	Semantic definition
Action: Making globally optimum decisions and defending against/fixing measured risks.		

Context-awareness	Optimum decision/reaction context-wise	Via sensors/ models
Interoperability	Sharing resources/ information for taking optimum decision and action	Via semantic and ontology definition
Autonomy	To be done autonomously by agents	Agent collaboration
Modularity	Resources to be mixed in various setups	Modular agents/actuators
Scalability	Agents/actuators/ models to be scalable	Registering mechanism
Heterogeneity	Actions/resources differ by object type	Via model/ resources
Reconfiguration: providing feedback to the model and preparing the component to be reused		
Context-awareness	To be done based on context requirements	Via the model
Interoperability	Providing understandable feedbacks to others/ receiving required data	Via model and semantic definition
Autonomy	Semi/fully autonomous and done by agents	Model/ Agents
Modularity	Components may be reused in new setups	Modular components
Scalability	Extended/reduced structure in new setup	Scalable model/object
Heterogeneity	Done based on object type. Same feedback mechanism	Via model Same agent functionality

4 Conclusion

Based on available technologies, a structure based on multi-agent systems was suggested as the dependability and security model. Moreover, intelligent agents are shown to be capable of equipping the process of dependability and security supervision and control with the smart systems' properties to improve it and make it more efficient. The next step of the study would be testing the model in various cases and extending its performance and capabilities (H3). One case is simulating the example described above, and the other will focus on the data security risks (e.g. intrusion attack, DDoS attack) on one component to test the models performance in detecting and blocking it, and after disinfection, reconfiguring the component to be used again by the system. The experiment is to be done by simulating DDoS attack i.e. by overloading and increasing data traffic, assessing the models' reactions in handling the risk and its learning progresses for feedback.

References

1. Kühnle, H. and G. Bitsch, Smart Manufacturing Units. 2015: p. 55-70.
2. Huang, S., et al., Cyber-physical system security for networked industrial processes. International Journal of Automation and Computing, 2015. 12(6): p. 567-578.
3. Wells, L.J., et al., Cyber-physical security challenges in manufacturing systems. Manufacturing Letters, 2014. 2(2): p. 74-77.
4. Wu, G., J. Sun, and J. Chen, A survey on the security of cyber-physical systems. Control Theory and Technology, 2016. 14(1): p. 2-10.
5. Zhang, L., Q. Wang, and B. Tian, Security threats and measures for the cyber-physical systems. The Journal of China Universities of Posts and Telecommunications, 2013. 20, Supplement 1: p. 25-29.
6. Karnouskos, S., Chapter 6 - Industrial Agents Cybersecurity, in Industrial Agents. 2015, Morgan Kaufmann: Boston. p. 109-120.

7. DeSmit, Z., et al., Cyber-physical Vulnerability Assessment in Manufacturing Systems. Procedia Manufacturing, 2016. 5: p. 1060-1074.
8. Hu, F., et al., Robust Cyber–Physical Systems: Concept, models, and implementation. Future Generation Computer Systems, 2016. 56: p. 449-475.
9. Sanislav, T., G. Mois, and L. Miclea, An approach to model dependability of cyber-physical systems. Microprocessors and Microsystems, 2016. 41: p. 67-76.
10. Orojloo, H. and M.A. Azgomi. A method for modeling and evaluation of the security of cyber-physical systems. In: 2014 11th International ISC Conference on Information Security and Cryptology. 2014.