Publications

2017

Trustworthiness Requirements for Manufacturing Cyber-Physical Systems

Radu F. Babiceanu
Embry-Riddle Aeronautical University

Remzi Seker
Embry-Riddle Aeronautical University, sekerr@erau.edu

Scholarly Commons Citation

Babiceanu, R. F., & Seker, R. (2017). Trustworthiness Requirements for Manufacturing Cyber-Physical Systems. *Procedia Manufacturing, 11*(). https://doi.org/10.1016/j.promfg.2017.07.202

Available online at www.sciencedirect.com

ScienceDirect

Procedia Manufacturing 11 (2017) 973 – 981

Procedia MANUFACTURING

27th International Conference on Flexible Automation and Intelligent Manufacturing, FAIM2017, 27-30 June 2017, Modena, Italy

Trustworthiness requirements for manufacturing cyber-physical systems

Radu F. Babiceanu[a]*, Remzi Seker[a]

[a]*Department of Electrical, Computer, Software, and Systems Engineering, Embry-Riddle Aeronautical University*
Daytona Beach, FL 32114-3900, United States

Abstract

Distributed manufacturing operations include cyber-physical systems vulnerable to cyber-attacks. Long time not considered a priority, cybersecurity jumped to the forefront of manufacturing concerns due to the need to network together legacy, newer equipment, and entire operation centers. This paper proposes trustworthiness solutions for integrated manufacturing physical-cyber worlds, where trustworthiness is defined to complement system dependability requirements with cybersecurity requirements, such that the resulting manufacturing cyber-physical system delivers services that can justifiably be trusted. Acknowledging the inevitability of cyber-attacks, the paper models the cybersecurity component using the resilient systems framework, where system resilience is viewed as preservation of a required state of cybersecurity.

Keywords: cyber-physical systems; trustworthiness requirements; manufacturing cybersecurity; system resilience; denial of service

1. Introduction

The current manufacturing worldwide operations trend imposes the presence of all established requirements in terms of manufacturing design processes and actual operations, combined with an increased safety and flexibility of

* Corresponding author. Tel.: +1-386-226-7535; fax: +1-386-226-6678.
E-mail address: babicear@erau.edu

doi:10.1016/j.promfg.2017.07.202

operations. In addition, it requires the presence of more recent cybersecurity protection of electronic transactions between distributed operation centers [1].

The high-tech progress in material science research, and the information and communication technologies made the development of manufacturing cyber-physical systems a reality. Not only physical facilities can be linked together through network applications and coordinate their applications, but also physical operations can be simulated in real-time in cyber centers. The resulting benefits are significant, and to name a few, cyber-physical coordination leads to reduced raw material used in testing, prototyping, and actual operations, as well as increased safety of finished products [2]. Moreover, the manufacturing cyber-physical systems include a wide range of sensing devices and data processing capabilities that can provide online monitoring of manufacturing processes, thus further reducing the chances of scrapped lots and increasing the safety of the actual manufacturing operations, through production abort commands, whenever hazardous events, or out-of-specifications environment conditions are detected [3].

Since all good things come with a price tag, the path towards manufacturing cyber-physical systems has one of its own. Just as all other network-based or Internet-based systems, cyber-physical distribution of manufacturing operations include systems vulnerable to cyber-attacks. Long time not considered a priority, cybersecurity jumped to the forefront of manufacturing concerns due to the need to network together legacy, newer equipment, and entire operation centers. Many of the legacy operations are controlled by Supervisory Control and Data Acquisition (SCADA) systems that automatically monitor and adjust process control activities and control physical pieces of equipment [4, 5]. However, many SCADA systems were designed and built in the 1980s without any regard of cybersecurity. Recent research discusses also the need to network traditional stand-alone equipment such as PLC-controlled and CNC machines, which were never designed with any control measure for data security. The newer systems have their cybersecurity problems of their own, as many of the Internet of Things devices embedded on physical manufacturing equipment, such as sensors and data processing and communication hardware, are reported to be easily hacked and become the port of entry for intruders to the manufacturing network data centers [6, 7]. Given all the above issues, within the manufacturing and cybersecurity fields, the capability of virtualized manufacturing operations to prevent, respond, thwart and/or recover from cyber-attacks is now becoming an active area of research.

This paper proposes trustworthiness solutions for integrated manufacturing physical-cyber worlds, where trustworthiness is defined to complement system dependability requirements with cybersecurity requirements, such that the resulting manufacturing cyber-physical system delivers services that can justifiably be trusted. System dependability, traditionally, includes operational availability, reliability, safety, and maintainability requirements, which can only be enhanced by the advancement of cyber-physical systems in manufacturing operations. Cybersecurity includes aspects such as confidentiality, integrity, availability, authenticity, and assurance of data transactions and/or computer systems, and to a lesser extent anonymity of data records and transactions. Acknowledging the inevitability of cyber-attacks, this paper models the cybersecurity component using the resilient systems framework, where system resilience is viewed as preservation of a required state of cybersecurity [8, 9].

From this point forward, the paper is structured as follows. Section 2 presents the trustworthy manufacturing cyber-physical model, with its dependability and cybersecurity requirements, and introduces the concept of system resilience in the face of cyber-attacks. Next, Section 3 provides insights for the cyber-resilience mechanisms through simulation modeling. The paper concludes with a brief section summarizing the importance of cybersecurity adoption within manufacturing domain and a discussion related to needed further investigation of manufacturing cyber-physical systems.

2. Trustworthy Manufacturing Cyber-Physical Systems

Previous authors' work identified the framework for the development of manufacturing cyber-physical systems, emphasizing aspects such as complex event processing, virtualization, Internet of Things adoption, Big Data analytics, and cyber-attacks targets and vehicles [1-3]. This current work goes further into modeling aspects by adding to the mix traditional operational requirements such as availability, reliability, safety, and maintainability, many times known as system dependability, and detailing cybersecurity protection mechanisms.

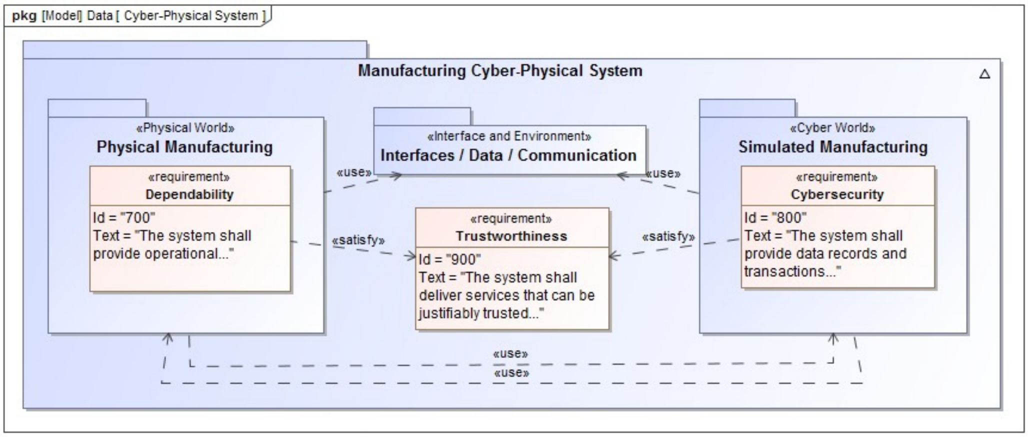
pkg [Model] Data [Cyber-Physical System]
Manufacturing Cyber-Physical System
«Physical World»
Physical Manufacturing
«requirement»
Dependability
Id = "700"
Text = "The system shall provide operational..."
«Interface and Environment»
Interfaces / Data / Communication
«requirement»
Trustworthiness
Id = "900"
Text = "The system shall deliver services that can be justifiably trusted..."
«Cyber World»
Simulated Manufacturing
«requirement»
Cybersecurity
Id = "800"
Text = "The system shall provide data records and transactions..."
«use»
«use»
«satisfy»
«satisfy»
«use»
«use»

Fig. 1. Trustworthiness requirements within the manufacturing cyber-physical systems framework.

The resultant system, presented in Fig. 1, is deemed as exhibiting trustworthiness requirements by delivering services that can be trusted with a certain level of confidence. The dependability and cybersecurity requirements that form the trustworthiness platform use a combination of lower level requirements usually present in physical processing and computer network systems. System operational availability, reliability, maintainability, and safety requirements are well studied in the manufacturing literature and are not the subject of this work. On the cyber world side, the cybersecurity requirements are part of the computer and network security domains, but have not been studied in detail from the manufacturing environment perspective. Both the dependability and cybersecurity requirements in the context of manufacturing domain are detailed in Fig. 2.

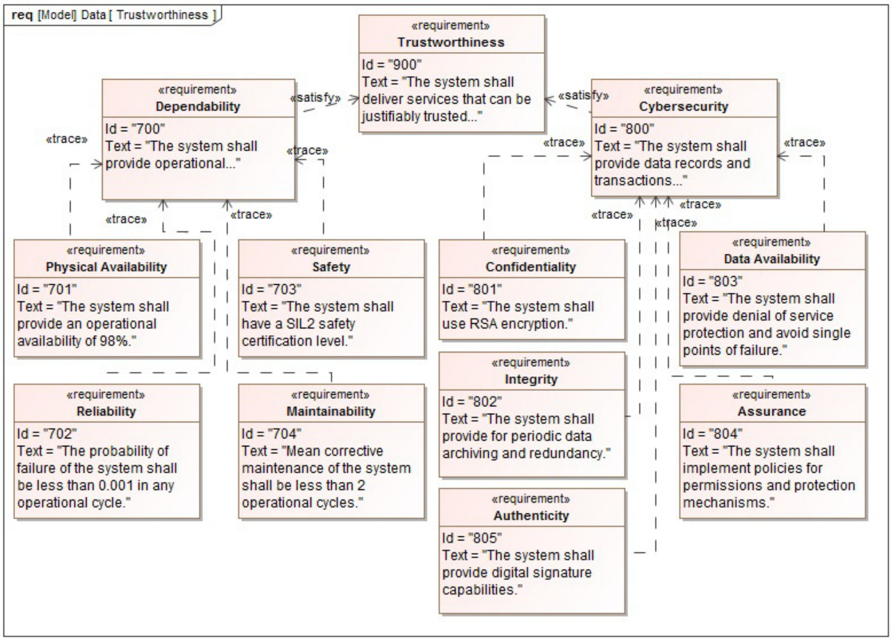
req [Model] Data [Trustworthiness]
«requirement»
Trustworthiness
Id = "900"
Text = "The system shall deliver services that can be justifiably trusted..."
«requirement»
Dependability
Id = "700"
Text = "The system shall provide operational..."
«requirement»
Cybersecurity
Id = "800"
Text = "The system shall provide data records and transactions..."
«satisfy»
«satisfy»
«trace»
«trace»
«trace»
«trace»
«trace»
«trace»
«trace»
«trace»
«trace»
«requirement»
Physical Availability
Id = "701"
Text = "The system shall provide an operational availability of 98%."
«requirement»
Safety
Id = "703"
Text = "The system shall have a SIL2 safety certification level."
«requirement»
Reliability
Id = "702"
Text = "The probability of failure of the system shall be less than 0.001 in any operational cycle."
«requirement»
Maintainability
Id = "704"
Text = "Mean corrective maintenance of the system shall be less than 2 operational cycles."
«requirement»
Confidentiality
Id = "801"
Text = "The system shall use RSA encryption."
«requirement»
Integrity
Id = "802"
Text = "The system shall provide for periodic data archiving and redundancy."
«requirement»
Authenticity
Id = "805"
Text = "The system shall provide digital signature capabilities."
«requirement»
Data Availability
Id = "803"
Text = "The system shall provide denial of service protection and avoid single points of failure."
«requirement»
Assurance
Id = "804"
Text = "The system shall implement policies for permissions and protection mechanisms."

Fig. 2. Elements of trustworthiness for the manufacturing cyber-physical system.

The actual requirements listed in Fig. 1 and 2 are likely examples of what dependability and cybersecurity requirements would be for actual distributed manufacturing operations. Availability, reliability, and maintainability of manufacturing equipment is defined by its vendors, so it could vary based on the scope and resources. Safety requirement is using the IEC 61508 [10] standard for programmable controllers in the process control industry, but, once again, it could vary based on the scope and resource. Confidentiality, integrity, and data availability are known in the security community as the CIA triad [11]. Confidentiality assures protection of data from disclosure to unauthorized parties and is usually enforced through data encryption. Integrity assures data protection from being modified by unauthorized parties and is usually ensured through archiving and redundancy of data transmission. Availability assures that authorized parties are able to access the data when needed, and it is obtained through different mechanisms that protect the system and data from external attacks, such as denial of service attacks. The other two cybersecurity requirements, authenticity and assurance are complementary to the CIA triad and further help distributed manufacturing actors in trustworthy data transactions through digital signature capabilities and permission and protection mechanisms.

3. System Resilience Research Methodology

There is a growing literature in the domain of system resilience, and a significant number of definitions were proposed. The common denominator of all resiliency definitions includes the following aspects: unexpected event, nominal performance, degradation of performance, recovery, and specific amount of time acceptable for each application. Thus, we define system resilience as the ability of the system to recover to its nominal performance level, in an acceptable amount of time, after the occurrence of an unexpected event that resulted in a degradation of the level of performance, well below the nominal level. There are at least two comprehensive literature overview in the resilience arena, with the second one published just a few months ago [12, 13]. While resilience can reside in both the physical and cyber worlds, and thus is a key aspect for low cost, continuous, manufacturing operations, this work builds models for the system resilience in the face of cyber-attacks, or cyber-resilience.

Looking again at the above resilience definition, one of its blurred aspects is related to the amount of time considered acceptable for each application. This carry a paramount importance for cyber-resilience given the extremely strict time requirements imposed on cyber systems. The recovery length of time could be short, in which case the system exhibits high resilience, or it could be longer, in which case the system is said to have low resilience. For two systems that are perturbed by the same external unexpected event at the same time, and degraded to the same level of lower performance, the low and high resilience systems bounce back to the initial level of performance in significant different timeframes. As an interesting fact, the same type of behavior was also observed in non-engineering systems [14]. The low and high cyber-resilience profiles are presented in Fig. 3 below.

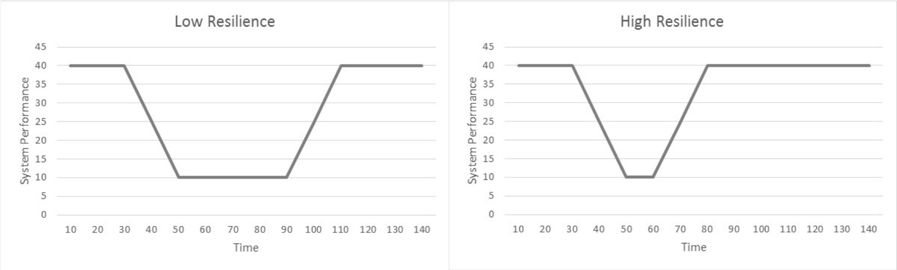

Fig. 3. Low and high resilience profiles.

The amount of time to recover to the initial level of performance, if possible, is one of the most used resilience metrics identified in several works [15-17]. Another straightforward metric is given by the impact on performance calculated either, as the difference between nominal level of performance and the degraded level of performance, the proportion of the degraded level of performance in relation to initial nominal performance level, or the area under the performance curve which is lost. Those metrics can be easily inferred on the chart of Fig. 3. There are other resilience metrics proposed in the literature, out of which this work will look at the network-related ones [18]. Even resilience is viewed as an after the fact approach measured through one of its metrics, the trustworthy manufacturing cyber-physical system considers embedding resilience mechanisms into both the physical and cyber worlds to eliminate or mitigate the effects of any system malfunction and/or breach. Specifically, this work considers cyber-resilience aspect and models resilience mechanisms with the objective of preservation of the required state of security.

This research objective is exemplified in the diagram of Fig. 4, where the distributed manufacturing system is subjected to directed external events, such as cyber-attacks, and random disturbances, which are both processed within the data module through cyber and physical resilience mechanisms. The resilience metrics need be chosen such that they model the changes in the system performance as inferred from Fig. 3. Also, the resilience mechanisms need be designed such that they minimize the adverse impact of the external events and recover the system to the required state of security in an acceptable amount of time. The type of mitigation and recovery algorithms depend on the scope and layout of the system under analysis, as distribution of manufacturing nodes within a network may differ from one layout to another.

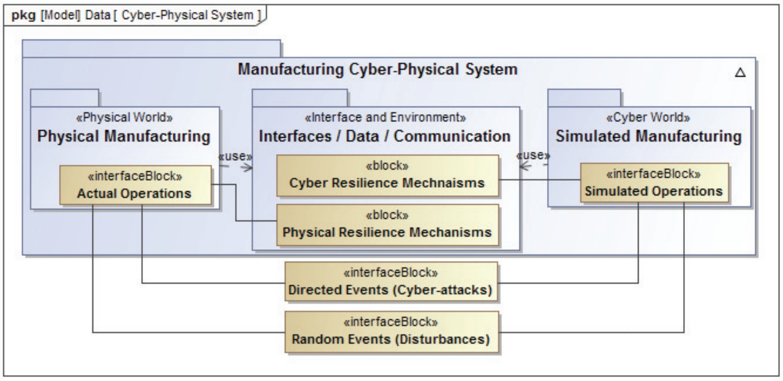
pkg [Model] Data [Cyber-Physical System]
Manufacturing Cyber-Physical System
«Physical World»
Physical Manufacturing
«interfaceBlock»
Actual Operations
«use»
«Interface and Environment»
Interfaces / Data / Communication
«block»
Cyber Resilience Mechnaisms
«block»
Physical Resilience Mechanisms
«use»
«Cyber World»
Simulated Manufacturing
«interfaceBlock»
Simulated Operations
«interfaceBlock»
Directed Events (Cyber-attacks)
«interfaceBlock»
Random Events (Disturbances)

Fig. 4. Distributed manufacturing system network.

4. Manufacturing Cyber-Resilience Mechanisms Simulation Model

Distributed manufacturing across different location geographically distinct requires a constant exchange of design, testing, control, and operations data. This adds to the communication needs between the physical world --physical manufacturing-- and cyber world --simulated manufacturing-- already discussed above. The simulation model considers the operations of a manufacturing system network formed of two distributed manufacturing organizations (systems), each of them including a certain number of manufacturing nodes, subjected to denial of service (DOS) attacks. The DOS attacks target either the two distributed systems or the network between the two distributed systems. The two distributed systems form a manufacturing network on their own with physical and cyber worlds components, while the larger network connecting the two distributed systems includes only cyber world components. The overall distributed system is presented in Fig. 5, where the block stereotype model either a physical or cyber component, while the flow specification stereotype model elements of the internal or external communication networks.

4.1. Cyber-resilience metrics and mechanism

The resilience metric included in the model is the performance of the communication link to forward packets (data and/or control packets) between two network nodes, and across the entire network when the network nodes are subjected to DOS attacks. The model considers that a node of a network is targeted with a defined probability, and the attack is successful with another defined probability. The actual packet flow performance comes from the network science domain and is defined as the percentage of maximum flow that a directed network supports as edges are blocked or removed from the network [15, 19]. Thus, the flow performance of a network link can be defined as:

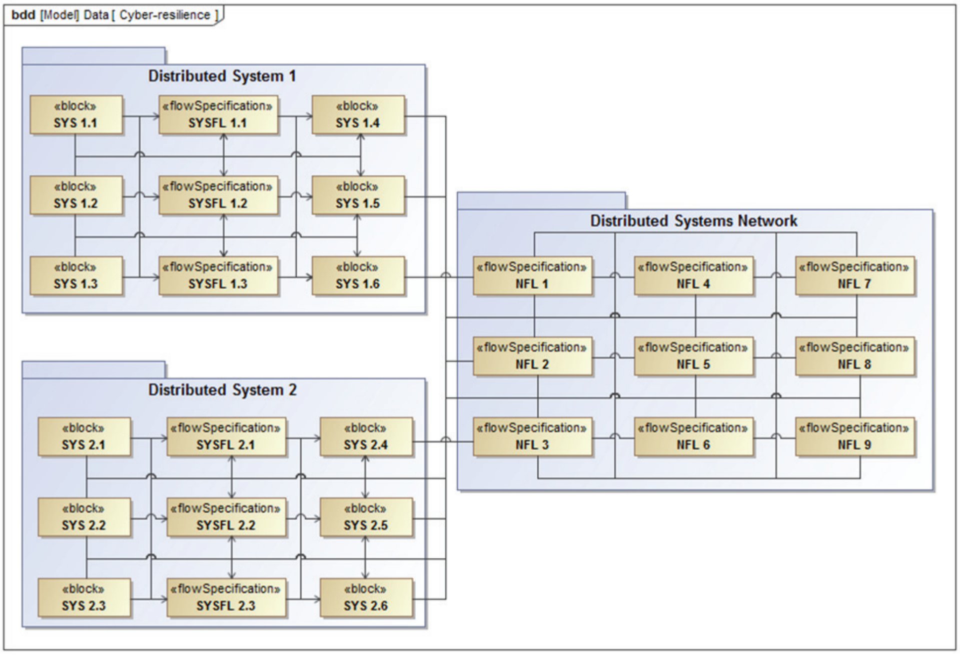
bdd [Model] Data [Cyber-resilience]
Distributed System 1
«block» SYS 1.1
«flowSpecification» SYSFL 1.1
«block» SYS 1.4
«block» SYS 1.2
«flowSpecification» SYSFL 1.2
«block» SYS 1.5
«block» SYS 1.3
«flowSpecification» SYSFL 1.3
«block» SYS 1.6
Distributed Systems Network
«flowSpecification» NFL 1
«flowSpecification» NFL 4
«flowSpecification» NFL 7
«flowSpecification» NFL 2
«flowSpecification» NFL 5
«flowSpecification» NFL 8
«flowSpecification» NFL 3
«flowSpecification» NFL 6
«flowSpecification» NFL 9
Distributed System 2
«block» SYS 2.1
«flowSpecification» SYSFL 2.1
«block» SYS 2.4
«block» SYS 2.2
«flowSpecification» SYSFL 2.2
«block» SYS 2.5
«block» SYS 2.3
«flowSpecification» SYSFL 2.3
«block» SYS 2.6

Fig. 5. Distributed manufacturing system network.

$$L(t) = \frac{F(t)}{Fmax} \tag{1}$$

where, $F(t)$ is the flow forwarded by a node into a link at time t, and F_{max} is the nominal flow forwarded by a node into a link.

It results that the link flow resilience can be defined as:

$$R(t) = P(t)Q(t)\frac{F(t)}{Fmax} \tag{2}$$

where, $P(t)$ is the probability that the node is attacked at time t, and $Q(t)$ is the probability that the attack on the node is successful.

The resilience mechanism included in the model is designed to re-route the packets subject to delays through other less crowded communication links should any of the node processing becomes slow or unable to forward data and/or control packets. A similar mechanism could be devised using the actual packet queues measured in front of the processing nodes with rerouting occurring based on algorithmic evaluation of queue lengths. A measure for the performance of the resilience mechanism, R, is defined in relation with the percentage of denied service. The denied service includes the number of packets that were discarded at the under-attack nodes. Packets can be discarded due to time delays in queue or exceeding queue capacity.

$$R = \frac{DS}{TS} \tag{3}$$

where, DS is the number of packets discarded, and TS is the total number of packets forwarded through the network.

4.2. Design of simulation experiments and simulation results

Using the distributed model depicted in Fig. 5, the nodes of the simulation model at time zero are linked as follows. Within the two distributed systems, each of the six nodes (block modules) have active links, with nominal performance, with each of the three flow specification modules. Outside the distributed systems, each of the six edge block modules also have active links, with nominal performance, with six out of the nine network flow specification modules. The simulation variables and decision modules include the created packets created (communication load), packet processing at nodes (packet forwarding), decision variables related to node forwarding and link flow (DOS attacks), and decision modules to re-route (resilience mechanisms). The communication load created in the system is the same for both sets of simulation replications and the node forwarding process comes from the same statistical distributions. Also, for both sets of simulation replications, the DOS attacks are using the same distributions and are initialized at the same clock time. In other words, equal intensity and duration DOS attacks are activated in the models.

In the first set of 100 simulation replications, DOS attacks target the internal distributed systems network and resilience mechanisms are activated once the attacks are detected. The results of this simulation, identified as component-level resilience profile, are presented in Fig. 6. The second set of 100 simulation replications consider DOS attacks targeted at the communication network outside the two distributed systems and the resilience profile, depicted as system-level resilience, are shown in Fig. 7. However, for both sets of replications the attacks still target all the nodes of the part of model under study that carry flow at the time when DOS attacks are activated.

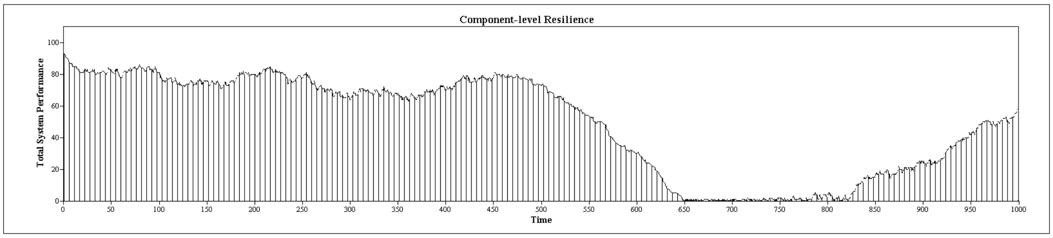

Fig. 6. Component-level resilience profile for the two distributed systems.

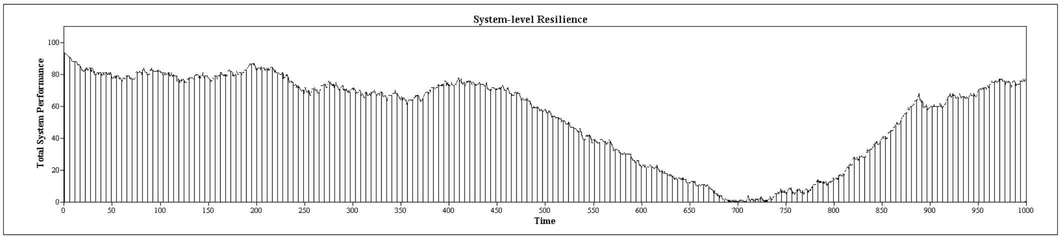

Fig. 7. System-level resilience profile for the network connecting the two distributed systems.

It can be seen from the two figures that the degradation in performance is more significant for the component-level resilience profile, which does not fully recover to its initial nominal performance level in the set simulation replication time. The calculated percentage of denied service for the two sets of simulation replications is depicted in Fig. 8. All the simulation variables listed above are coming from statistical distributions and can be customized for different system scenarios.

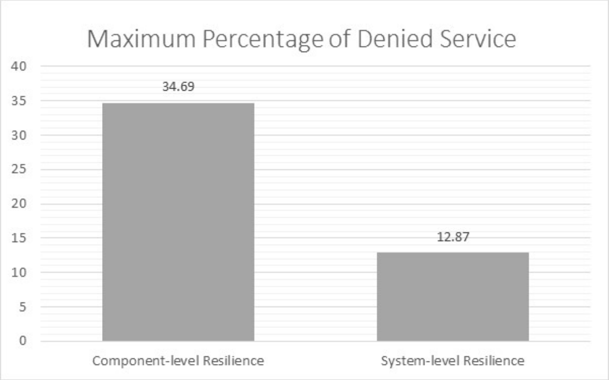

Fig. 8. Maximum percentage of packet denied service for the two sets of simulation.

5. Conclusions and Future Directions

This paper proposes a framework for the development of trustworthiness solutions for manufacturing cyber-physical systems, which include dependability and cybersecurity requirements. Detailed modeling is only performed for the cybersecurity aspects by modeling a series of denial of service attacks against an overall manufacturing network formed by physical and cyber world nodes. The results of the simulation study show that the cyber-resilience mechanisms are better deployed when the number of network nodes is larger to permit re-routing of packets in the network. By generalizing the results, it may be possible to adapt the solution to the cyber-resilience of system-of-systems models, in which case it may become apparent that the resilience of the system-of-systems level is higher than that of individual component systems of the system-of-systems.

Future research directions include the analysis of other cybersecurity attacks and their influence on the component-level and system-level cyber-resilience. On another direction, the work can be enhanced by adding other trustworthiness components to the system resilience model and evaluate their influence on the derived resilience metrics.

References

[1] R.F. Babiceanu, R. Seker, Big data and virtualization for manufacturing cyber-physical systems: A survey of the current status and future outlook, Computers in Industry, 81 (2016) 128-137.

[2] R.F. Babiceanu, R. Seker, Manufacturing operations, Internet of things, and big data: Towards predictive manufacturing systems, in: T. Borangiu, D. Trentesaux, A. Thomas, (Eds.), Service Orientation in Holonic and Multi-Agent Manufacturing, Springer Studies in Computational Intelligence, 594 (2015), pp. 157-164.

[3] R.F. Babiceanu, R. Seker, Manufacturing cyber-physical systems enabled by complex event processing and big data environments: A framework for development, in: T. Borangiu, D. Trentesaux, A. Thomas, (Eds.), Service Orientation in Holonic and Multi-Agent Manufacturing, Springer Studies in Computational Intelligence, 594 (2015), pp. 165-173.

[4] M. Goodman, Future Crimes: Everything is Connected, Everyone is Vulnerable, and What We Can Do About It, Random House, New York, 2015.

[5] P.A.A. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks, ISA Transactions, 46 (2007) 583-594.

[6] L. Wang, M. Torngren, M. Onori, Current status and advancement of cyber-physical systems in manufacturing, Journal of Manufacturing Systems, 37 (2015) 517-527.

[7] L.J. Wells, J.A. Camelio, C.B. Williams, J. White, Cyber-physical security challenges in manufacturing systems, Manufacturing Letters, 2(2014) 74-77.

[8] M.A. Thompson, M.J. Ryan, J. Slay, A.C. McLucas, A new resilience taxonomy, in: Proceedings of the INCOSE International Symposium, 2016.

[9] R.F. Babiceanu, R. Seker, Cybersecurity and resilience modeling for software-defined networks-based manufacturing applications, in: T. Borangiu, D. Trentesaux, A. Thomas, P. Leitao, J. Oliveira (Eds.), Service Orientation in Holonic and Multi-Agent Manufacturing, Springer Studies in Computational Intelligence, 694 (2017), pp. 167-176.

[10] International Electrotechnical Commission, IEC 61508-1 Functional safety of electrical/electronic/programmable electronic safety related systems – Part 1: General Requirements, Edition 2.0, International Electrotechnical Commission (2014).

[11] M. Goodrich, R. Tamassia, Introduction to Computer Security, Pearson, 2010.

[12] R. Francis, B. Bekera, A metric and frameworks for resilience analysis of engineered and infrastructure systems, Reliability Engineering and System Safety, 121 (2011) 90-103.

[13] N. Yodo, P. Wang, Engineering resilience quantification and system design implications: A literature review, Journal of Mechanical Design, 138 (2016) 11408-1-11408-13.

[14] S.R. Carpenter, Complex systems: Spatial signatures of resilience, Nature, 496 (2013) 308-309.

[15] M. Ouyang, Review on modeling and simulation of interdependent critical infrastructure systems, Reliability Engineering and System Safety, 121 (2014), 43-60.

[16] P. Erdi, Complexity explained, Springer, Berlin, 2010.

[17] S.S. Shah, R.F. Babiceanu, Resilience modeling and analysis of interdependent infrastructure systems, in: Systems and Information Engineering Design Symposium, 2015, pp. 154-158.

[18] T.G. Lewis, Network science, theory and applications, John Wiley & Sons, Hoboken, 2009.

[19] M.E.J. Newman, Networks, An introduction, Oxford University Press, Inc., New York, 2010.