Proceedings of the 2020 Winter Simulation Conference
K.-H. Bae, B. Feng, S. Kim, S. Lazarova-Molnar, Z. Zheng, T. Roeder, and R. Thiesing, eds.

PRODUCT LIFE CYCLE PERSPECTIVE ON ICT PRODUCT SUPPLY CHAIN RESILIENCE

Jānis Grabis

Institute of Information Technology
Riga Technical University
Kalku 1
Riga, LV-1658, LATVIA

ABSTRACT

Resilient supply chains are designed and operated to deal with disruptive events in an efficient manner. In ICT product supply chains, disruptions are often observed as vulnerabilities discovered in components used in the products. The vulnerabilities can be associated with the components themselves as well as with suppliers, and they can be averted by patching and supply chain reconfiguration. The paper elaborates a simulation model for analyzing relationships between the cost of treating the vulnerabilities and the supply chain configuration. We show that flexible supply chain configurations have the lowest cost and are the most resilient to vulnerabilities. The vulnerabilities associated with suppliers, for example, due to the loss of their trustworthiness, cause more-significant fluctuations in supply chain performance than the vulnerabilities associated with individual components. The monitoring cost have a significant impact on the selection of the most-resilient configuration.

1 INTRODUCTION

An Information and Telecommunications Technologies (ICT) product consists of multiple interrelated software and hardware components as well as related services (e.g., for a smart watch). Constituent parts of the ICT product are provided by a multitude of suppliers creating an ICT product supply chain. It is common that vulnerabilities are discovered in the ICT product supply chain. For instance, software components require regular security updates (Cavusoglu et al. 2008). There are many examples of supply-chain-induced vulnerabilities (Kshetri and Voas 2019). For example, 40 million Target credit card data were stolen by exploiting security shortcomings in HVAC devices used at the stores and provided by an external vendor, or 40,000 U.K. users were affected by a data leak in a third party customer chat-bot. The vulnerabilities discovered need to be addressed, which might result in changes in the supply chain configuration (Pariazar and Sir 2018). The supply chain configuration is a set of supply chain units and links among these units defining the underlying supply chain structure and key attributes of the supply chain network (Chandra and Grabis 2016). A resilient supply chain is configured in a way of being able to cope efficiently with disruptive events due to vulnerabilities (Tukamuhabwa et al. 2015). This paper perceives resilience as an ability to discover and treat vulnerabilities in ICT products before these vulnerabilities can be exploited by malicious parties.

The impact of vulnerabilities depends on the supply chain configuration. The existing research shows that the supply chain's resilience can be increased by selecting an appropriate supply chain configuration. Determinants of supply chain resilience are supply network density, complexity, and node criticality (Falasca et al. 2008). The supply chain resilience can be assessed by abilities to reduce the occurrence of disruptive events, to reduce consequences of these events, or to reduce the time to recover to normal performance. The overall supply chain strategy is crucial for achieving the resilience including such factors as continuous monitoring, transparency, collaboration, product design, and supply chain network design

978-1-7281-9499-8/20/$31.00 ©2020 IEEE

(Gunasekaran et al. 2015). Simulation has been proposed as a suitable technique to analyze supply chain resilience in the case of disruptive events (Wang et al. 2016).

The ICT product supply chain is often characterized by a tight coupling between product design and supply chain configuration. Therefore, product design and supply chain configuration need to be considered simultaneously. The ICT products also often have a limited life cycle, and security updates are provided only for a limited period of time (Massacci and Nguyen 2014). The lack of security updates leads to product retirement. This research investigates a problem of designing a resilient supply chain for an ICT product with a limited life cycle.

The objective of this paper is to identify relationships between the ICT product supply chain configuration and its resilience to vulnerabilities discovered in components provided by suppliers. The analysis is performed by means of a simulation model. The simulation model is elaborated and experimental studies are conducted. The contribution of the paper is a new simulation model for analyzing the relations between the supply chain configuration and its ability to deal with vulnerabilities. The experimentation is intended as a step towards theory building on ICT product supply chain resilience (Macdonald et al. 2018).

The rest of the paper is structured as follows: Section 2 discusses types of supply chain configurations and related work on supply chain resilience. The ICT product supply chain model is formulated in Section 3. Experimental studies are conducted in Section 4, and Section 5 concludes.

2 BACKGROUND

The supply chain is a network of supply chain units collaborating in transforming raw materials into finished products to serve common end-customers. The supply chain configuration defines supply chain participants and relationships among them. Supply chains often experience random disturbances. Resilient supply chains are able to cope with these disturbances in an effective manner.

2.1 Supply Chain Configuration

Ponis and Koronis (2012) define supply chain resilience as an ability to proactively plan and design the supply chain network for anticipating unexpected disruptive events, respond adaptively to disruptions while maintaining control over structure and function, and transcend to a post robust state of operations. Various supply chain configuration strategies can be pursued to achieve the resilience (Gunasekaran et al. 2015). Chandra and Grabis (2016) define lean, flexible, agile, and service-oriented supply chain configuration strategies. Lean supply chains focus on establishing long-term links among the supply chain units and reducing the number of units and links. Flexible supply chains have built-in redundancies and cushions in the form of extra units and links to deal with changes and uncertainties. The supply chain units and links are less specialized and multiple functions can be performed. Service-oriented supply chains have much less strong associations with particular spatial location of supply chain units and customers. More importantly, a primary focus switches from the physical movement of products to the electronic movement of information and delivery of services. Mari et al. (2015a) classify supply chains according to their network topology, including supply chains having regular, random, small-world, and scale-free underlying network properties. The regular networks have nodes with similar numbers of connections. The scaled networks have few nodes with a very large number of connections and many nodes with a small number of connections. These networks behave differently in presence of random and target disruptions. This paper considers random attacks. The product design in the supply chain model can be represented using Bill-Of-Material schemas, matrix schemas, and AND/OR graphs (Yao and Askin 2019).

In this paper, a simple joint representation of product design and supply chain configuration is adopted (Figure 1). It shows the product produced by a focal company and its components. To represent the supply chain configuration, suppliers are indicated for every component. Three different supply chain configurations are distinguished, namely, dominant supplier, dedicated suppliers, and flexible suppliers. Few suppliers provide most of the components in the dominant supplier configuration. In the extreme case, all components are provided by a single supplier. This configuration can be perceived as a lean supply chain with a very small number of nodes and connections. A high level of efficiency can be achieved at the expense of the dependency on the small number of nodes in the supply chain. The opposite solution is the dedicated suppliers configuration, where every component is provided by a separate supplier. The resulting network is a regular network with a relatively large number of nodes and small number of connections. In the case of flexible suppliers configuration, suppliers provide multiple components, while none of them can be considered a dominant supplier. The configuration is flexible in a sense that a single supplier can provide multiple components and the resulting network is a random or regular network.

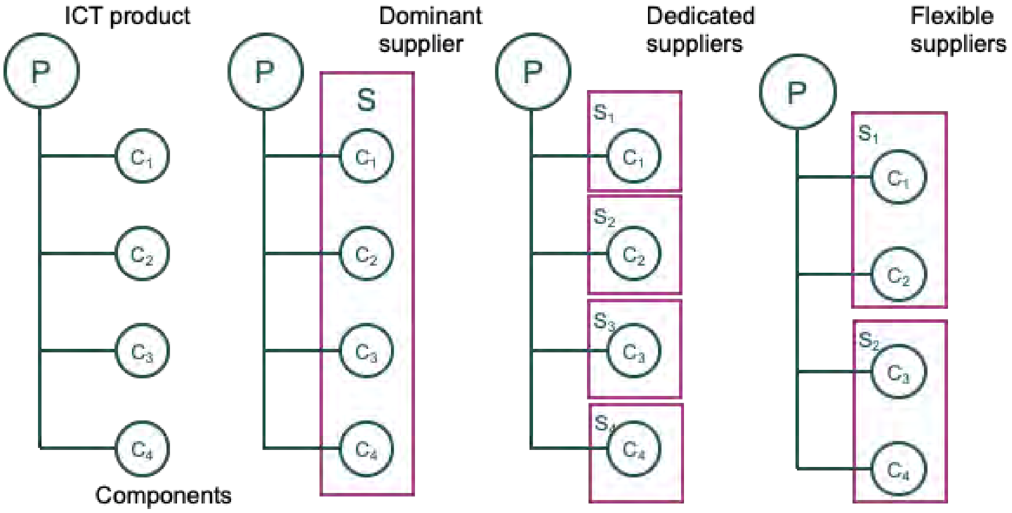

Figure 1: Joint representation of product design and supply chain configuration for the cases of dominant supplier, dedicated suppliers, and flexible suppliers.

2.2 Related Work

The existing research investigates resilience of supply chain configurations from the perspective of network theory or tactical level operations management. There are few publications investigating ICT product supply chains.

Perera et al. (2017) review research on supply chain configuration from the network theory perspective. They discuss basic network, analytical, and simulation models. The simulation models are found suitable for modeling random failures and targeted attacks. Modularity and disassortativity are identified as common features of real-world supply chain networks. An action-based model to deal with disruptions in the network is proposed by Arora and Ventresca (2018). It analyzes supply availability subject to removal of nodes in the supply chain. The networks have different levels of resilience depending on industry. The network theory is also employed by Mari et al. (2015a). An agent-based simulation modeling is performed to determine supply availability after targeted and random disruptions. They found that an efficient and resilient supply chain should have the Power law as an underlying degree distribution, short characteristic path length, and a high clustering coefficient. Furthermore, it should be robust to both targeted and random disruption. However, none of the typical network models meets these requirements. Mari et al. (2015b) identify information systems as one of the causes of disruptions in supply chains.

Goldbeck et al. (2020) analyze disruptions in various physical supply chains to emphasize the need for pre-disruption investment in capacity and adaptive post-disruption response. The resilience is measured by the ability to meet end-user demand subject to disruptive events. Pooling of the resources is shown to have significant impact on the resilience. Cigolini et al. (2014) simulate the impact of various supply chain configuration attributes, such as the number of stages on its performance. The model considers specific manufacturing and ordering policies. The importance of information sharing is emphasized. Similarly, Pero et al. (2010) use system dynamics and Petri net models to analyze relations between the topological features of a supply chain and its performance. They focus on inventory management aspects and find that the results depend on the number of suppliers in a stage, while the number of stages is not a significant aspect. Carvalho et al. (2012) simulate an automotive supply chain to analyze its resilience. Resilience strategies based on flexibility and redundancy are particularly considered, and flexibility is shown to increase the resilience. Lead time and cost are used as the key performance measures.

ICT products are ubiquitous and of major importance in businesses and society. These products are highly modular and their components are sourced globally. However, they often lack transparency and their designs evolves rapidly. Therefore, the importance of the supply chain perspective of ICT products grows rapidly (Luo et al. 2013). The concurrent product supply chain design is widely accepted in supply chain management theory and practice (Gran and Grunow 2016). Data analytics help to uncover complex supply chain topologies (Zhao et al. 2018), though currently analysis is based on static data structures. There are a number of developments on secure supply chain management (Hasan et al. 2020) as well as security concerns specifically from the ICT perspective (Polatidis et al. 2017). However, these are methods based on traditional security management frameworks and rely on static analysis and periodic product and process inspection.

To summarize the brief literature review, the existing network-theory-based models typically do not consider the time dimension, while the existing simulation models make assumptions about operational characteristics of the supply chain. The proposed model focuses on ICT product supply chains at the strategic level over the product life cycle. An integrative approach to supply chain risk management and resilience proposed by Shekarian and Mellat Parast (2020) defines that specific resilience enhancers address certain supply chain risks. From this perspective, the proposed model concerns supply and control risks, which can be addressed by flexibility (i.e., flexible supply chain configuration) and collaboration (i.e., information exchange and treatment of vulnerabilities). While the supply risks and respective mitigation strategies are well-studied, their interactions with the control risks using flexibility and collaboration as mitigation strategies are considered to a limited extent.

3 MODEL

A model representing the resilient ICT product supply chain is formulated and simulated to obtain insights on the impact of supply vulnerabilities on the supply chain performance.

3.1 Notation

The following notation is used in the model:

i – index referring to components and I is the number of components
j – index referring to suppliers and J is the number of suppliers
t – index referring to the time period
T – length of the product's life cycle
c_{ij} – equals to 1 if the ith component is provided by the jth supplier and 0 otherwise
v – cost of patching a vulnerability
p – penalty for not patching a vulnerability per time period
m – monitoring cost per supplier
π_1 – the probability that a supplier will fail during the product life cycle
π_2 – the probability that a component will fail during the product life cycle
X_{it} – equals to 1 if ith component's vulnerability is observed in the tth period and 0 otherwise
Y_{jt} – equals to 1 if jth supplier's vulnerability is observed in the tth period and 0 otherwise
Z_t – equals to 1 if vulnerabilities are patched in the tth time period and 0 otherwise
Ω_t – equals to 1 if vulnerabilities are not patched in the tth time period and 0 otherwise
TC – the total cost of treating the vulnerabilities

The other notation is introduced as necessary.

3.2 Problem Statement

The research problem is the design of an ICT product supply chain that is resilient to vulnerabilities discovered in sourced components. The objective is to find the ICT product supply chain configuration with the lowest cost of treatment of the vulnerabilities. It is assumed that the ICT product consists of a number of components. The components are supplied by external suppliers. These can be both hardware and software components as well as services. Vulnerabilities in the components are occasionally discovered. They can be associated with either components or suppliers themselves. The vulnerabilities imply that the ICT product becomes potentially unsecure, and the situation should be remedied. The situation can be remedied by applying a patch, which is an often-used solution for ICT product supply chains. Patching is perceived as a proactive defense to ensure supply chain resilience (Wang et al. 2016).

The key assumptions are:

1. The ICT product has a fixed-length life cycle;
2. Vulnerabilities are discovered at random time periods;
3. Vulnerabilities are eliminated by applying a patch;
4. If a vulnerability concerns a component, then only this component is patched;
5. If a vulnerability concerns the supplier, then all components provided by the supplier are patched (or replaced);
6. A company can opt for not patching the vulnerabilities and accepting penalty for that;
7. In order to discover vulnerabilities, suppliers should be monitored resulting in the monitoring cost per supplier.

3.3 Model Formulation

The model is formulated to minimize cost of running a resilient supply chain by choosing a suitable ICT product supply chain configuration. The ICT product *P* is defined by its components:

$$P=\left(\mathbf{C},\beta\right),$$

where $\mathbf{C}$ is the set of components and $\beta:\mathbf{C}\rightarrow P$ is function mapping the components into the final product. The current model assumes a simple composition of the product without dependencies among the components.

The ICT product supply chain *D* consists of the focal company *F* and its suppliers:

$$D=\left(F,\mathbf{J},\mathbf{C},\gamma\right),$$

where $\mathbf{J}$ is the set of suppliers and $\gamma:\mathbf{C}\times\mathbf{J}$ defines relations among the components and the suppliers. The model uses c_{ij} to indicate that the *i*th component is provided by the *j*th supplier.

The cost of running a resilient supply chain consists of three parts, namely, cost of patching, penalty for running unpatched system, and cost of monitoring the suppliers. The total cost is calculated over the entire product's life cycle (1):

$$TC=PC+NC+MC \tag{1}$$

$$PC=v\sum_{t=1}^{T}Z_t\left(\sum_{j=1}^{J}\sum_{i=1}^{I}c_{ij}Y_{jt}+\sum_{i=1}^{I}X_{it}\right) \tag{2}$$

$$NC=p\sum_{t=1}^{T}\Omega_t\left(T-t+1\right)\left(\sum_{j=1}^{J}\sum_{i=1}^{I}c_{ij}Y_{jt}+\sum_{i=1}^{I}X_{it}\right) \tag{3}$$

$$MC=m\times J \tag{4}$$

The cost of patching vulnerabilities *PC* is incur for every vulnerability observed and patched in the given time period (2). The penalty for not patching vulnerabilities *NC* incurs for every vulnerability observed and not patched in the given time period (3). Moreover, it incurs repeatedly over the remaining part of the product life cycle. The monitoring cost *MC* incurs for each of the suppliers (4). The indicator Y_{jt}

indicates failure (i.e., discovery of the vulnerability) of the *j*th supplier and X_{it} indicates failure of the *i*th component (Figure 2). The failure probability is π_1 and π_2, respectively. All components should be patched in the case of the supplier's failure. In practice, that could imply a change of the supplier leading to supply chain reconfiguration. A component is patched only once within a time period.

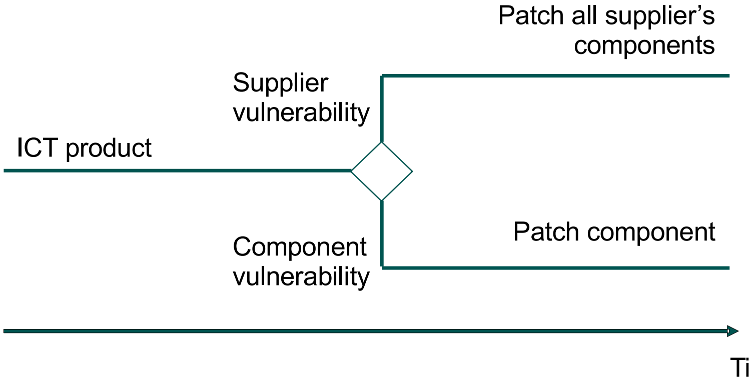

Figure 2: Distinction between supplier and component vulnerabilities.

The focal company has a choice whether to patch the vulnerability (Figure 3). The vulnerability is patched if the cost of patching is smaller than the penalty of not patching over the remaining time (5):

$$\text{if } v \le p \times \left(T - t + 1\right) \text{ then } Z_t = \text{true} \tag{5}$$

The indicator Z_t points towards the patching and $\Omega_t = \neg Z_t$ indicates not-patching. The expression $p \times \left(T - t + 1\right)$ states that not-patching penalty incurs for the remaining time periods. The patching options apply to both supplier and component vulnerabilities.

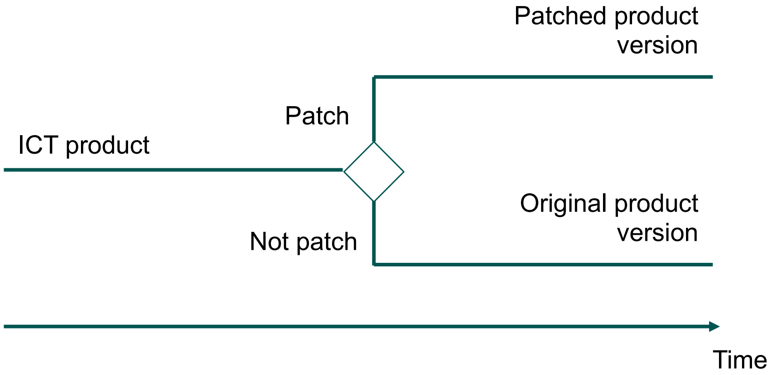

Figure 3: Distinction between patching and not-patching vulnerabilities.

3.4 Simulation

Monte Carlo simulation is used to explore the supply chain vulnerability by generating random events and analyzing the process dynamics. It is performed for a single product over its life cycle:

1. The model parameters are initialized.
2. For each time period proceed with Step 3.

3. For each supplier generate supplier failure with probability π_1 taking into account the number of periods. If not failed then $Y_{jt} = 0$ and go to Step 4, otherwise $Y_{jt} = 1$ and:
   (a) If Z_t is true as calculated in (5), then all components for the given supplier are patched and the patching cost are applied;
   (b) If Z_t is not true (i.e., Ω_t is true), then ignore the vulnerability and incur the not-patching penalty for all components provided by the given supplier.
4. For each component generate a component failure with probability π_2 taking into account the number of periods. If not failed, then X_{it}=0 and go to Step 5, otherwise X_{it}=1 and:
   (a) If Z_t is true, then patch the given component and incur the patching cost;
   (b) If Z_t is not true, then ignore the vulnerability and incur the not-patching penalty for the component.
5. Go back to Step 3 unless all suppliers are considered.
6. Go back to Step 2 unless the end of the product life cycle is reached.
7. Calculate the final values of the performance measures (1).

The simulation is performed for multiple ICT product supply chain configurations and the configuration yielding the best performance is considered as the most suitable. The simulation model is implemented using the Python general purpose programming language.

4 EXPERIMENTAL INSIGHTS

We conducted experimental studies with the simulation model to determine relationships between the ICT product supply chain configuration and its resilience. It is considered that a resilient supply chain has the lowest total cost of treating vulnerabilities. The performance measures considered are:

- *TC* – the total cost of treating vulnerabilities
- *PC* – the cost of patching vulnerabilities
- *NC* – the penalty for not-patching vulnerabilities
- *MC* – the monitoring cost
- *SC* – the cost due to suppliers' failure (part of *PC* and *NC* attributable to the suppliers' failure)
- *CC* – the cost due to components' failure (part of *PC* and *NC* attributable to the components' failure)

The specific research questions are:

- What is the impact of patching cost, not-patching penalty, and monitoring cost on the total cost of treating vulnerabilities?
- Which ICT product supply chain configuration type is the most resilient according to its ability to deal with vulnerabilities?
- Is the choice between patching and not patching affected by the configuration?

We used the values of the parameters as given in Table 1. The number of components is 12. The number of suppliers varies from 1 to 12 for the configurations D1 to D3, respectively. The patching cost v=10. The product life cycle is one year consisting of 12 time periods. The cost for not patching the vulnerability are expressed as a multiple of the patching cost $p = \lambda v / T$. The monitoring cost are expressed as a fraction of the not-patching penalty $m = \mu p$, where μ is a monitoring cost multiplier.

Three supply chain configurations are considered. D1 corresponds to the dominant supplier configuration. It involves one supplier providing all components. D3 corresponds to the dedicated suppliers configuration. It has twelve suppliers each providing exactly one component. D2 represents the flexible configuration. There are four suppliers each providing three components. The supplier failure probability is varied between 0.04 and 0.2. The component failure probability is varied between 0.1 and 0.5. The high value indicates that there is 50 % chance that a component vulnerability will be discovered in a year. π_2 is larger than π_1 because component failures are more common in practice. The probabilities are selected in-line with ICT industry practices of classifying vulnerabilities (Ashbaugh 2008).

Table 1: Experimental factors.

#	Factor	Values	Description
1	D	D1, D2, D3	Supply chain configuration
2	λ	2.5, 5	Not-patching penalty multiplier
3	μ	0.25, 0.5	Monitoring cost multiplier
4	π_1	0.05, 0.1, 0.2	Supplier failure probability
5	π_2	0.1, 0.25, 0.5	Component failure probability

Each experimental treatment is simulated for 200 replications (what is selected using the Heidelberg and Welch (1983) test with rounding up to the nearest hundred). The analysis of variance indicates that all experimental factors have significant impact on *TC* at least at the 99 % level of significance.

Figure 4 shows the share of *SC, CC,* and *MC* in the total cost. As expected, *SC* has the largest share for the dominant supplier configuration, which also has the lowest monitoring cost. The choice of the configuration significantly affects the distribution between *CC* and SC. From the managerial perspective, that suggests that supplier failures are more costly in dominant supplier situations and high resiliency could only be achieved having highly trusted dominant suppliers. The monitoring cost substantially increase in the case of the dedicated suppliers configuration, while the suppliers' failure cost are reduced. This is illustrated in Figure 5, showing that the monitoring cost multiplier has the most significant effect on the resilience for the dedicated suppliers configuration.

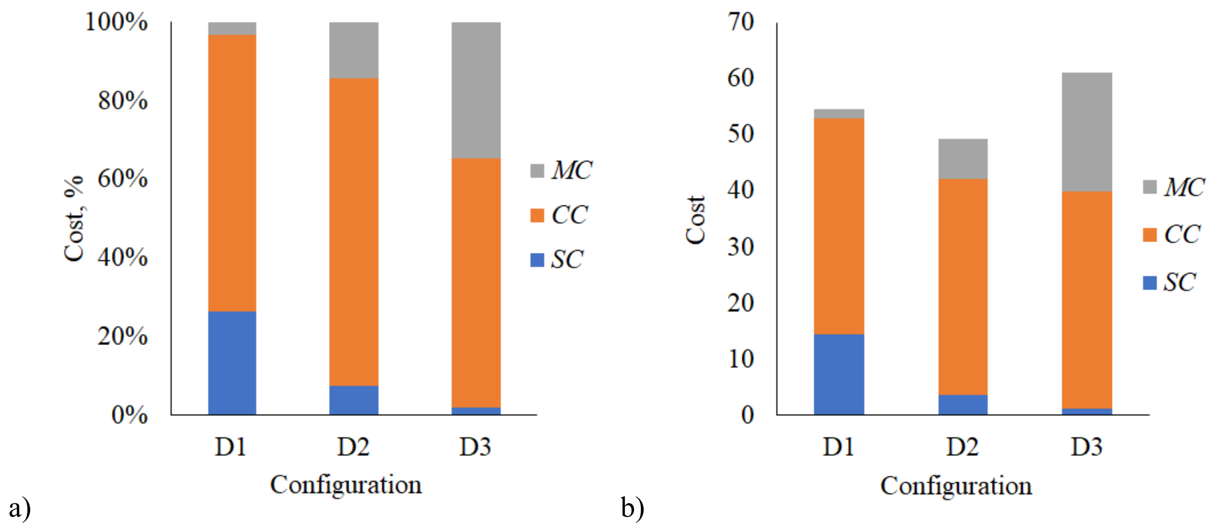

Figure 4: The share of the cost according to the configuration a) expressed as a percentage of the total cost; and b) in absolute units.

The ICT product supply chain configuration has a decreasing number of components per supplier going from D1 to D3. Figure 6 indicates that there is a nonlinear relationship between the total cost and the number of components per supplier. The flexible supplier configuration (D2) is the most resilient to the vulnerabilities. The exception is the case with very high supplier vulnerability, when D1 and D2 are equal. The supplier vulnerability obviously does not affect the D3 configuration, since every supplier failure leads to treating exactly one component. The supplier failure causes larger variations, because the event is more rare and causes more significant disruption in supply chain configuration. The observations are in line with those reported in literature that flexible supply chains are better prepared for dealing with disturbances.

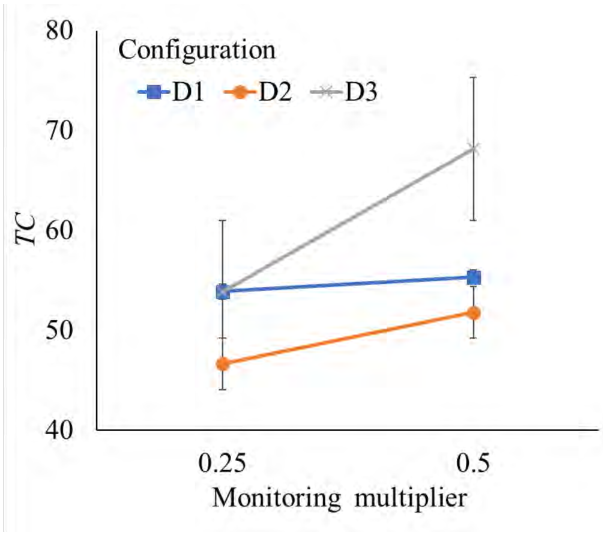

Figure 5: The total cost depending on the monitoring cost multiplier. The 95 % confidence interval is shown.

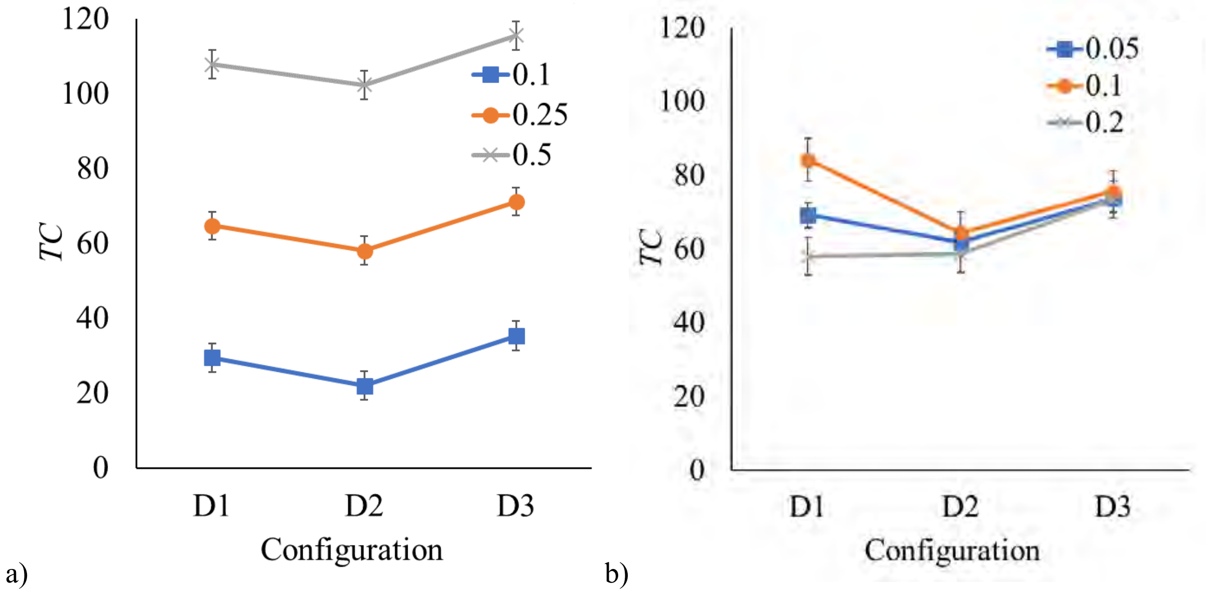

Figure 6: Total cost depending on a) component failure probability π_2; and b) supplier failure probability π_1.

In the model, there is a fixed transition point of preferring not patching to patching, and it appears late in the product life cycle. It depends on the ratio between the patching cost and the not-patching penalty. Figure 7 tracks dynamics of the patching and not-patching cost according to the time period for different experimental treatments. The cost are averaged over all simulation replications for the given time period. The patching cost increase as vulnerabilities are identified randomly in any time period. Once the patching becomes more expensive, accepting the risk of not patching, the patching cost remain constant and the not-patching penalty gradually increases. The model could be expanded to incorporate actual failures and to simulate their consequences.

Figure 8 shows the distribution of the total cost according to the patching or not-patching decision. The allocation of the cost between *PC* and *NC* does not change according to the choice of the configuration. The differences are explained by increasing *MC,* as one switches from the dominant supplier configuration to the dedicated suppliers configuration. The dedicated suppliers configuration could be highly resilient if not for the monitoring cost.

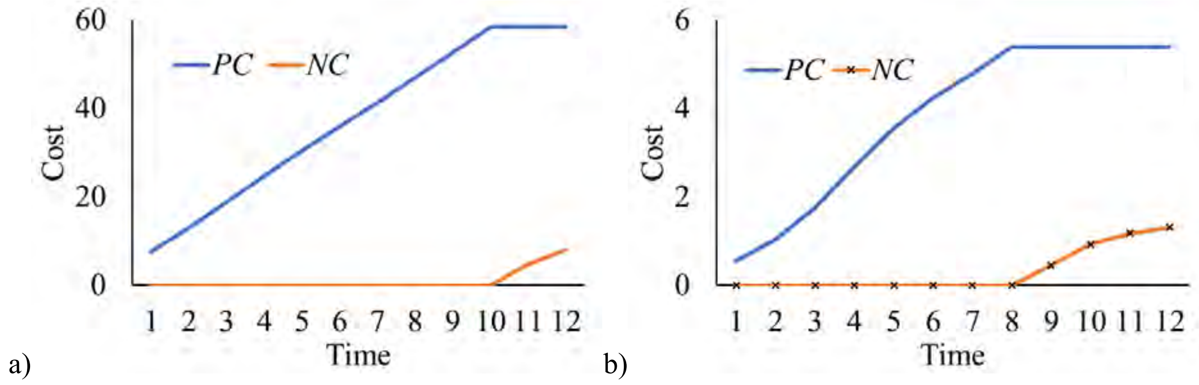

Figure 7: Dynamics of patching and not-patching cost over the life cycle; a) D1 configuration, low patching and monitoring cost; and b) D3 configuration, low patching and high monitoring cost.

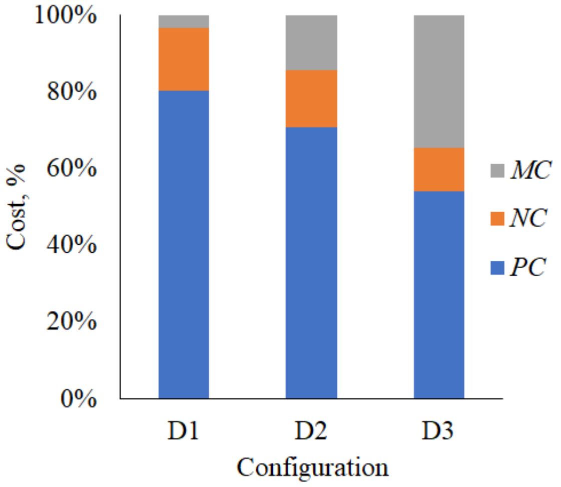

Figure 8: The distribution of the total cost according to the patching/not patching decision.

5 CONCLUSION

The ICT product supply chain resilience to cope with vulnerabilities discovered in the product's components is investigated. The ICT product supply chains are characterized by coupling among components and their suppliers and non-physical nature of many components allowing for flexible treatment of vulnerabilities by patching. Simulation is a suitable technique to evaluate the dynamic impact of disruptive events on a supply chain configuration and its resilience. It has been shown experimentally that flexible configurations are the most resilient. The supplier failures cause more significant variations in supply chain performance. This observation is of particular importance, because current trends in ICT product supply chains emphasize trustworthiness of partners in general rather than just evaluation of individual components.

The model developed is simple and makes only few assumptions about supply chain operations. The use of simulation modeling instead of analytical treatment allows for a variety of extensions. The obvious extension is a more complex supply chain configuration, though existing research suggests limited impact. More complex product structures could also be considered, because ICT products indeed have complex interdependencies among the components, which might affect the patching cost. Finally, exploitation of vulnerabilities also could be modeled, especially, to better understand relations between patching and not-patching options. Currently, all vulnerabilities are treated uniformly in the model, and an extension could be developed to represent variability in severity and complexity of these vulnerabilities. Simulation modeling is well suited for incorporation of additional stochastic factors.

The monitoring aspect is of major importance. Grabis et al. (2020) discuss using various data sources to identify product and supplier vulnerabilities. There are public repositories reporting known vulnerabilities for various components. Evaluation of the trustworthiness of suppliers is more complicated and requires analysis and combination of multiple data sources and is associated with the degree of uncertainty.

ACKNOWLEDGMENTS

The valuable comments and suggestions made by the anonymous reviewers and the track coordinators are gratefully acknowledged. This research is funded in parts by the Ministry of Education and Science, Republic of Latvia, project ARTSS, project No. VPP-COVID-2020/1-0009.

REFERENCES

Arora, V., and M. Ventresca. 2018. "Modeling Topologically Resilient Supply Chain Networks". *Applied Network Science* 3(19):1–20.

Ashbaugh, D. A. 2008. *Security Software Development: Assessing and Managing Security Risks*. Boca Raton: Auerbach Publication.

Benthall, S. 2017. "Assessing Software Supply Chain Risk Using Public Data". In *Proceedings of IEEE 28th Annual Software Technology Conference,* September 25th–28th, Gaithersburg, MD, USA, 1–5.

Carvalho, H., A. P., Barroso, V. H. MacHado, S. Azevedo, and V. Cruz-Machado. 2012. "Supply Chain Redesign for Resilience Using Simulation". *Computers and Industrial Engineering* 62(1):329–341.

Cavusoglu, H., H. Cavusoglu, and Z. Jun. 2008. "Security Patch Management: Share the Burden or Share the Damage?". *Management Science* 54(4):657–670.

Chandra, C., and J. Grabis. 2016. *Supply Chain Configuration*. 2nd ed. New York: Springer.

Cigolini, R., M. Pero, T. Rossi, and A. Sianesi. 2014. "Linking Supply Chain Configuration to Supply Chain Performance: A Discrete Event Simulation Model". *Simulation Modelling Practice and Theory* 40:1–11.

Falasca, M., C. W. Zobel, and D. Cook. 2008. "A Decision Support Framework to Assess Supply Chain Resilience". In *Proceedings of the 5th International Conference on Information Systems for Crisis Response and Management (ISCRAM)*, May 4th–7th, Washington, DC, USA, 596–605.

Gerace, T., and H. Cavusoglu. 2009. "The Critical Elements of the Patch Management Process". *Communications of the ACM* 52(8):117–121.

Grabis, J., J. Stirna, and J. Zdravkovic. 2020. "Capability Management in Resilient ICT Supply Chain Ecosystems", In *Proceedings of the 22nd International Conference on Enterprise Information Systems,* May 5th–7th, Prague, The Czech Republic, 393–400.

Gran, T., and M. Grunow. 2016. "Concurrent Product and Supply Chain Design: A Literature Review, an Exploratory Research Framework and a Process for Modularity Design". *International Journal of Computer Integrated Manufacturing* 29(12):1255–1271.

Goldbeck, N., P. Angeloudis, and W. Ochieng. 2020. "Optimal Supply Chain Resilience with Consideration of Failure Propagation and Repair Logistics". *Transportation Research Part E: Logistics and Transportation Review*133:1–20.

Gunasekaran, A., N. Subramanian, and S. Rahman. 2015. "Supply Chain Resilience: Role of Complexities and Strategies". *International Journal of Production Research* 53(22):6809–6819.

Hasan, M. M., D. Jiang, A. M. M. S. Ullah, and M. Noor-E-Alam. 2020. "Resilient Supplier Selection in Logistics 4.0 with Heterogeneous Information". *Expert Systems with Applications* 139:1–24.

Hearnshaw, E. J. S., and M. M. J. Wilson. 2013. "A Complex Network Approach to Supply Chain Network Theory". *International Journal of Operations and Production Management* 33(4):442–469.

Heidelberger, P., and P. D. Welch. 1983. "Simulation Run Length Control in the Presence of an Initial Transient". *Operations Research*.31:1109–1144.

Kshetri, N., and J. M. Voas. 2019. "Supply Chain Trust". *IT Professional* 21(2): 6–10.

Last, D. 2015. "Using Historical Software Vulnerability Data to Forecast Future Vulnerabilities". In *Proceedings – 2015 Resilience Week, RSW 2015*, August 18th–20th, Philadelphia, PA, USA.

Lu, T., X. Guo, B. Xu, L. Zhao, Y. Peng, and H. Yang. 2013. "Next Big Thing in Big Data: The Security of the ICT Supply Chain". In *Proceedings of the International Conference on Social Computing,* September 8th–14th, Alexandria, VA,USA, 1066–1073.

Macdonald, J. R., C. W. Zobel, S. A. Melnyk, and S. E. Griffis. 2018. "Supply Chain Risk and Resilience: Theory Building through Structured Experiments and Simulation". *International Journal of Production Research* 56(12):4337–4355.

Mari, S. I., Y. H. Lee, and M. S. Memon. 2015a. "Complex Network Theory-based Approach for Designing Resilient Supply Chain Networks". *International Journal of Logistics Systems and Management* 21(3):365–384.

Mari, S. I., Y. H. Lee, M. S. Memon, Y. S. Park, and M. Kim. 2015b. "Adaptivity of Complex Network Topologies for Designing Resilient Supply Chain Networks". *International Journal of Industrial Engineering: Theory, Applications and Practice* 22(1):102–116.

Massacci, F., and V. H. Nguyen. 2014. "An Empirical Methodology to Evaluate Vulnerability Discovery Models". *IEEE Transactions on Software Engineering* 40(12):1147–1162.

Pariazar, M., and M. Y. Sir. 2018. "A Multi-Objective Approach for Supply Chain Design Considering Disruptions Impacting Supply Availability and Quality". *Computers and Industrial Engineering* 121:113–130.

Perera, S., M. G. H. Bell, , and M. C. J. Bliemer. 2017. "Network Science Approach to Modelling the Topology and Robustness of Supply Chain Networks: A Review and Perspective". *Applied Network Science* 2(33):1–25.

Pero, M., T. Rossi, C. Noé, and A. Sianesi. 2010. "An Exploratory Study of the Relation between Supply Chain Topological Features and Supply Chain Performance". *International Journal of Production Economics* 123(2):266–278.

Polatidis, N., M. Pavlidis, and H. Mouratidis. 2018. "Cyber-attack Path Discovery in a Dynamic Supply Chain Maritime Risk Management System". *Computer Standards and Interfaces* 56:74–82.

Shekarian, M. and M. Mellat Parast. 2020. "An Integrative Approach to Supply Chain Disruption Risk and Resilience Management: A Literature Review". *International Journal of Logistics Research and Applications,* in press.

Tukamuhabwa, B. R., M. Stevenson, J. Busby, and M. Zorzini. 2015. "Supply Chain Resilience: Definition, Review and Theoretical Foundations for Further Study". *International Journal of Production Research* 53(18):5592–5623.

Wang, J., R. R. Muddada, H. Wang, J. Ding, Y. Lin, C. Liu, and W. Zhang. 2016. "Toward a Resilient Holistic Supply Chain Network System: Concept, Review and Future Direction". *IEEE Systems Journal* 10(2):410–421.

Yao, X., and R. Askin. 2019. "Review of Supply Chain Configuration and Design Decision-making for New Product". *International Journal of Production Research* 57(7):2226–2246.

Zhao, K., K. Scheibe, J. Blackhurts, and A. Kumar. 2018. "Supply Chain Network Robustness Against Disruptions: Topological Analysis, Measurement, and Optimization". *IEEE Transactions on Engineering Management* 66(1):127–139.

AUTHOR BIOGRAPHY

JĀNIS GRABIS is a Professor at the Faculty of Computer Science and Information Technology, Riga Technical University, Latvia. He obtained his PhD from the Riga Technical University in 2001 and worked as a Research Associate at the College of Engineering and Computer Science, University of Michigan-Dearborn. He has published in major academic journals including OMEGA, European Journal of Operational Management, International Journal of Production Research, Computers & Industrial Engineering and others. He has been a guest-editor for two top academic journals and member of the program committee of several academic conferences. Janis Grabis has co-authored a monograph on supply chain configuration published by Springer. His research interests are in supply chain management, enterprise applications and project management. His email address is grabis@iti.rtu.lv.