ISBN 13 978-952-5183-62-7

Tuomo Sipola*, Tero Kokkonen, Markku Puura, Kalle-Eemeli Riuttanen, Kari Pitkäniemi, Elina Juutilainen, and Teemu Kontio

Digital Twin of Food Supply Chain

Abstract: Food supply chain is one of the most critical parts of a modern society. Consequently, cybersecurity of the supply chain is a major concern as new threats emerge. Cyber ranges can be used to prepare for such cybersecurity threats by creating realistic scenarios mirroring real-world setups. The aim of this study is to describe a digital twin of the food supply chain built for a cyber range. This descriptive case study explains the general capabilities of the digital twin and its use in the cyber range environment. Creation of a digital twin enables the use of cyber ranges to train organisations related to the food supply chain.

Keywords: cybersecurity, digital twin, critical systems, food supply chain

***Corresponding Author: Tuomo Sipola:** Jamk University of Applied Sciences, E-mail: tuomo.sipola@jamk.fi
Tero Kokkonen: Jamk University of Applied Sciences, E-mail: tero.kokkonen@jamk.fi
Markku Puura: Jamk University of Applied Sciences, E-mail: markku.puura@jamk.fi
Kalle-Eemeli Riuttanen: Jamk University of Applied Sciences, E-mail: kalle-eemeli.riuttanen@jamk.fi
Kari Pitkäniemi: Jamk University of Applied Sciences, E-mail: kari.pitkaniemi@jamk.fi
Elina Juutilainen: Jamk University of Applied Sciences, E-mail: elina.juutilainen@jamk.fi
Teemu Kontio: Jamk University of Applied Sciences, E-mail: teemu.kontio@jamk.fi

1 Background and Aims

In the modern digitalised food supply chain, cyber security has an extremely important role. Food supply chain consists of food production, processing, distribution and retail. Such systems include traditional and modern internet of things (IoT) devices. An effective solution to enhance the knowledge and skills of staff members against cyber threats is the cyber security exercise where the learning audience train their skills with a realistic scenario and technical infrastructure mimicking required systems and networks [7]. Such technical infrastructure is called cyber range and/or cyber arena.

Karjalainen and Kokkonen introduce requirements for cyber arena environments [6]: (i) Realism, (ii) Isolated and controlled environment, (iii) Internet simulation, (iv) User and network traffic generation, (v) Attack execution and simulation, (vi) Organisations' infrastructures, (vii) Collaboration and (viii) Planning, executing, monitoring and analysing.

According to Gartner Glossary of information technology [2] *"A digital twin is a digital representation of a real-world entity or system."* It states that a digital twin is implemented as a software object or model mirroring the real-world object. Cyber arena can be realised as a digital twin, which satisfies the requirements set by cyber security exercises. Themes related to digital twins such as physical and virtual processes, and virtual environments [5] are relevant in the cyber arena.

This study aims to describe the implementation of Food Production Cyber Arena, which meets the eight high-level requirements mentioned above. Studies such as Alim et al. [1] have implemented digital twins with physical testbeds to mirror farmland canal systems. However, in the present case study a complete digital twin of the food supply chain is described. This digital representation facilitates the creation of a simulated supply chain for a cyber exercise aimed at organisations working in the domain of food production and processing. For example, food production companies could exercise their response to cyber attacks targeted at critical points in their processes. A cyber exercise in the food supply domain could include participants from a food processing factory. Staff members from departments such as management, communications and operations participate. The scenario includes a cyber attack to the factory, to which the participants should react. The resolution of the problem will provide resilience information to the departments.

2 Building the Digital Twin

Institute of Information Technology at Jamk University of Applied Sciences hosts a cyber security, artificial intelligence and data-analytics focused research, development and training center called JYVSECTEC (Jyväskylä Security Technology). Since 2011 JYVSECTEC has implemented and maintained cyber arena known as RGCE (Realistic Global Cyber Environmet) [4]. RGCE has been implemented piece by piece during various research and development projects.

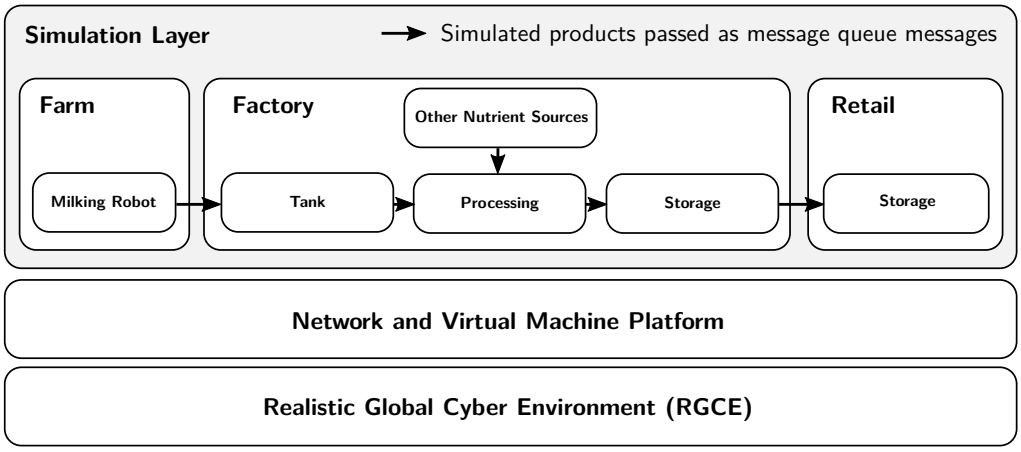

Fig. 1. Food supply chain simulation building blocks.

In the ongoing project *Food Chain Cyber Resilience*, critical food production infrastructure is mimicked as a digital twin for cyber security exercises for food production organisations [3].

Fig. 1 illustrates the setup of the food supply chain simulation. The simulation was mainly implemented using Node.js runtime environment. The various services run on virtual machines in containers on the Virtual Machine Platform. The services communicate via the (virtual) network. Messages are passed using REST APIs or mock-ups of protocols such as Modbus. Such messages are usually formatted as JSON.

The supply chain itself is modeled as (i) machines representing the various machines and storages in the supply chain and (ii) messages that are passed from one machine to another. Machines can represent, e.g., milking robots, food processing machines and packaging machines. The products passed from machine to machine are simulated using the Bull queue system for Redis. These messages contain the relevant domain information, e.g., a message could contain the amount of milk in litres, and metadata, such as the measurement unit.

3 Conclusion

The use of digital twins of domain systems as part of cyber exercises improves the immersivenes by simulating the real supply chains. This way the participants can exercise in a realistic environment, which mirrors the systems and processes in their ordinary work. Implementing the digital twin requires modular design with appropriate messaging simulating the real-world counterparts. Further research includes the full validation of the system as part of a real cyber exercise.

Acknowledgment

Funded by the Regional Council of Central Finland/Council of Tampere Region with fund of Leverage from the EU, European Regional Development Fund (ERDF), Recovery Assistance for Cohesion and the Territories of Europe (REACT-EU). Implemented as part of the *Food Chain Cyber Resilience* project.

References

[1] M. E. Alim, S. R. Wright, and T. H. Morris. A laboratory-scale canal scada system testbed for cybersecurity research. In *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pages 348–354, 2021. doi:10.1109/TPSISA52974.2021.00038.

[2] Gartner, Inc. Gartner Glossary, 2022. URL: https://www.gartner.com/en/information-technology/glossary/digital-twin.

[3] Jamk University of Applied Sciences, Institute of Information technology / JYVSECTEC. Food chain cyber resilience, 2022. URL: https://jyvsectec.fi/2021/09/food-chain-cyber-resilience/.

[4] Jamk University of Applied Sciences, Institute of Information technology / JYVSECTEC. Realistic global cyber environment (RGCE), 2022. URL: https://www.jyvsectec.fi/rgce.

[5] D. Jones, C. Snider, A. Nassehi, J. Yon, and B. Hicks. Characterising the digital twin: A systematic literature review. *CIRP Journal of Manufacturing Science and Technology*, 29:36–52, 2020. doi:10.1016/j.cirpj.2020.02.002.

[6] M. Karjalainen and T. Kokkonen. Comprehensive cyber arena; the next generation cyber range. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pages 11–16, 2020. doi:10.1109/EuroSPW51379.2020.00011.

[7] T. Kokkonen, J. Päijänen, and T. Sipola. Multi-national cyber security exercise, case Flagship 2. In *14th International Conference on Education Technology and Computers (ICETC 2022)*, page 7, 2022. doi:10.1145/3572549.3572596.