Handling interconnected cascading Risks: an interoperable holistic Framework

John Wondoh[1,2,*], Karamjit Kaur[1,2], Matt Selway[1,2], Mansi Patel[1,2], Andrew McRae[3], Georg Grossmann[1,2], Markus Stumptner[1,2], Don Sands[3] and Alan Johnston[4]

[1]*Industrial AI Research Centre, University of South Australia STEM, Australia*

[2]*Future Energy Exports Cooperative Research Centre, Perth, Australia*

[3]*Synengco Pty Ltd, Queensland, Australia*

[4]*MIMOSA, Tuscaloosa, Alabama, USA*

[1]*firstname.lastname@unisa.edu.au*

[3]*firstname.lastname@synengco.com*

[4]*atjohn@mimosa.org*

Abstract

In critical industries such as Energy or Defense that consists of complex interconnected systems, risks generally do not occur in isolation and are dynamic in nature. Traditional risk management frameworks do not possess the capability to reflect the cumulative effect of dynamic interconnected risks. Whilst the individual risks arising at component level from an asset health monitoring may not be regarded as significant based on their likelihood and impact, the assessment may be completely different when this analysis is aggregated and cascaded to the system level by assessing the connected components. The inability to assess the cascading impact of risk events within and across the system boundary as well as across the different levels and types of risks is hampering decision makers to produce effective decisions that can control the expected risks and identify emergent risks.

Within a complex system, multiple analytical models and techniques can be employed to perform analysis on a component for different contexts such as reliability, efficiency and safety. For example, health and monitoring systems generate risk events based on an asset's health which are assessed by risk models for their impact. The assessments produced by individual risk models need to be shared and propagated across siloed systems and multiple system levels in the hierarchy in an interoperable manner. We provide details of a framework which can enable organisations to attain a holistic view of the system, by sharing the outputs produced by various risk models and analysis methods in a standard format that can be used by other risk models and systems. An extra layer of assessment can thus be performed on top of existing independent analysis, that can empower organizations to have a more coherent and comprehensive view of their asset status. This is essential to avoid potentially major oversights across the systems engineering lifecycle.

Keywords: cascading risk, interconnected risk, interoperable analytics, risk model.

Introduction

Risk management is necessary for the reliable operation of large-scale critical infrastructure, including energy and defense infrastructure and ecosystems. These infrastructures are characterised by their complex structures, which typically consist of an aggregation of systems operating within and across organisational units [1]. In addition, an engineering infrastructure may interact with external systems by contracting their ability to satisfy operational goals. Therefore, critical engineering infrastructures must be robust and uninterruptedly provide their functions.

Due to their complex structures and interactions, critical infrastructures are prone to disruptive failures resulting from cascading failures if risks are not detected early, their impact evaluated and mitigated before their actual occurrence [2,3]. The operational independence property of each system in a System-of-Systems [12] suggests that a dependency between two systems may have had less design effort and precision than the dependencies between each element of a single system, as the systems were designed separately and only coupled later. Comprehensive risk management within each system or organisational unit is insufficient to avoid cascading disruptive failures since several complex interactions must be accounted for. Therefore, risk management in critical engineering infrastructure cannot be performed entirely in silos but must be propagated and consolidated for better large-scale analysis and mitigation. There is a need for interoperable risk analytics that consider risk information from other systems for a more holistic and broader risk impact perspective.

Our work provides an open specification for interoperable risk analytics. The final specification will be made publicly available on the MIMOSA website[1] to make it easy to adopt and improve. The primary artifact for facilitating interoperability among Risk Management Systems (RMSs) is the risk event. This event provides descriptive attributes about a given identified risk and its impact. We say a risk event can be used for interoperability, as well as to facilitate risk analytics if it has the following characteristics:

- It provides risk properties necessary for analysis by other RMSs.
- It can be evaluated and validated with evidence.
- It can facilitate the synthesis of treatment actions based on recommendations seamlessly.

We demonstrate the use of the specified interoperable risk events with a use case example. We show that regardless of the complex nature of critical engineering infrastructure, interoperability can be achieved either through hierarchical systems across organisational units or entirely between organisations with separate interests and functions. Furthermore, less complex systems can also benefit from risk interoperability to improve their overall performance and resilience.

Problem & Approach Overview

Infrastructure is a network of actors, systems, and processes that operate collectively to provide some functionality. The actors can be people, industries, and organisations. Infrastructure is critical if its smooth operation is essential for a nation's economy or defence [6]. For instance, a power plant's failure to produce electric power significantly affects a country's economy. Risk assessment and impact analysis at a large scale are, therefore, paramount to the smooth operation of these systems. In Example 1, with a simple illustration, we show why risk management should not be performed in isolation but should collaboratively interoperate with other RMSs to facilitate a holistic impact analysis and decision-making.

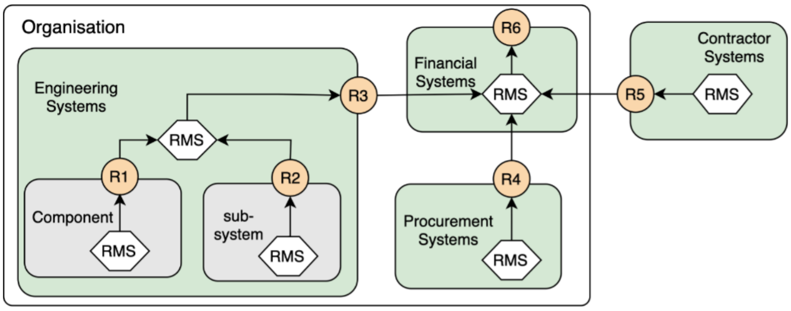

Figure 1 RMS Interactions within and outside an organization (The RMS is not necessarily contained within each component, only that there is some RMS responsible for it.)

Example 1. The example in Figure 1 provides a scaled-down illustration of RMS interactions in engineering infrastructure. These interactions are facilitated primarily by risk events, labelled R1 to R6. Each RMS is associated with at least one infrastructure participant, e.g., a

[1] http://www.mimosa.org

component, subsystem, or system. In addition, external participants, e.g., contractors, have their associated RMSs that the larger system must consider. For example, assume the risk of failure for a given component has increased significantly; the RMS associated with it updates its risk properties. A risk event for the component is then generated with the updated risk data. The RMS associated with the engineering system consumes this risk event and assesses it, along with information about all other operational assets. Consequently, each RMS will receive new risk data, propagated from the component and cascaded hierarchically within and horizontally across interacting organisations (considering the contractor systems).

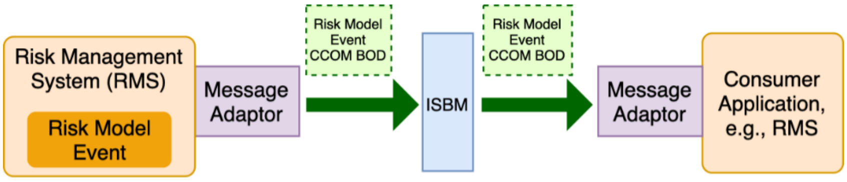
Risk Management System (RMS)
Risk Model Event
Message Adaptor
Risk Model Event CCOM BOD
ISBM
Risk Model Event CCOM BOD
Message Adaptor
Consumer Application, e.g., RMS

Figure 2 Risk Interoperability Approach Overview

The example described above is currently only possible at a limited scale within an organization. To perform risk analytics at a large scale across several systems, RMSs must be capable of interoperability. This capability is limited due to the divergent definitions of risk, leading to several specifications for risk events. Each risk event must capture the properties of a risk in a meaningful way so that it is interpretable by other systems that consume it. In Figure 2, we show an overview of how the risk events can be used to facilitate RMS interoperability. A publish-subscribe approach has been adopted to facilitate the sharing of risk event information by RMSs, allowing RMSs and other interested systems to receive updated risk information on an event-driven basis. The implementation specification for the publish-subscribe platform adopted in this work is the OpenO&M ISBM [1]. RMSs can publish and consume risk events based on channel configuration and permitted access. The message adaptor transforms the internal data of different RMSs, or their managed Risk Models, to a standard data exchange format for communication.

Risk Event Specification

We provide an open specification for risk events to aid in RMS interoperability. This specification describes a flexible metamodel for defining a risk event's structure, considering the various systems and actors that produce and consume this event. To ensure that the proposed metamodel is suitable for large-scale engineering systems, we evaluated several existing risk modelling and analytics techniques [7,8,9,4,5] to determine the general requirements of a risk event. The evaluation focused on the kinds of output expected from RMSs, the requirements for interoperable risk analytics, and the minimal data content required by an external system for decision-making. While our specification focuses on risk events for engineering infrastructure, it is flexible enough to represent risk events with various levels of detail for organisations, people, systems, and components. Figure 3, provides the open risk event metamodel suitable for large-scale critical engineering infrastructure.

The risk event is the central artifact in this metamodel. It interacts with two essential artifacts, i.e., the RMS and the function. The RMS uses risk model(s) to produce and publish risk events. The input data required by the risk models may include other risk events, historical data, and operational data about the assets or actors. We define a function as services or goods that an asset or actor provides while in operation. The risk event is associated with some function, such that it can disrupt the provision of the function if the risk is not mitigated. Each risk event is associated with a specific risk type. There are several risk types, including the *risk of failure* and *risk of change*, associated with the management and operation of critical engineering infrastructure. No specific taxonomy of risk types is included in the metamodel to allow for flexible risk event specification. The risk type is essential because the system that consumes the risk event will process it based on its associated type. Note that the risk types within a given domain must be consistent with the ontology of that domain. A risk event can be composed of, or causally linked to, other risk events, e.g., higher-level events, such as system-level events, can be composed of several components and subsystem risk events.

A risk event has mandatory properties which form its core properties. These properties must be included for every type of risk event and every level within the hierarchy of risk events. The core properties are the minimum data content required for the risk event evaluation and analysis, along with the risk type and the function affected by the risk. These properties consist of the probability and impact of the risk event. The *probability* property captures the *probability value(s)*, the *time horizon* within which the probability value remains valid, and the *confidence* (or uncertainty) associated with the probability. The *impact* captures information about how the system or organisation will be affected by the risk event if it is not handled. Like the probability property, it captures the impact value, the time horizon, and confidence. In commercial organizations, the impact is typically measured in monetary terms.

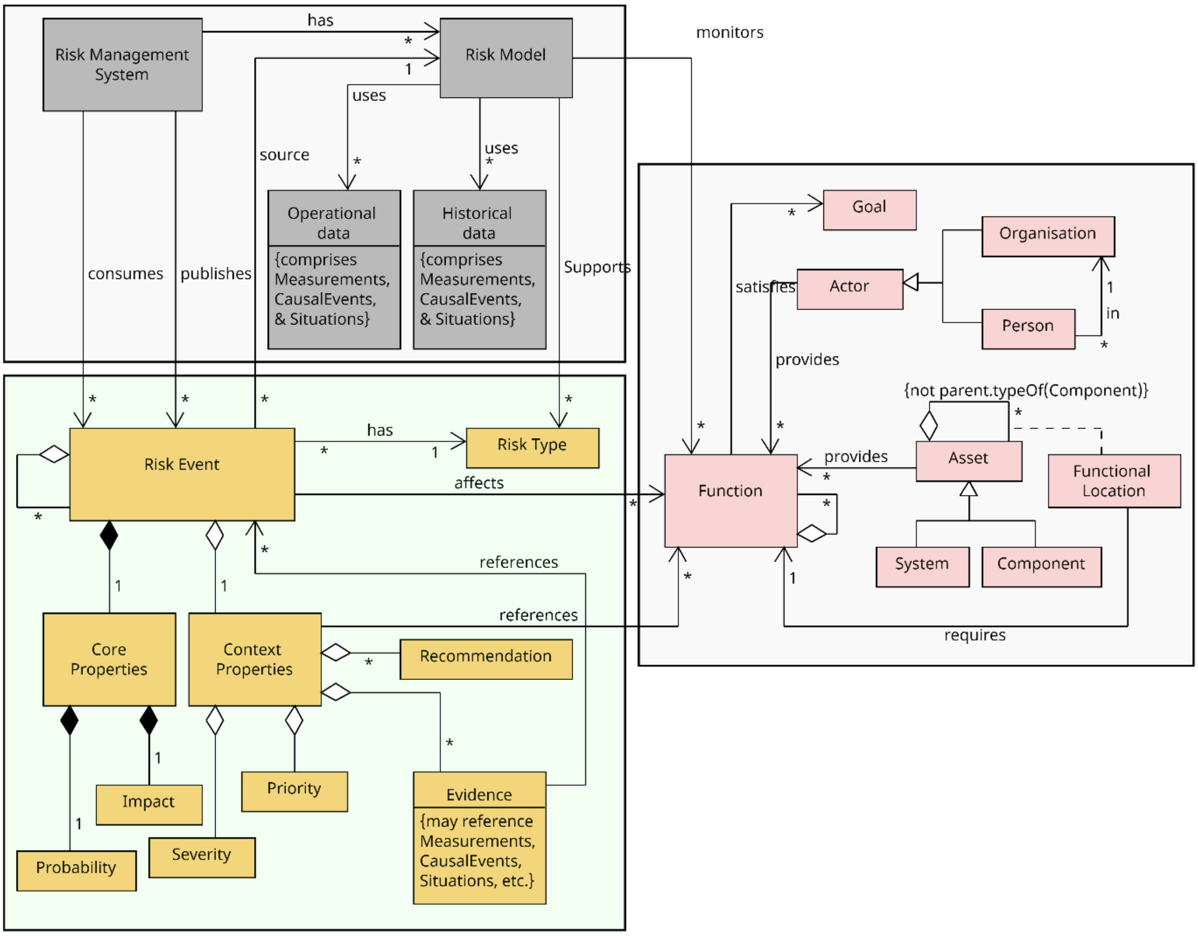

Figure 3 Risk event metamodel

Additional properties necessary to understand and process the probability and impact of a risk event are captured within the context properties of the risk event. While context properties are not mandatory, their inclusion within the risk event specification is encouraged. We discuss these context properties shown in Figure 3 below:

- *Severity Level*: Numeric estimate of the severity of the risk impact of the event.
- *Priority Level*: Numeric estimate of the priority to which the event should be addressed.
- *Evidence, Measurement, Situation*: The evidence is necessary to validate and verify risk events by other systems. The evidence can be associated with any causal properties that led to the production of the risk event, including measurements or other risk events.

- *Function*: Information about the providers of the function and their structure may be included in the context properties of the risk event. A component's identifier and functional location may be included to identify it uniquely. For a system, its identifier and breakdown structure may be included.
- *Recommendation*: This includes the treatment action or advisory on how the risk event should be handled.

RMS Interoperability

We adopt the Open Industrial Interoperability Ecosystem (OIIE) architecture (published as part of ISO/TS 18101-1:2019) which provides an interoperability solution enabling systems to communicate effectively in both inter- and intra- enterprise contexts using a variety of standards, data models, and exchange protocols [10]. Hence, we leverage a standards-based approach for achieving interoperability, as opposed to traditional methods that can be expensive and fragile. In addition, one benefit of a standards-based approach is its suitability for complex critical infrastructures that require multiple applications to manage their associated systems.

Using Risk Events

Risk events are shared with other RMSs and decision support applications via a publish-subscribe mechanism of standards-based messaging middleware. An essential benefit is that it increases scalability since all explicit dependencies between producers and consumers are eliminated [11]. The participants of risk interoperability are:

- The publisher(s), which include the RMSs and other systems providing inputs to the RMSs and their risk models.
- The consumer(s), which may be an RMS or any decision support system.
- A standards-based messaging middleware with publish-subscribe capability.

We use a messaging middleware conforming to the OpenO&M ISBM specification, part of the OIIE specifications. It is a vendor-neutral, supplier-neutral standard based on the ISA-95 Part 6 Messaging Service Model standard suitable for facilitating interoperability in a neutral way between applications or systems. The risk event transmitted on the ISBM must be converted to a valid information model. We use the MIMOSA CCOM (Common Conceptual Object Model) information model[2]. In particular, the risk event is structured as a CCOM Business Object Document (BOD)[3], the exchange model for the ISBM. Risk events generated by an RMS must be transformed appropriately to a CCOM BOD to ensure that the consumer can interpret and use the data. Each risk event property is converted to an equivalent CCOM representation, e.g., the *impact* and *confidence* are represented as CCOM's *Measure* and *Probability* data types.

To minimise the effort required to structure risk event messages by RMSs, an adaptor can be implemented to perform the transformation before publication. Similarly, adaptors are required on the consumer end if the message needs to be transformed from a CCOM BOD to a format more suitable for the consumer. The advantage of using the ISBM and CCOM BOD is that they provide an open interface that facilitates interoperability among industrial applications and systems through structured communication.

Use case

This approach has been used in the Future Energy Exports[4] (FEnEx) CRC towards interoperable Industry 4.0 technologies in LNG and hydrogen export plants. In our example use case, we considered the risk associated with motors within a *gas well system*. We considered how risks from components, specifically motors, of the well system could affect other systems within the

[2] https://www.mimosa.org/mimosa-ccom/

[3] https://www.mimosa.org/mimosa-ccom/ccom-bod-structure/

[4] https://www.fenex.org.au/research-areas/digital-technologies-and-interoperability/

organisation, such as the production and procurement management systems. The measurements and operating conditions of the motors are monitored and provided by the *Condition Monitoring System* (CMS). This system provides data such as vibrations and other measurements that can be used to evaluate the motor's failure risk. The *Procurement Management System* (PMS) is also involved in the use case to procure a replacement motor.

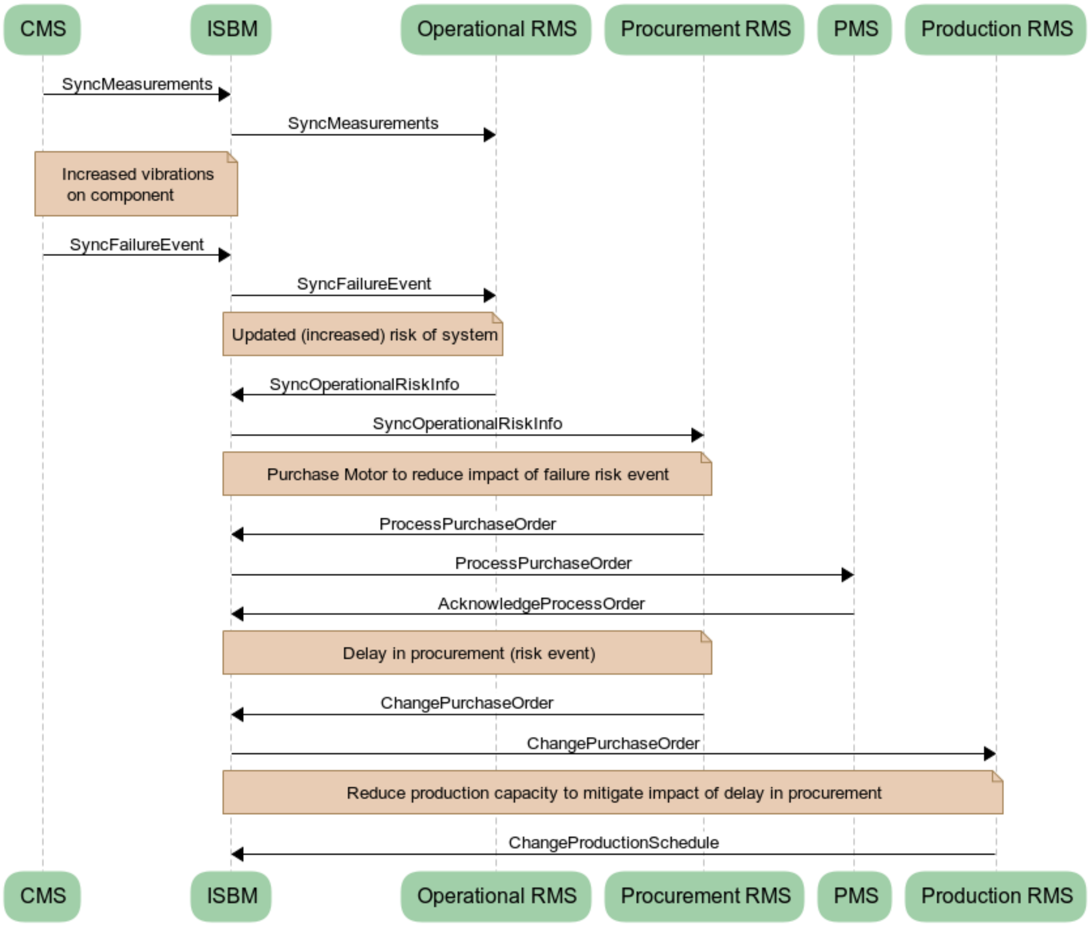

Figure 4 RMS interoperability risk event communication sequence

The sequence of messages exchanged through the ISBM to demonstrate the use case is shown in Figure 4, which also maps to the propagation illustrated in Figure 1. When the CMS detects excessive vibrations on a Motor, it publishes a failure risk event on the ISBM. The Operational RMS consumes the event and determines the impact of the motor's failure on the overall well system. The analysis performed by the Operational RMS is published over the ISBM for further analysis by other RMSs. For example, the Procurement RMS would generate a recommendation to procure a replacement motor to mitigate the impact of motor failure on the overall system. Based on this recommendation, the PMS will send a purchase order to potential vendors, one of which will be accepted with the promise to supply the motor by the required date. Suppose the risk of a delivery day increases which may prevent the motor from arriving on time due to supply chain issues. This risk is published on the ISBM by the PMS. The Production RMS will pick up this delay risk event and generate an advisory to change (reduce) the production schedule. The use case thus showcases how the risk events produced from various types of risk models deployed in an organization are propagated to other risk models to obtain an integrated risk profile at the enterprise level.

Conclusion and Future Scope

Traditional risk management frameworks do not possess the capability to reflect the cumulative effect of interconnected risks in the absence of interoperable analytics. Whilst individual risks at the component level may not be regarded as significant based on their likelihood and impact, the assessment may differ entirely when analyses are aggregated and cascaded to the system level by assessing the connected components. A holistic view of the entire system can empower decision-makers to bring advancements and competitiveness to the industry. To attain this holistic view, the output produced from each of the available analysis methods should be encoded in a format that can be shared and used by other analysis methods. This paper presents a conceptual model for representing risk events to facilitate interoperable risk analytics for large-scale engineering systems. We also provided a methodology that can be adopted for sharing risk vertically and horizontally across organisations and systems.

Acknowledgements

The work has been supported by the Future Energy Exports CRC (www.fenex.org.au) whose activities are funded by the Australian Government's Cooperative Research Centre Program. This is FEnEx CRC Document 2022/20.RP3.0048-FNX-009.

References

1. Zio, E 2016, ‘Challenges in the vulnerability and risk analysis of critical infrastructures’, *Reliability Engineering & System Safety*, vol. 152, pp. 137–150.
2. Dueñas-Osorio, L & Vemuru, SM 2009, ‘Cascading failures in complex infrastructure systems’, *Structural Safety*, vol. 31, no. 2, pp. 157–167.
3. Pederson, P, Dudenhoeffer, D, Hartley, S & Permann, M 2006, ‘Critical infrastructure interdependency modeling: a survey of US and international research’, *Idaho National Laboratory*, 25, p.27.
4. Fang, C, Marle, F, Zio, E & Bocquet, J-C 2012, ‘Network theory-based analysis of risk interactions in large engineering projects’, *Reliability Engineering & System Safety*, vol. 106, pp. 1–10.
5. Fu, Y, Li, M & Chen, F 2012, ‘Impact propagation and risk assessment of requirement changes for software development projects based on design structure matrix’, *International Journal of Project Management*, vol. 30, no. 3, pp. 363–373.
6. Rinaldi, SM, Peerenboom, JP, & Kelly, TK 2001, ‘Identifying, understanding, and analyzing critical infrastructure interdependencies’. *IEEE control systems magazine, 21*(6), pp.11-25.
7. El Yamami, A, Ahriz, S, Mansouri, K, Qbadou, M & Illoussamen, E 2017, ‘Representing IT Projects Risk Management Best Practices as a Metamodel’, *Engineering, Technology & Applied Science Research*, vol. 7, no. 5, pp. 2062–2067.
8. Franch, X, Kenett, R, Mancinelli, F, Susi, A, Ameller, D, Annosi, MC, Ben-Jacob, R, Blumenfeld, Y, Franco, OH, Gross, D & López, L 2015, ‘The RISCOSS platform for risk management in open source software adoption’, *In IFIP International Conference on Open Source Systems*, pp. 124-133.
9. Kamissoko, D, Marmier, F & Gourc, D 2016, ‘Project risk management conceptual model’, *3rd International Conference on Logistics Operations Management (GOL).*
10. Kaur, K, Selway, M, Grossmann, G, Stumptner, M & Johnston, A 2018, ‘Towards an open-standards based framework for achieving condition-based predictive maintenance’, *Proceedings of the 8th International Conference on the Internet of Things*, pp. 1-8.
11. Eugster, PTh, Felber, PA, Guerraoui, R & Kermarrec, A-M 2003, ‘The many faces of publish/subscribe’, *ACM Computing Surveys*, vol. 35, no. 2, pp. 114–131.
12. SEBoK Authors. "System of Systems (SoS) (glossary)." in SEBoK Editorial Board. 2022. The Guide to the Systems Engineering Body of Knowledge (SEBoK), v. 2.7, R.J. Cloutier (Editor in Chief). Hoboken, NJ: The Trustees of the Stevens Institute of Technology. Accessed 2022-10-26. www.sebokwiki.org