Human Factors, Architecture, Sustainable Urban Planning and Infrastructure, Vol. 229, 2026, 128–137
https://doi.org/10.54941/ahfe1007961

Human-Centered Risk Scenario Modelling for Urban and Infrastructure Resilience

Taivo Kangilaski and Jaanus Kaugerand

Tallinn University of Technology, Ehitajate tee 5, 19086, Estonia

ABSTRACT

Cities and infrastructure networks are increasingly exposed to interconnected risks that propagate across physical, digital and organizational boundaries. Traditional risk registers and isolated analyses do not capture this dynamic and multi-domain behavior. This paper proposes a human-centered risk scenario modelling methodology that integrates process logic, spatial dependencies, human roles and regulatory constraints into a unified architectural framework. The approach extends classical bow-tie analysis, introduces modular behavioral structures and applies human-factors principles, particularly situational awareness, to interpret evolving risk conditions. A prototype implementation demonstrates how the methodology can be embedded in an enterprise architecture environment to support coherent scenario reasoning. The proposed method provides a conceptual foundation for strengthening urban resilience through clearer causal understanding, improved situational awareness and more informed decision-making.

Keywords: Human-centered risk modelling, Scenario-based analysis, Urban and infrastructure resilience

INTRODUCTION

Urban environments depend on tightly interlinked socio-technical systems. Heating networks rely on electricity and ICT, evacuation capacity depends on building layout and communication, and water, gas and power infrastructures share spatial corridors and maintenance resources. As these interdependencies intensify, risks become more complex: a single disturbance, such as a fire, pipeline rupture or ICT outage, can cascade across domains and challenge operators' ability to anticipate and respond effectively.

Human-factors research, particularly Endsley's situational awareness model (1995), shows that resilience depends not only on technical reliability but also on how well people perceive system states, comprehend their significance and anticipate future developments under stress (Teichmann et al., 2023). Infrastructures are operated and restored by people whose decisions rely on information clarity, visibility of dependencies and interpretable system behaviour.

Current risk management approaches remain largely static. Risk registers typically list hazards and consequences without modelling how events evolve or interact, while bow-tie diagrams tend to represent isolated cause–effect relations without accounting for spatial propagation, resource constraints

Received February 3, 2026; Revised April 15, 2026; Accepted April 29, 2026; Available online July 20, 2026

or cross-domain interactions. Although scenario-based analyses are used in sectors such as energy, water and ICT, they are often siloed and weakly integrated with process architectures or compliance frameworks.

This paper addresses these limitations by proposing a human-centered risk scenario modelling methodology that integrates causal logic, spatial relations, organizational roles and regulatory requirements within a unified conceptual structure. The approach strengthens situational awareness and reasoning about interdependencies, enabling analysis of how risk scenarios evolve over time. Demonstrated in the context of urban infrastructures, the contribution of this work is methodological, emphasizing conceptual integration and structural reasoning, supported by a prototype implementation embedded in an enterprise architecture environment rather than empirical validation.

RELATED WORK

Research on situational awareness and human decision-making provides an essential foundation for understanding resilience in complex socio-technical systems. Endsley's three-level model (1995) distinguishes between perception of system elements, comprehension of their meaning and projection of future states. Studies in critical infrastructure environments have shown that situational awareness is often hindered by fragmented information flows, poor visibility of dependencies and the absence of structured causal reasoning (Park et al., 2013; Ouyang, 2014; Rinaldi et al., 2001). These limitations reduce operators' ability to anticipate escalation pathways or coordinate effective responses.

Bow-tie diagrams remain widely used because they offer a clear representation of threats, barriers and consequences. However, traditional bow-ties typically represent risks as static cause–effect structures and seldom integrate spatial, organizational or temporal dimensions (de Ruijter and Guldenmund, 2016; Ionut et al., 2018). Although recent extensions of bow-tie methodology address dynamic behavior in distributed systems, they rarely incorporate human roles, regulatory constraints or process relationships in a systematic way.

Scenario-based modelling has long been recognized as a means of analyzing cascading and interdependent failures. Research on multi-domain propagation highlights that disruptions often evolve non-linearly and unpredictably (Rinaldi et al., 2001; Buldyrev et al., 2010). While these models provide insight into cross-infrastructure interactions, they are usually developed outside enterprise architecture environments. This limits their integration with organizational governance, workflows or compliance structures.

Another important stream of literature concerns the relationship between risk modelling and compliance management. Studies show a persistent gap between regulatory requirements and the modelling tools used in practice. Standards such as ISO 9001, ISO 14001, ISO 45001 and NIS2 emphasize risk-based thinking, yet organizations often struggle to operationalize these requirements coherently (Sadiq et al., 2007; Hildebrandt and López, 2024).

Earlier work by Kangilaski and Kaugerand (2024) demonstrated that enterprise architecture tools can be used to integrate risks, compliance

obligations and environmental aspects. However, that work focused on internal organizational processes rather than spatially distributed urban infrastructures. The present methodology builds upon these foundations by incorporating spatial dependencies, cross-domain interactions and dynamic scenario evolution, thereby addressing gaps identified in both human factors and risk modelling research.

METHODOLOGY

The proposed methodology integrates process structures, human roles, spatial interdependencies and regulatory constraints into a unified modelling framework. Rather than treating risks as isolated hazards, the method conceptualizes them as evolving trajectories shaped by system behavior, environmental conditions and human decision making. The methodology is organized around three principles: human centeredness, modular abstraction and scenario dynamics.

HUMAN-CENTEREDNESS

A human centered approach requires grounding the modelling effort in an accurate understanding of operational reality. The process begins with documenting business processes and workflows at a level that enables identification of hazard sources, points of failure and relevant environmental conditions. This process-oriented view ensures that risk events are identified at the locations where they realistically emerge.

Identification of risk events relies on the perspectives of experts from different organizational roles. Individuals in operational, technical and managerial positions observe different aspects of the system and therefore recognize distinct classes of threats. Involving multiple domains reduces disciplinary bias and increases the likelihood that low visibility or weak signal events are captured.

Once risk events are identified, their causal mechanisms are analyzed through established qualitative methods such as cause effect diagrams and iterative questioning. The results are synthesized into a preliminary event graph that connects events, preconditions and consequences across operational and spatial contexts. Although informative, such graphs rapidly become too complex for decision support, which motivates the introduction of abstraction mechanisms (Kangilaski, Kaugerand, 2024).

Event taxonomy and Object Reuse in the Modelling Environment

A structured event taxonomy and repository-based object reuse ensure semantic consistency across the modelling environment. In complex socio-technical systems, risk events emerge from diverse operational, spatial and organizational contexts, making uncontrolled terminology prone to semantic drift (Gruber, 1995; Uschold & Gruninger, 1996). Each risk event is therefore defined as a unique object classified by event type, causal mechanism, intensity level and domain boundary, providing a stable semantic structure across behavioural modules and scenarios.

Events are reused across process models, event graphs and scenario networks through occurrences within an enterprise architecture repository, a practice consistent with shared-repository modelling approaches (Schekkerman, 2004; White & Miers, 2008). This reuse preserves traceability, avoids duplication and enables refinements to propagate consistently throughout the modelling landscape.

Recurring use of the same event objects across different contexts reveals structural regularities in the broader event graph. Such recurring event patterns provide the empirical basis for abstraction into reusable behavioural modules, as emphasized in knowledge engineering literature (Studer et al., 1998). Together, taxonomy-based classification and object reuse form the semantic backbone of the proposed framework, supporting coherent modularization and scenario construction.

MODULAR ABSTRACTION

Because the preliminary event graph captures all identified risk events and their causal relationships, it rapidly becomes too complex to support system-level reasoning. Maintaining a single global event graph for a socio-technical system would result in limited interpretability and usability. Modular abstraction addresses this challenge by transforming detailed causal structures into manageable representations while preserving essential behavioural logic.

The abstraction process is based on identifying recurrent behavioural patterns within the event graph. Although such patterns may occur in different locations or operational contexts, their internal causal logic is structurally similar. These recurring structures are therefore grouped into behavioural families that represent generalized classes of risk behaviour.

Each behavioural family is abstracted into a reusable risk module that captures common initiation conditions, escalation pathways, intensity levels and relevant human actions without reference to any specific asset or process. Complexity is distributed across localized module sub-graphs, while modules expose only a limited set of input and output events that function as semantic interfaces for scenario construction. Context-specific attributes are intentionally omitted at this stage and introduced only during module instantiation, allowing consistent causal logic to be reused across different operational settings. These behavioural modules can be further grouped into higher-level module classes based on the dominant type of behaviour they represent.

Modular abstraction thus reduces cognitive and structural complexity while providing standardized building blocks for assembling dynamic scenario networks. By linking modules through event-level interfaces rather than maintaining a monolithic event graph, the framework enables context-sensitive scenario generation and prepares the ground for scenario dynamics. Table 1 summarizes the main module classes used in the framework, grouping individual behavioural modules according to their primary functional characteristics.

Table 1: Summary of behavioral module classes.

Module Class	Purpose	Example Modules
Physical Hazard Modules	Model the escalation of physical hazards, including energy release, structural degradation, and hazardous material behavior.	Fire Ignition and Localised Spread; Fire Escalation and Compartment Growth; Pipeline Leak & Rupture Dynamics; Structural Load Failure; Flooding and Water Ingress Dynamics
Technological & ICT Modules	Capture failures in electrical, digital, sensor, automation and communication systems, including signal delays, false alarms and system degradation.	Electrical Failure Propagation; SCADA Alert Delay; Sensor Fault & False-Negative Detection; Control System Override Failure; Power Supply Interruption
Human & Organizational Modules	Represent human perceptual, cognitive and organizational behavior including detection, misinterpretation, response delays, coordination challenges and procedure execution.	Human Detection and Interpretation; Delayed Alarm Activation; Evacuation Activation & Movement Bottlenecks; Communication Breakdown Between Agencies; Maintenance Misconfiguration
Environmental Influence Modules	Model external environmental or meteorological conditions that modify hazard propagation or system reliability.	Wind-Driven Spread; Temperature Stress; Humidity-Induced Sensor Drift; Heavy Precipitation Load; Frozen Ground or Surface Ice
Urban Interdependency Modules	Capture cross-domain dependencies between infrastructures, buildings, transportation networks, energy grids and shared operational resources.	Building Systems Interdependency; Spatial Adjacency Propagation; Cross-Infrastructure Energy Dependency; Transport Access Constraint Module; Shared Resource Bottleneck Module

From Behavioral Modules to Risk Analysis

Once behavioural modules have been derived, the system's causal structure has been sufficiently abstracted to support systematic risk evaluation. While modularization clarifies how different classes of behaviour unfold, it does not yet address how risky these behaviours are or where prevention and mitigation are most effective.

At this stage, the event space is organized into discrete behavioural units with stable internal logic (Figure 1, 2). Each module exposes loss-of-control events, escalation pathways and potential intervention points, providing a consistent basis for formal risk analysis. Applying risk assessment before modularization would lead to fragmented analyses, whereas applying it at the module level ensures coherence and comparability.

Risk analysis is therefore applied selectively within each behavioural module to loss-of-control events that function as critical branching points in scenario evolution. This establishes the link between modular structures and dynamic scenario construction through bow-tie analysis.

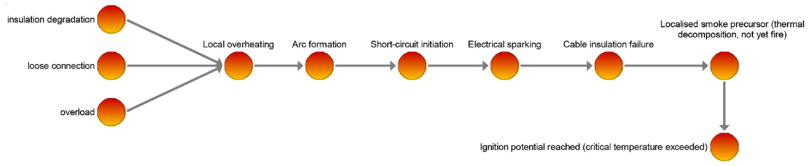

Figure 1: Content of electrical failure propagation module.

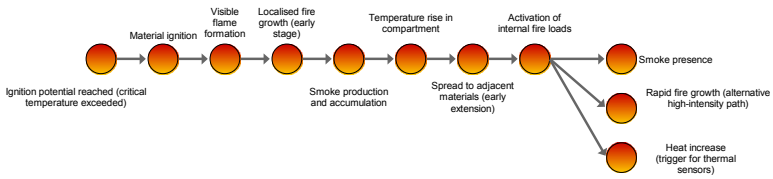

Figure 2: Content of fire ignition and localized spread module.

Risk Analysis for Modules

Although every event triplet (Threat → Risk Event → Consequence) within a module can be expressed as a bow-tie structure, the methodology applies bow-tie analysis only where it adds meaningful analytical value. Bow-ties are developed for risk events that represent a genuine loss of control, expose preventive and mitigative measures that can be influenced by operational decisions, and function as branching points that shape the direction of scenario evolution. In this way, bow-tie diagrams are used to strengthen causal understanding rather than to document all theoretical triplets.

The selected bow-tie analyses remain part of the module's internal event sub-graph, where they clarify which barriers can prevent escalation, which controls can limit consequences, and how human actions interact with system dynamics. To preserve consistency across the modelling environment, each risk event may appear as an internal, causally embedded event in only one behavioural module. In all other modules the same event can function only as an input or output node. This rule ensures that every event has a single authoritative causal context, prevents duplication of logic, and supports reuse of bow-tie structures across scenario configurations.

Once the structural logic of modules and their associated risk points has been defined, the methodology is able to describe how these elements interact across time and space. This makes it possible to model not only isolated behaviours but also the development of full scenario trajectories.

Extended Bow-Tie Representation and Its Role in Module Construction

Earlier work extended classical bow-tie representations to integrate process activities, responsibilities and regulatory obligations alongside causal risk structures (Kangilaski and Kaugerand, 2024). This demonstrated that bow-tie diagrams can function not only as risk analysis artefacts but also as links between operational behaviour and organizational governance.

The present methodology embeds this extended bow-tie directly within behavioural modules. Selected loss-of-control events inside each module are

expressed using the extended notation, which preserves its analytical role while introducing a new architectural function: defining the semantic input and output events of the module.

In this representation, the left side of the bow-tie corresponds to module entry conditions, while the right side defines output events that enable transitions to downstream modules. Preventive and mitigative barriers remain explicitly connected to processes, organizational roles and regulatory requirements, ensuring continuity with governance and compliance practices. At the same time, the bow-tie's input and output points act as structural interfaces through which modules are assembled into coherent scenario trajectories (Figure 3).

By situating bow-tie logic within the module architecture, the approach provides a consistent mechanism for linking detailed risk analysis with dynamic, system-level scenario modelling.

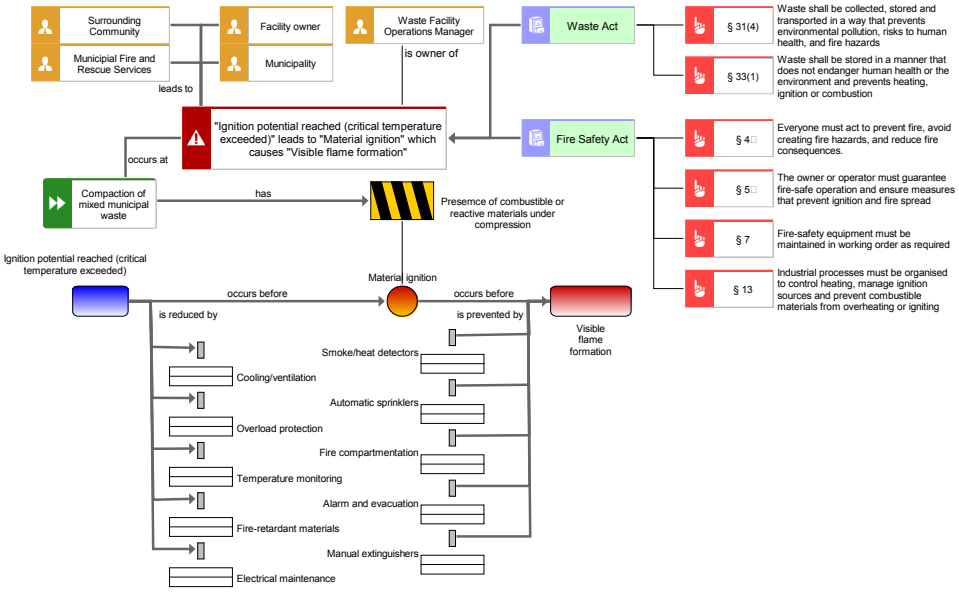

Figure 3: Extended bow tie, from module risk events sequence.

Scenario Dynamic

Once risk events have been identified, analysed and abstracted into behavioural modules, dynamic scenarios can be constructed to represent how risks evolve over time. This transition from modules to scenarios follows directly from the modelling logic: modules describe internal behavioural structures, while scenarios capture interactions between multiple modules under specific contextual conditions.

Scenarios are not derived directly from the original event graph. Instead, the graph defines semantic interfaces—input and output events—that determine how modules can be connected. When the output event of one module corresponds to the input event of another, a transition becomes possible, forming the basis for assembling scenario trajectories.

Scenario construction begins with an initiating event, representing either a detected incident or a hypothetical disturbance used for preparedness

analysis. The corresponding module is instantiated with context-specific parameters such as environmental conditions, asset characteristics or resource availability. As the module evolves, it generates output events that may activate downstream modules, resulting in a sequence or network of interacting modules (Figure 4). Scenario branching arises naturally when multiple transitions are feasible, when resource constraints affect mitigation success, or when environmental factors modify escalation pathways.

Scenario dynamics explicitly incorporate human factors. Human actions such as detection, interpretation, coordination and intervention are treated as events that can accelerate, redirect or suppress scenario development. This supports perception, comprehension and projection by allowing operators to observe key events, understand their causal implications and anticipate likely downstream developments.

The resulting approach combines modularity with dynamic behaviour. It avoids the rigidity of static bow-tie representations while preserving causal clarity, enabling risk trajectories to be analysed across technical, organizational and spatial dimensions and supporting resilience assessment, preparedness planning and real-time decision support.

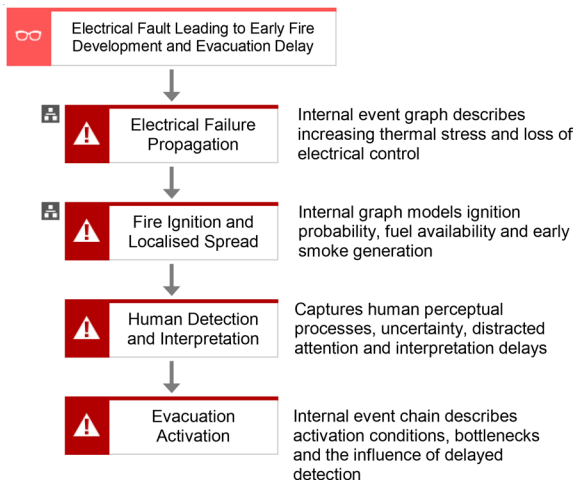

Figure 4: Example scenario.

USING THE MODEL IN PRACTICE

The practical value of the methodology lies in how behavioural modules and dynamic scenarios support preparedness, operational decision-making and governance in urban infrastructure systems. The modular architecture allows planners to explore how different initiating events evolve under varying conditions such as building characteristics, weather, resource availability or network topology. By instantiating modules with real-world parameters and analysing downstream transitions, organizations can identify critical branching points, escalation pathways and capability gaps, providing a more robust basis for preparedness planning than static documentation.

Because modules encode causal structure, intensity levels and resource dependencies, they also support risk prioritization and investment decisions. Comparing scenarios across locations or assets helps reveal where failures are most sensitive to local conditions, how escalation may propagate across infrastructures and which interventions most effectively reduce scenario severity, thereby strengthening the justification of mitigation investments.

The same modularity supports training and inter-agency exercises. Reusable, parameterizable modules enable simulation of diverse operational contexts using consistent behavioural logic, while dynamically branching scenarios reflect participant actions and environmental changes. A shared modelling structure improves communication, clarifies responsibility boundaries and enhances collective situational awareness during cross-agency collaboration.

In real-time operations, the model strengthens situational awareness by supporting perception, comprehension and projection. When an incident such as a leak, ignition or system anomaly is detected, the corresponding module instance is activated with current contextual data, allowing downstream developments to be anticipated and bottlenecks or intervention points to be identified without replacing expert judgement.

Embedded in an enterprise architecture environment, the methodology also supports governance and compliance by maintaining traceability between risks, processes, roles, assets and regulatory requirements. Feedback from incidents and exercises can be used to refine modules and scenario pathways, enabling the model to evolve into a dynamic organizational memory of risk behaviour and intervention effectiveness.

CONCLUSION

This paper presented a human-centered methodology for modelling risk scenarios in urban and infrastructure systems. By integrating process logic, spatial dependencies, human roles and regulatory constraints into a unified architectural framework, the approach overcomes limitations of traditional risk analyses that treat risks as static and domain-isolated. Modular behavioural structures transform complex event graphs into reusable and interpretable building blocks, while dynamic scenario composition enables analysis of how risks evolve under changing conditions.

The methodology strengthens situational awareness by supporting perception, comprehension and projection across technical, organizational and spatial dimensions. Embedded in an enterprise architecture environment, it enhances preparedness planning, investment prioritization, training and real-time decision-making through consistent causal reasoning, and functions as a dynamic organizational memory that evolves alongside the systems it represents.

Future research may focus on quantifying scenario dynamics, integrating real-time data streams, automating module instantiation and examining scalability across regional or cross-border infrastructures. Overall, the work provides a coherent conceptual and practical foundation for human-centered and resilience-oriented risk modelling in complex urban environments.

REFERENCES

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. Nature, 464(7291), 1025–1028. https://doi.org/10.1038/nature08932

de Ruijter, A., Guldenmund, F. (2016). The bowtie method: A review. Safety Science, 88, 211–218. https://doi.org/10.1016/j.ssci.2016.03.001

Endsley, M. R. (1995). Toward a theory of situation awareness in dynamic systems. Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), 32–64, https://doi.org/10.1518/001872095779049543

Gruber, T. R. (1995). Toward principles for the design of ontologies used for knowledge sharing. International Journal of Human–Computer Studies, 43(5–6), 907–928. https://doi.org/10.1006/ijhc.1995.1081

Hollnagel, E. (2014). Safety-I and Safety-II: The Past and Future of Safety Management. Ashgate. https://doi.org/10.1201/9781315605685

Hugo A.L.A., Hildebrandt, T.T. (2024). Three Decades of Formal Methods in Business Process Compliance: A Systematic Literature Review. DOI:10.48550/arXiv.2410.10906

Ionut, V, Panaitescu, F.-V. L., Panaitescu, M. I., Dumitrescu, L. G. and Turof, M. (2018). Risk management with Bowtie diagrams. IOP Conference Series: Materials Science and Engineering. DOI:10.1088/1757-899X/400/8/082021

Kangilaski, T., Kaugerand, J. (2024). Documenting and Analysing Business- and Operational Risks, 10th International Conference on eDemocracy & eGovernment (ICEDEG): Lucerne, Switzerland, June 24-26, 2024, IEEE, 1–8. https://doi.org/10.1109/ICEDEG61611.2024.10702076

Ouyang, M. (2014). Review on modeling and simulation of interdependent critical infrastructure systems. Reliability Engineering & System Safety, 121, 43–60. https://doi.org/10.1016/j.ress.2013.06.040

Park, J., Seager, T., Rao, P., Convertino, M., and Linkov, I. (2013). Integrating risk and resilience approaches to catastrophe management in engineering systems. Risk Analysis, 33(3), 356–367. https://doi.org/10.1111/j.1539-6924.2012.01885.x

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Systems Magazine, 21(6), 11–25. https://doi.org/10.1109/37.969131

Sadiq, Shazia & Governatori, Guido & Namiri, Kioumars. (2007). Modeling Control Objectives for Business Process Compliance. 149-164. DOI:10.1007/978-3-540-75183-0_12

Schekkerman, J. (2004). How to survive in the jungle of enterprise architecture frameworks. Institute for Enterprise Architecture Developments.

Studer, R., Benjamins, V. R., & Fensel, D. (1998).Knowledge engineering: Principles and methods. Data & Knowledge Engineering, 25(1–2), 161–197. https://doi.org/10.1016/S0169-023X(97)00056-6

Teichmann, M., Ehala, J., Kaugerand, J., Meriste, M. and Rannat, K. (2023). Let's Add Highly Stressed People to the Cyber-Physical-Social System. Conference on Cognitive and Computational Aspects of Situation Management (Vol. 102, pp. 54–65).

Uschold, M., & Gruninger, M. (1996).Ontologies: Principles, methods and applications. Knowledge Engineering Review, 11(2), 93–155. https://doi.org/10.1017/S0269888900007797

White, S. A., & Miers, D. (2008). BPMN Modeling and Reference Guide: Understanding and Using BPMN. Future Strategies Inc

Woods, D. D. (2020). The theory of graceful extensibility: basic rules that govern adaptive systems. Environment Systems and Decisions, 38, 433-457. DOI:10.1007/s10669-018-9708-3