Proc. of the European Safety and Reliability Conference (ESREL 2026)
Edited by José C. Matos, Paulo B. Lourenço, Michael Beer, Daniel Oliveira, Edoardo Patelli, Hélder S. Sousa, Rui A. Silva and Monica Santamaria
 Published by Research Publishing, Singapore.
doi: 10.3850/ESREL2026061419_esrel26-p26236-cd

Proposal for an Integrated GMA-STAMP Foresight Method to Develop EBIOS RM Scenarios for Anticipating Cybersecurity Risks in the Maritime Sector

Eric Rigaud

Mines Paris, PSL University, Centre for research on risks and crises (CRC), 06904 Sophia Antipolis, France.
E-mail: eric.rigaud @minesparis.psl.eu

Clément Iphar

Mines Paris, PSL University, Centre for research on risks and crises (CRC), 06904 Sophia Antipolis, France.
E-mail: clement.iphar@minesparis.psl.eu

Alejandra Cue Gonzalez

Mines Paris, PSL University, Centre for Observation, Impacts, Energy (O.I.E.), 06904 Sophia Antipolis, France
E-mail: alejandra.cue_gonzalez @minesparis.psl.eu

Aldo Napoli

Mines Paris, PSL University, Centre for research on risks and crises (CRC), 06904 Sophia Antipolis, France.
E-mail: aldo.napoli @minesparis.psl.eu

The maritime transition, which integrates autonomous vessels and alternative energies while addressing port safety and security issues, raises challenges for long-term risk management. The multiplicity of possible technological, organizational, and regulatory configurations challenges risk analysis approaches based on the extrapolation of historical data and the identification of isolated failures. In this context, a foresight approach becomes necessary to explore the space of possible futures, identify coherent configurations and their associated vulnerabilities, and design robust transition strategies. This paper proposes an original foresight methodological framework articulating General Morphological Analysis (GMA) and the Systems-Theoretic Accident Model and Processes (STAMP) model to develop prospective scenarios when applying the EBIOS Risk Manager (EBIOS RM) method, in order to systematically analyze the emerging cyber risks of the maritime transition. EBIOS RM addresses cyber risks by combining compliance analysis and scenario development aimed at identifying intentional risks, particularly targeted or sophisticated attacks. The GMA-STAMP coupling for developing EBIOS RM scenarios addresses the dual need to explore uncertainty and apprehend complexity. GMA generates the space of possible configurations, while STAMP enables the modeling of control structures and emerging vulnerabilities. This articulation aims to identify configurations that are both coherent and secure, while revealing potential cybersecurity issues.

Keywords: technological change, maritime navigation, foresight, EBIOS RM, GMA, STAMP

1. Introduction

The maritime sector is undergoing a profound transformation driven by converging technological, environmental, and regulatory pressures. The International Maritime Organization's decarbonization targets, the emergence of Maritime Autonomous Surface Ships (MASS), and the increasing digitalization of port operations are reshaping the industry's technological landscape at an unprecedented pace (IMO, 2023). This transformation entails a fundamental reconfiguration of operational architectures, communication protocols, and human-machine interactions, with far-reaching implications for safety and security.

From a cybersecurity perspective, these developments introduce novel attack surfaces and threat vectors that existing risk assessment frameworks struggle to anticipate. Traditional approaches to cyber risk analysis typically rely on historical incident data, known vulnerability databases, and current threat intelligence to identify and prioritize risks (Shameli-Sendi et al., 2016). While effective for established systems, such retrospective methods face inherent

limitations when applied to emerging technologies whose operational contexts, interdependencies, and failure modes remain largely unexplored. The question is no longer merely how to protect existing maritime systems, but how to anticipate cybersecurity challenges in systems that do not yet exist in their final form.

This challenge calls for a shift from predictive to possibilistic risk analysis—an approach that systematically explores the space of plausible futures rather than extrapolating from past trends (Godet & Roubelat, 1996). Foresight methods offer promising avenues for such exploration, yet their integration with structured cybersecurity risk assessment frameworks remains underdeveloped. Existing scenario-based methods, including EBIOS Risk Manager (EBIOS RM) (ANSSI, 2018), provide robust frameworks for threat modeling but typically assume a stable technological baseline. Conversely, foresight techniques such as General Morphological Analysis (GMA) excel at mapping possible configurations but lack the analytical depth required to identify systemic vulnerabilities within those configurations.

This paper addresses this methodological gap by proposing an integrated framework that articulates three complementary approaches: EBIOS Risk Manager for structured threat scenario development, General Morphological Analysis for systematic exploration of future configurations, and the Systems-Theoretic Accident Model and Processes (STAMP) for modeling control structures and emergent vulnerabilities. The resulting methodology enables analysts to generate prospective cybersecurity scenarios grounded in coherent representations of possible technological futures, rather than mere extensions of current threat landscapes.

The framework is designed for application to the maritime sector, with particular attention to automated message exchange technologies—such as the Automatic Identification System (AIS) and Vessel Traffic Services (VTS)—whose integrity is critical for both navigation safety and environmental protection. The methodology will be implemented in the context of the Pelagos Sanctuary, a marine protected area in the north-western Mediterranean Sea, where cybersecurity and ecological imperatives intersect.

The remainder of this paper is organized as follows. Section 2 presents the theoretical foundations underpinning the proposed methodology, reviewing EBIOS RM, GMA, and STAMP and their potential synergies. Section 3 details the integrated five-phase methodology. Section 4 concludes with a discussion of expected contributions and directions for future research.

2. Theoretical underpinnings

2.1. *The EBIOS Risk Manager method*

EBIOS Risk Manager is a digital risk assessment and treatment method developed by the French National Agency for the Security of Information Systems (ANSSI) and published in 2018 (ANSSI, 2018).

EBIOS Risk Manager is structured around five sequential and iterative workshops (ANSSI, 2018). The first workshop, "Security Baseline," establishes the study scope, identifies feared events for the organization, and determines the business values to protect. The second workshop, "Risk Sources," characterizes the threat ecosystem by identifying potential risk sources, their targeted objectives, and their capabilities. The third workshop, "Strategic Scenarios," constructs high-level attack paths linking risk sources to targeted objectives on business values. The fourth workshop, "Operational Scenarios," details the technical operational methods enabling the realization of strategic scenarios by exploiting supporting assets of the system. Finally, the fifth workshop, "Risk Treatment," defines security measures proportionate to the identified risks.

EBIOS RM proposes a formal risk analysis framework that explicitly integrates the dimension of evolving cyber threats, unlike more classical approaches centered on vulnerabilities (Shameli-Sendi et al., 2016; Refsdal et al., 2015). The method also offers structured vocabulary and taxonomy facilitating communication between different domains of expertise (Dubois et al., 2010).

2.2. *The Scenario Dimension in EBIOS Risk Manager*

The scenario-based approach constitutes the methodological core of EBIOS Risk Manager, representing a paradigm shift from traditional vulnerability-centric risk analysis to threat-driven risk modeling (Kordy et al., 2014). This dual-level scenario structure enables organizations to bridge the gap between strategic business

concerns and tactical technical implementations, creating a comprehensive narrative of potential attacks from initial motivation to final impact (Haqaf & Koyuncu, 2018).

The power of EBIOS RM lies in the systematic articulation between strategic scenarios representing high-level attack paths that connect risk sources to their ultimate objectives on business values (workshop 3) and operational scenarios translating strategic scenarios into concrete technical attack sequences, detailing the specific methods and vulnerabilities that could be exploited to achieve strategic objectives. (workshop 4) . One strategic scenario typically generates multiple operational scenarios, as different technical paths may lead to the same strategic objective (Atzeni et al., 2011). This multiplicative effect enables comprehensive coverage of the attack surface.

This articulation creates a traceable chain from business impact to technical implementation. Decision-makers can understand how specific technical vulnerabilities could enable high-level threats to their strategic objectives, while technical teams can prioritize security efforts based on their contribution to mitigating business-critical risks (Bojanc & Jerman-Blazic, 2013). The method thus establishes a common language bridging organizational silos.

Building upon the scenario-based framework of EBIOS RM, this research aims to apply the method in a prospective setting to investigate how technological transformations will impact cybersecurity risks in the coming years. The General Morphological Analysis (GMA) approach is employed to structure and support the scenario development process, enabling rigorous exploration of plausible future threat landscapes and their implications for risk assessment.

3.2. *The General Morphological Analysis*

General Morphological Analysis is a method for systematically structuring and investigating complex problem spaces, originally developed by Swiss astrophysicist Fritz Zwicky in the 1940s (Zwicky, 1969). Initially applied to astronomical and engineering problems, the method was progressively formalized and extended to social sciences, policy analysis, and futures studies (Zwicky & Wilson, 1967). Contemporary GMA, particularly as developed by Tom Ritchey and the Swedish Morphological Society since the 1990s, provides a rigorous framework for exploring multidimensional problem spaces and constructing internally consistent scenarios in contexts characterized by complexity and uncertainty (Ritchey, 2011).

GMA aims to support systematic exploration of all possible configurations within a complex problem space, identifying plausible solutions or scenarios that might otherwise be overlooked through conventional analytical approaches (Álvarez & Ritchey, 2015). The method is particularly suited for wicked problems, those characterized by multiple stakeholders, conflicting objectives, high uncertainty, and numerous interacting variables (Rittel & Webber, 1973; Ritchey, 2005). Unlike probabilistic forecasting methods that attempt to predict the most likely future, GMA adopts a possibilistic approach, mapping the entire space of plausible futures without presuming to know which will materialize (Godet & Roubelat, 1996).

The GMA process unfolds through several interconnected phases (Ritchey, 2011). The problem definition and boundary setting phase establishes the scope of analysis, identifies key stakeholders, and clarifies the purpose and time horizon of the study. The parameter identification phase determines the essential dimensions or variables that characterize the problem space, selecting those that are both relevant and relatively independent. The configuration space construction follows, where each parameter is decomposed into discrete states or conditions representing the range of possible values or configurations that parameter might assume. This creates a multidimensional morphological field—a matrix structure where each row represents a parameter and each column represents one of its possible states. The Cartesian product of all parameter states defines the total configuration space, representing all theoretically possible combinations. The consistency analysis phase constitutes the analytical core of GMA. Here, pairs of parameter states are systematically examined to determine their mutual compatibility (Ritchey, 2002). Cross-consistency assessment establishes which combinations are internally coherent and plausible versus those that are contradictory or impossible. This pairwise evaluation generates a consistency matrix that captures the structural relationships within the problem space. Based on the consistency matrix,

the scenario synthesis phase identifies pathways through the morphological field that maintain internal consistency across all parameters. These consistent configurations represent plausible scenarios or solution spaces (Ritchey, 2018). Finally, the evaluation and selection phase assesses the synthesized scenarios against strategic criteria, stakeholder preferences, or policy objectives, enabling prioritization and decision support.

The integration of EBIOS Risk Manager and General Morphological Analysis creates a powerful methodological synergy for prospective cybersecurity risk assessment. While EBIOS RM provides a structured framework for constructing threat scenarios and linking strategic objectives to operational attack paths, its conventional application relies heavily on current threat intelligence and known attack patterns, potentially limiting its capacity to anticipate novel risks emerging from technological disruption (Nurse et al., 2014). GMA addresses this limitation by systematically exploring the multidimensional space of possible futures, identifying plausible configurations of technological, organizational, and threat landscape parameters that may not be immediately apparent through traditional threat analysis (Bishop et al., 2007; Schwartz, 1996). In this integrated approach, GMA supports the upstream phases of EBIOS RM by generating structured, internally consistent prospective contexts within which risk sources, capabilities, and attack vectors can evolve.

Building upon the EBIOS RM-GMA framework for prospective scenario development, the Systems-Theoretic Accident Model and Processes (STAMP) is employed to analyze the systemic implications of technological transformations on cybersecurity. STAMP enables the modeling of control structures and safety constraints within future configurations, revealing emergent vulnerabilities that result from inadequate interactions rather than isolated component failures.

2.3. *The Systems-Theoretic Accident Model and Processes model*

Systems-Theoretic Accident Model and Processes is a causality model for safety analysis developed by Nancy Leveson at the Massachusetts Institute of Technology in the early 2000s. Originally designed to address limitations of traditional safety analysis methods in increasingly complex socio-technical systems, STAMP represents a paradigm shift from component failure-based models to a systems thinking approach centered on control and constraints (Leveson, 2004; 2011). Unlike traditional safety models that view accidents as resulting from chains of failures or human errors, STAMP posits that accidents occur when system behavior violates safety constraints due to inadequate control of interactions among system components.

STAMP aims to provide a comprehensive framework for analyzing safety and security in complex systems where emergent behaviors, component interactions, and organizational factors play critical roles. The approach is particularly suited for cyber-physical systems, networked systems, and contexts where software, automation, and human decision-making intersect in complex ways (Leveson & Thomas, 2018). STAMP addresses a fundamental limitation of traditional risk analysis methods: their focus on component reliability and linear causal chains, which proves insufficient for understanding accidents in systems where complexity, coupling, and emergent properties dominate. In the cybersecurity domain, STAMP has been extended to analyze security issues as violations of security constraints within control structures (Young & Leveson, 2014).

The primary analytical technique derived from STAMP is System-Theoretic Process Analysis (STPA), a hazard analysis method that systematically identifies scenarios in which control actions could be inadequate or improperly executed (Leveson & Thomas, 2018). STPA proceeds through four main steps. Step 1 involves defining the analysis purpose, system boundaries, and identifying accidents and hazards (undesired states) to prevent. Step 2 models the hierarchical control structure, identifying controllers, control actions, feedback mechanisms, and the process models maintained by each controller. Step 3 systematically identifies unsafe control actions (UCAs) by examining four guiding questions for each control action: when providing the control action causes a hazard, when not providing it causes a hazard, when providing it too early or too late causes a hazard, and when stopping it too soon or applying it too long causes a hazard. Step 4 identifies causal scenarios explaining why each unsafe control action might occur, considering

factors such as incorrect process models, inadequate feedback, control algorithm flaws, coordination failures, or delayed control actions.

The integration of STAMP into prospective cybersecurity scenario development addresses the unique challenges posed by the convergence of artificial intelligence, digitalization, autonomous systems, and alternative energy technologies. These transformations fundamentally alter control architectures in ways that EBIOS RM and GMA, while valuable for identifying threats and exploring configurations, do not explicitly capture. STAMP's hierarchical control structure model and systematic unsafe control action analysis enable identification of emergent vulnerabilities specific to these converging technologies, such as AI-based perception manipulation, distributed system coordination failures, autonomous system constraint violations, or energy system exploitation, that arise not from isolated component failures but from inadequate control in fundamentally transformed socio-technical systems. This systems-level analysis is essential for developing scenarios that capture how the intersection of these technologies creates qualitatively new cybersecurity risk patterns in future systems and operations.

The following sections present the research methodology that operationalizes this integrated framework and evaluate its effectiveness in generating prospective cybersecurity scenarios.

3. Integrated methodology for prospective cybersecurity risk assessment

3.1. *Objectives and scope*

The integrated EBIOS RM-GMA-STAMP methodology aims to enable systematic identification and analysis of cybersecurity risks emerging from technological transformations. The methodology pursues four primary objectives:

- **Objective 1:** Generate comprehensive yet manageable sets of plausible future technological configurations accounting for AI, digitalization, autonomous systems, and alternative energy convergence.
- **Objective 2:** Develop prospective threat scenarios grounded in future configurations rather than current threat intelligence extrapolations.
- **Objective 3:** Identify systemic vulnerabilities arising from inadequate control structures and interaction failures in transformed systems.
- **Objective 4:** Support strategic cybersecurity decision-making robust across multiple plausible technological futures.

The methodology applies to systems undergoing significant technological transformation, particularly critical infrastructure and cyber-physical systems where safety and security intersect.

3.2. *Foundational Principles*

Six foundational principles guide the methodology's application:

- **Principle 1: Possibilistic futures.** Map plausible futures without predicting specific outcomes, acknowledging technological uncertainty while maintaining analytical rigor.
- **Principle 2: Multi-level integration.** Integrate morphological configurations (possible states), threat scenarios (adversarial attempts), and systemic analysis (vulnerability conditions).
- **Principle 3: Systems thinking.** Consider emergent properties, feedback loops, and hierarchical control structures rather than isolated components.
- **Principle 4: Participatory analysis.** Engage diverse stakeholders whose collective knowledge enriches scenario development and validation.
- **Principle 5: Iterative refinement.** Progress through iterative cycles of analysis, refinement, and validation rather than linear progression.
- **Principle 6: Transparency and traceability.** Document analytical decisions, assumptions, and reasoning to enable validation and replication.

3.3. *Methodological phases*

Phase 1: Scoping and Baseline Establishment

The purpose of the first phase is to define the scope of the study, engage relevant stakeholders, and characterize the current state of the system.

The initial phase begins with the identification of relevant stakeholders and the constitution of a multidisciplinary team bringing together expertise in cybersecurity, maritime

operations, and the specific technologies under consideration. This team collectively defines the missions, business objectives, and critical values requiring protection throughout the study. A comprehensive documentation of the current system architecture, operational processes, and security posture provides the baseline against which future configurations will be assessed. The existing threat landscape is characterized through analysis of known adversaries, historical incidents, and sector-specific threat intelligence. Finally, the key drivers of technological transformation—whether regulatory mandates, economic incentives, or societal expectations—are identified to inform the subsequent construction of the morphological space.

The output of the first phase includes the study scope, a model of the current system, a baseline threat characterization, the identification of business values and feared events, as well as the key transformation drivers.

Phase 2: Morphological Space Construction

The purpose of the second phase is to structure the space of plausible future technological configurations using GMA.

This phase applies General Morphological Analysis to map the space of possible futures. The process begins with the identification of fundamental parameters that characterize technological variation across the relevant dimensions, including artificial intelligence adoption levels, connectivity architectures, degrees of autonomy, and alternative energy integration. For each parameter, discrete states are defined representing the range of plausible future values or configurations that the parameter might assume within the study's time horizon. These parameters and their associated states are organized into a morphological field, a structured matrix enabling systematic combination. Pairwise compatibility assessment then examines each combination of parameter states to determine their mutual consistency, distinguishing configurations that are internally coherent and plausible from those that are contradictory or technically infeasible.

The outputs of this phase include the morphological field, the consistency matrix, and a set of internally consistent future configurations.

Phase 3: Configuration selection and control structure modeling

The purpose of the third phase is to select representative configurations and model their control structures using STAMP.

Building upon the morphological field, this phase synthesizes complete configurations by selecting consistent pathways through the parameter space. From the potentially large number of consistent configurations, a subset is selected for detailed analysis based on criteria including strategic relevance to organizational objectives, potential for novel threat emergence, and technological distinctiveness ensuring adequate coverage of the future space. Each selected configuration is then elaborated through detailed descriptions encompassing system architecture, operational processes, and dependencies on external ecosystem elements. The STAMP framework is subsequently applied to model the hierarchical control structure of each configuration, identifying the controllers responsible for maintaining safe and secure operations, the control actions they execute, the feedback mechanisms providing situational awareness, and the security constraints that must be enforced to prevent undesirable outcomes.

The output of the third phase includes the selected configurations (typically three to six), their detailed descriptions, the associated control structure diagrams, and the identified security constraints.

Phase 4: Prospective Threat Scenario Development

The purpose of the fourth phase is to construct strategic and operational scenarios using adapted EBIOS RM workshops.

This phase operationalizes the EBIOS Risk Manager method within the prospective configurations developed in previous phases. The analysis begins with risk source identification and characterization, examining how technological transformations alter adversary motivations, capabilities, resources, and opportunities for access. Particular attention is given to threat actors whose relevance may increase or decrease across different configurations. Strategic scenarios are then constructed as high-level attack paths linking identified risk sources to the business values established during scoping, with explicit integration of the control structure weaknesses revealed through STAMP analysis.

These strategic scenarios are subsequently decomposed into operational scenarios detailing the technical attack sequences, specific vulnerabilities exploited, and unsafe control actions that could enable adversaries to achieve their objectives within each future configuration.

The output of this phase includes the risk source profiles, the strategic scenarios (four to eight per configuration), the operational scenarios (eight to fifteen per configuration), and the identified unsafe control actions.

Phase 5: Risk Assessment and Treatment Strategy

The purpose of the fifth phase is to assess scenarios and develop risk treatment strategies robust across futures.

The final phase evaluates the scenarios developed in Phase 4 and derives actionable security recommendations. Each scenario is assessed according to severity, measured by potential impact on business values, and likelihood, determined by the conjunction of risk source capability and configuration-specific vulnerability. A cross-configuration analysis distinguishes scenarios that appear across multiple futures—representing robust threats warranting immediate attention—from those specific to particular configurations, which may require conditional or adaptive responses. Security measures are then defined and categorized according to their temporal applicability, distinguishing immediate actions from medium-term investments and long-term capability development, as well as their robustness across the configuration space. The phase concludes with the synthesis of strategic recommendations articulating priority investments, monitoring indicators for emerging threats, and organizational capability development needs, consolidated into an implementation roadmap.

The output of this phase includes the risk matrices, the prioritized scenarios, the treatment strategy portfolio, as well as the strategic recommendations and the implementation roadmap.

3.4. Validation and iteration

The methodology incorporates continuous validation through three mechanisms. Technical consistency validation ensures that identified configurations, scenarios, and control structures are technically feasible and internally consistent through expert review of technological assumptions and attack scenario plausibility. Stakeholder validation engages organizational decision-makers to verify that scenarios address relevant concerns, business value characterizations are accurate, and recommended strategies are actionable within organizational constraints. Cross-method coherence validation verifies that outputs from GMA configurations, EBIOS scenarios, and STAMP control structures maintain mutual consistency, triggering iterative refinement when contradictions or gaps are identified.

4. Conclusion

This paper has presented an original foresight methodological framework integrating General Morphological Analysis (GMA) and the Systems-Theoretic Accident Model and Processes (STAMP) to support the development of prospective scenarios within the EBIOS Risk Manager method. The articulation of these three approaches creates a complementary analytical chain: GMA systematically explores the space of plausible future configurations, STAMP reveals emergent vulnerabilities rooted in inadequate control structures and interaction failures, and EBIOS RM connects these insights to actionable threat scenarios and treatment strategies. The resulting five-phase methodology offers a traceable, iterative, and participatory process that adopts a possibilistic stance toward the future, adapted to the complexity and uncertainty inherent in the maritime technological transition.

The implementation of this methodology will focus on the Pelagos Sanctuary, a marine protected area in the north-western Mediterranean Sea dedicated to the conservation of marine mammals. In this context, the integrity and reliability of automated message exchange technologies — such as AIS and VTS — are critical not only for vessel safety but also for the enforcement of environmental protection measures, including speed restrictions and collision avoidance with cetaceans. Cyberattacks targeting these systems could compromise the effectiveness of environmental safeguards, making the prospective identification of such risks both a cybersecurity and an ecological imperative. Future research will operationalize the methodology through expert workshops and stakeholder engagement within the Pelagos

context, with the aim of generating prospective threat scenarios and validating the framework's transferability to other maritime regions undergoing comparable technological transformations.

Funding

The research presented in this article was developed as part of the JASON project. JASON aims to capitalize on scientific research, technological advances, and the results of previous projects implemented in the field of environmental protection and maritime safety in the geographical cooperation area covered by the Interreg Maritime program. JASON is co-financed by the Italy-France Maritime Interreg Program 2021-2027, with ERDF funding of €3,754,665.

References

Álvarez, A., and T. Ritchey. 2015. "Applications of General Morphological Analysis." *Acta Morphologica Generalis* 4 (1): 1–40. https://www.swemorph.com/amg/pdf/amg-4-1-2015.pdf

ANSSI. 2018. *EBIOS Risk Manager – The Method*. Paris: Agence Nationale de la Sécurité des Systèmes d'Information. https://cyber.gouv.fr/publications/la-methode-ebios-risk-manager-le-guide.

Atzeni, A., C. Cameroni, S. Faily, J. Lyle, and I. Fléchais. 2011. "Here's Johnny: A Methodology for Developing Attacker Personas." In *Proceedings of ARES 2011*, 722–727. https://doi.org/10.1109/ARES.2011.115.

Bishop, P., A. Hines, and T. Collins. 2007. "The Current State of Scenario Development: An Overview of Techniques." *Foresight* 9 (1): 5–25. https://doi.org/10.1108/14636680710727516.

Bojanc, R., and B. Jerman-Blažič. 2013. "A Quantitative Model for Information-Security Risk Management." *Engineering Management Journal* 25 (2): 25–37. https://doi.org/10.1080/10429247.2013.11431972

Dubois, E., P. Heymans, N. Mayer, and R. Matulevičius. 2010. "A Systematic Approach to Define the Domain of Information System Security Risk Management." In *Intentional Perspectives on Information Systems Engineering*, 289–306. https://doi.org/10.1007/978-3-642-12544-7_16.

Godet, M., and F. Roubelat. 1996. "Creating the Future: The Use and Misuse of Scenarios." *Long Range Planning* 29 (2): 164–171. https://doi.org/10.1016/0024-6301(96)00004-0.

Haqaf, H., and M. Koyuncu. 2018. "Understanding Key Skills for Information Security Managers." *International Journal of Information Management* 43:165–172. https://doi.org/10.1016/j.ijinfomgt.2018.07.013.

Kordy, B., L. Pièvre-Cambacédès, and P. Schweitzer. 2014. "DAG-Based Attack and Defense Modeling: Don't Miss the Forest for the Attack Trees." *Computer Science Review* 13: 1–38. https://doi.org/10.1016/j.cosrev.2014.07.001.

Leveson, N. G. 2004. "A New Accident Model for Engineering Safer Systems." *Safety Science* 42 (4): 237–270. https://doi.org/10.1016/S0925-7535(03)00047-X.

Leveson, N. G. 2011. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge, MA: MIT Press.

Leveson, N. G., and J. P. Thomas. 2018. *STPA Handbook*. Cambridge, MA: MIT. Available at: http://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.

Nurse, J. R., S. Creese, M. Goldsmith, and K. Lamberts. 2014. "Trustworthy and Effective Communication of Cybersecurity Risks: A Review." In *2014 1st International Workshop on Socio-Technical Aspects in Security and Trust*, 60–68. 10.1109/STAST.2011.6059257

Refsdal, A., B. Solhaug, and K. Stølen. 2015. *Cyber-Risk Management*. Cham: Springer. https://doi.org/10.1007/978-3-319-23570-7.

Ritchey, T. 2002. *General Morphological Analysis: A General Method for Non-Quantified Modelling*. Stockholm: Swedish Morphological Society. https://www.swemorph.com/pdf/gma.pdf.

Ritchey, T. 2005. *Wicked Problems: Structuring Social Messes with Morphological Analysis*. Stockholm: Swedish Morphological Society. https://www.swemorph.com/pdf/wp.pdf.

Ritchey, T. 2011. *Wicked Problems – Social Messes: Decision Support Modelling with Morphological Analysis*. Berlin: Springer. https://doi.org/10.1007/978-3-642-19653-9.

Rittel, H. W., and M. M. Webber. 1973. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4 (2): 155–169. https://doi.org/10.1007/BF01405730.

Schwartz, P. 1996. *The Art of the Long View: Planning for the Future in an Uncertain World*. New York: Currency Doubleday.

Shameli-Sendi, A., R. Aghababaei-Barzegar, and M. Cheriet. 2016. "Taxonomy of Information Security Risk Assessment (ISRA)." *Computers & Security* 57: 14–30. https://doi.org/10.1016/j.cose.2015.11.001.

Zwicky, F. 1969. *Discovery, Invention, Research through the Morphological Approach*. Toronto: Macmillan.

Zwicky, F., and A. G. Wilson, eds. 1967. *New Methods of Thought and Procedure: Contributions to the Symposium on Methodologies*. Berlin: Springer. https://doi.org/10.1007/978-3-642-87617-2.