Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen

doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P7383-cd

Towards Dynamic Safety Control Structures in STAMP to Manage Safety-Critical Industrial Establishments

Francesco Simone

Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Via Eudossiana 18, 00184 Rome (RM), Italy. E-mail: francesco.simone@uniroma1.it

Antonio Javier Nakhal Akel

Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Via Eudossiana 18, 00184 Rome (RM), Italy.

Elena Stefana

Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Via Eudossiana 18, 00184 Rome (RM), Italy. E-mail: elena.stefana@uniroma1.it

Giulio Di Gravio

Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Via Eudossiana 18, 00184 Rome (RM), Italy. E-mail: giulio.digravio@uniroma1.it

Riccardo Patriarca

Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Via Eudossiana 18, 00184 Rome (RM), Italy. E-mail: riccardo.patriarca@uniroma1.it

The Directive 2012/18/EU (also known as Seveso III Directive) is at the core of safety management in industrial establishments dealing with dangerous substances. The establishments falling under the Seveso III Directive – and all other entities involved – can be recognized as parts of a Socio-Technical System (STS), due to the presence of tightly interacting technical, social, and organizational elements. This paper relies on the System-Theoretic Accident Model and Processes (STAMP) principles to let critical interactions among system elements emerge. The approach starts with the construction of a dedicated Safety Control Structure (SCS) for the processes described in the Seveso III Directive. However, since the interactions included are highly variable because of their interplays, and because of time and causal dependencies, the traditional SCS perspective limits the analysts' capabilities. In traditional STAMP, such interaction is implicit, requiring *ad-hoc* solutions to be interpreted. This paper discusses the benefit of adding a dynamic dimension to the SCS to properly consider temporal and causal developments, as well as dependencies within the various processes. Such dynamicity is related to the definition of triggers being able to activate (or deactivate) the mutual dependencies among agents, based on their correlation and their presence in specific circumstances. Results show how such dynamic dimension is a core feature for operationalizing any SCS in real case scenarios.

Keywords: systems theory, major accident hazard, risk management, industrial plants, operations management.

1. Introduction

In systems, where multiple elements cooperate to reach a common goal, it is not uncommon to identify rules influencing the behaviors of the system elements. The identification of these governing rules becomes more challenging when dealing with the so-called Socio-Technical Systems (STSs), which are characterized by tight interactions among technical, social, and organizational elements, thus leading to increasing complexity (Emery, 2016).

The more complex a system is, the harder it is to associate its processes with precise principles and criteria. Unexpected behaviors have room to emerge from complexity, even when some explicit rules and constraints exist. In other words, not all rules manifest vividly: some can appear at some time, and some may be not visible to the operator at any time. But when some of these rules are known, are they beneficial – or even needed – to better understand socio-technical complexity?

In this paper we argue how considering known rules – if any – when studying complex systems provides an additional tool in the arsenal of comprehensive system understanding.

This awareness emerged during a research project we are currently conducting, i.e., Resilience Engineering for Safe Energy Transition (RESET), cf. the acknowledgement section for full details. The RESET project aims at studying complex STSs in light of energy transition scenarios, eventually providing guidelines for a safe shift towards greener processes. In particular, the project focuses on the safety management of critical industrial establishments, which store, handle, produce, or deal with hazardous substances. Accidents occurring in these industrial establishments have the potential to cause severe consequences on both the human health and the surrounding environment. It was the infamous case of a chemical plant in Seveso, Italy, where a major accident occurred in 1976: a plant's reactor overheated, releasing a vast toxic cloud of dioxin into the surrounding area (Eskenazi et al., 2004). This event prompted the European Union (EU) to strengthen the industrial safety regulations and the environmental protection measures, with the objective of preventing similar occurrences in the future. As a result, the Seveso Directive (officially known as the Directive 82/501/EEC) was first introduced in 1982, and then updated and revised multiple times up to its latest version, i.e., the Directive 2012/18/EU or Seveso III Directive (European Council, 2012), which is currently in force in the EU. The Seveso III Directive ultimately aims at managing the risks associated with the use of hazardous substances. To this purpose, it establishes responsibilities and requirements for dealing with such substances, stressing the need to (e.g.) comprehensively assess risks in a safety report, whose outcomes shall be effectively put in practice by means of a safety management system, whose effectiveness must be periodically checked via authorities' inspections – known rules available!

What is identified in the Seveso III Directive is – clearly – a STS, as its processes involve: (i) establishment's technical components (e.g., storage tanks), (ii) people (e.g., plant's workers), and (iii) organizations (e.g., authorities), tightly interacting to ensure system safety. Recent advancements in safety science acknowledged the need to rely on systemic approaches to deal with socio-technical complexity. Among these systemic approaches for safety management, the System-Theoretic Accident Model and Processes (STAMP) by Leveson (2004) and its nested techniques, i.e., the System-Theoretic Process Analysis (STPA), and the Causal Analysis using System Theory (CAST), gradually affirmed in the last decades, with several operational cases being presented in the available literature (Patriarca et al., 2022). The STAMP principles permit visualizing and studying a complex STS through its hierarchical safety control structure (SCS), which highlights all the interactions among the various system elements (Leveson, 2012). However, such interactions are flattened statically in a SCS, leaving only an inherent possibility to include rules for describing their behaviors with additional details. Knowing these rules is among the tasks of an analyst, who shall be able to read the SCS appropriately, eventually gaining insights into the complex system the SCS is representing. The relationships among system elements can be temporally and/or causally dependent, and, in some cases, the rules behind these dependencies are known – but not includable in a traditional SCS.

In this paper we discuss over an excerpt of a SCS describing the STS identified in the Seveso III Directive. Studying the SCS permits gaining insights on how to add a dynamic dimension to the SCS representation, i.e., highlighting temporal and causal dependencies among and within the system elements. These relationships are aligned with the content of the Seveso III Directive itself, which provides known rules for guiding – at least partially – the complex STS behaviors. On these premises, this paper argues how explicating additional details regarding the SCS's elements is needed for a more comprehensive understanding of the STS a SCS is representing.

The remainder of this paper is organized as it follows. In **Section 2**, there are presented some essential notions to understand a SCS.

Subsequently, **Section 3** reports and shortly describes the SCS for the Seveso III Directive. The SCS is then enriched with specification of causal and temporal relationships among the SCS's elements. Finally, **Section 4** includes concluding remarks on this work and some proposals for future research developments.

2. Methodological Background

Introduced by Leveson (2004), the STAMP integrates Systems Theory and Control Theory to enhance the understanding of system safety. Inspired by Systems Theory, it emphasizes the interconnectedness of the system elements, advocating for a holistic approach. On the other hand, Control Theory contributes by focusing on the dynamic equilibrium among the system elements and control loops, whose disruptions lead to system failures. Accordingly, the STAMP views safety problems as control problems, aiming at identifying accident scenarios, their potential causes, and their consequences.

2.1. *Safety Control Structures (SCSs)*

In practice, the principles behind STAMP are leveraged through the system's hierarchical SCS, mapping the system agents and their interactions. Graphically, a SCS consists of blocks (depicting agents) and arrows (depicting interactions), each with specific meanings:

- *Feedback*. It is an information exchanged by an agent to another, to make the second aware of some information kept by the first. The feedback is represented by an arrow connecting a bottom block with an upper block (e.g., "Feedback (C to A)" connecting "Agent C" to "Agent A", cf. **Fig. 1**);
- *Control action*. It is an information exchanged by an agent to another, to modify the behavior of the second one. The control action is represented by an arrow connecting an upper block with a bottom block (e.g., "Control action (A to C)" connecting "Agent A" to "Agent C", cf. **Fig. 1**);
- *Controlled process*. It is an agent subjected to the control action of another agent defined as controller (e.g., "Agent C", cf. **Fig. 1**);
- *Controller*. It is an agent imposing a control action on another agent defined as controlled process (e.g., "Agent A", cf. **Fig. 1**).

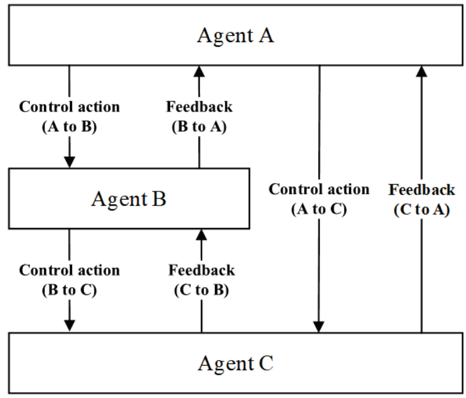

Fig. 1. Exemplary SCS with two-level hierarchy. Blocks represent the system agents, arrows represent the interactions among them.

Note that the controlled processes can be also controllers and *vice versa*. This happens because the SCS usually includes the representation of multiple hierarchical levels. In the simple example presented in **Fig. 1**, it is depicted a two-level hierarchy: "Agent B" is controlled by "Agent A", but, in turn, it controls "Agent C".

3. A SCS for the Seveso III Directive

The Seveso III Directive provides guidance for managing industrial facilities employing dangerous substances in their processes. The Seveso III Directive clearly identifies agents responsible of its effective put in practice, eventually detailing which information they must exchange to fulfill this aim. Several processes can be recognized in the Seveso III Directive (e.g., inspection of establishments, post-accident investigations, consultation with the public); in this paper, we only focus on one of them (i.e., the modification of establishments), eventually showing how known rules can enrich a SCS representation. In particular, **Fig. 2** shows an excerpt of the SCS depicting the STS described in the Seveso III Directive related to the process of the modification of establishments. Following STAMP, six agents have been included (cf. **Fig. 2**):

- *European authorities*. Referring to (i) the European Commission, which is responsible for proposing updates to the Seveso III Directive and overseeing its actual implementation in Member States; and (ii) the European Parliament and the Council of the EU, which approve the Directive and its amendments ensuring that the legislative process reflects the public interest;

- *Competent authorities*. Referring to all the national and/or regional bodies designated by an EU member State to enforce the implementation of the Seveso III Directive within its territory. They are responsible for ensuring that Seveso establishments comply with the requirements of the Seveso III Directive by (e.g.) approving and monitoring safety reports;
- *Operator of establishment (1)*. It is the natural or legal person having the control over the "Industrial establishment (1)" where a dangerous substance is present. The operator is responsible for ensuring that the "Industrial establishment (1)" complies with the Seveso III Directive;
- *Operator of establishment (2)*. It is the equivalent of "Operator of establishment (1)", but referring to a second establishment, namely, "Industrial establishment (2)";
- *Industrial establishment (1)*. It identifies every department, worker, and technical or technological apparatus involved in the processes of the establishment falling under the Seveso III Directive;
- *Industrial establishment (2)*. It refers to another establishment that, in a way similar to "Industrial establishment (1)", falls under the Seveso III Directive.

On the other hand, the relationships among the agents included in **Fig. 2** describe all the feedback loops and the control actions involved in the management of modification to Seveso establishments. Indeed, before starting the establishment's operations, or making any modification to it, the operator shall notify the competent authorities with the so-called notification, which is a sort of ID-card for Seveso establishments (feedback "Notification (1)", and "Notification (2)", cf. **Fig. 2**). The notification shall be updated every time there are: (i) necessary changes that may affect major-accident hazards, permanent facility closures, or any alterations to previously reported information, or (ii) changes in facility processes, potentially affecting the risk management of the establishment. Along with the notification, any establishments changing something in their processes require a review of the safety report, and of the way in which it is practically implemented, i.e., the major accident prevention policy, and the safety management system (feedback "Safety report (1)", "Major accident prevention policy (1)", "Safety management system (1)", "Safety report (2)", "Major accident prevention policy (2)", and "Safety management system (2)", cf. **Fig. 2**).

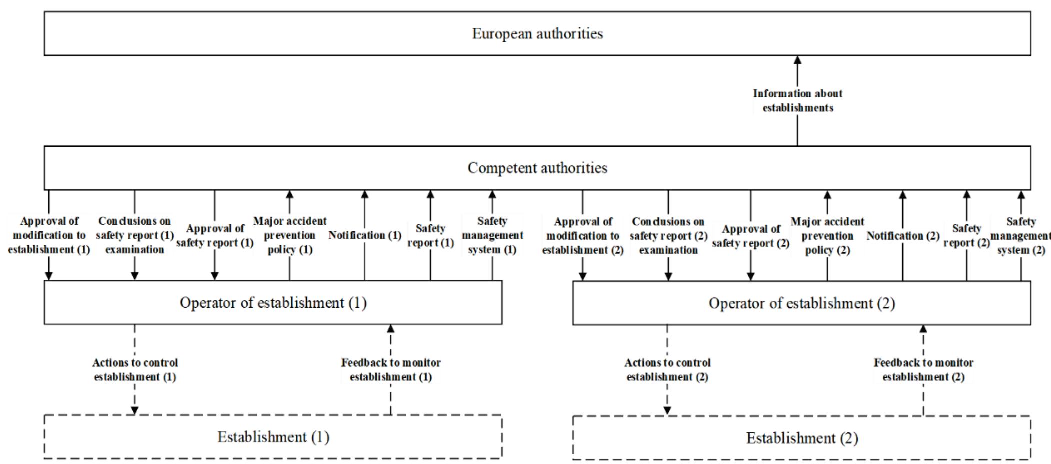

Fig. 2. Excerpt of a SCS mapping the agents identified in the Seveso III Directive and their interactions with respect to the process of modification to establishments. Dashed elements indicate additional hierarchical levels not comprehensively detailed in the figure.

Please note that all the information included in these documents is most likely related to the establishment's operations, thus dependent on the information coming from the lower – and undeveloped, cf. **Fig. 2** – levels of the SCS (feedback "Feedback to monitor establishment (1)", and "Feedback to monitor establishment (2)", cf. **Fig. 2**). Operators must keep the competent authorities updated on changes, obtaining the approval of the safety report before actually implementing the modifications. In particular, the safety report must be submitted for approval within specified time frames, and it requires an update at least every five years.

The competent authorities review the submitted safety report, evaluating the establishment's major accident prevention policy and the safety management system, too, eventually informing the operator of the outcomes of the examination (control actions "Conclusion on safety report (1) examination", and "Conclusion on safety report (2) examination", cf. **Fig. 2**). The competent authorities' conclusions may include actions and recommendations to be implemented in the establishment before the acceptance of the safety report. Accordingly, there is a chance that the safety report and its related documentation is revised by the operator and submitted multiple times before the final acceptance (control actions "Approval of safety report (1)", and "Approval of safety report (2)", cf. **Fig. 2**). If the update of the safety report is related to a modification of the establishment, the approval of the modification must be communicated to the operator, too (control actions "Approval of modification to establishment (1)", and "Approval of modification to establishment (2)", cf. **Fig. 2**).

Even if such a process is mainly associated with the national competent authorities' duties, the European authorities shall be updated of any change in the notification of establishments. Thus, whenever a modification is approved (and consequently the notification changes), the competent authority shall provide updated information to the European authorities (feedback "Information about establishments", cf. **Fig.2**).

3.1. *Explicating the Dependencies of the SCS Elements*

Leveraging the SCS in **Fig. 2** for managing and analyzing safety in a Seveso establishment becomes quite challenging if knowing little with respect to the description of the process in **Section 3**. It is clear how the SCS representation in **Fig. 2** is incomplete and not capable of comprehensively representing the STS it models. To this end, the SCS shall be paired with additional data, meant at explicating the causal and temporal dependencies of the SCS's elements. Accordingly, we propose enriching the SCS in **Fig. 2** with the information included in **Table 1**. This latter assigns each feedback and control action mapped in the SCS to an ID, which is then used for explicating additional information with respect to their existence.

An important consideration is necessary at this point with respect to the difference between what we define as a model, and the model's instantiations. Whether an agent (or a relationship) is meaningful for the STAMP model, it must be chosen by the modeler when defining the scope of analysis. For example, the case presented in this paper focuses only on the modification of establishments, thus, no agent like (e.g.) the inspection authorities have been modeled, even if they are part of the STS described in the Seveso III Directive. The scope of the analysis permits eliciting all the agents and all their relationships having the potential to exist in the SCS.

On the other hand, in a model's instantiation, this potential is – or is not – fulfilled. Accordingly, even if part of the model, some elements may not exist under specific circumstances or may change in time. We highlight two possibilities to describe the existence of the SCS's elements (cf. **Table 1**), which are described in the following paragraphs.

3.1.1. *Causal Relationships*

Causal relationships explicate all the cases in which a SCS's element is causally dependent by another. An element may need another element to exist, or it may be needed by an element to ensure its existence. Thus, causal relationships have been detailed by two subtypes, i.e., "Needed for" and "Needs" (cf. **Table 1**) to depict such possibilities.

For example, the control action CA02 (i.e., "Conclusions on safety report (1) examination", cf. **Table 1**) is necessary for the control action CA01 (i.e., "Approval of safety report (1)", cf. **Table 1**) to exist: if the conclusions on the safety report assessment are not present, there is no chance the safety report can be approved.

Table 1. Causal and temporal relationships (i.e., "CA" means Control Action, "FB" identifies Feedback) of the SCS's elements in Fig. 2. The value "N/A" indicates no available information regarding causal or temporal relationships for the element. The table content written in italic font indicates those actions that are not explicitly mapped in the SCS but trigger – or are triggered by – elements in the SCS.

ID	SCS's element	Causal relationships		Temporal relationships	
		Needed for	Needs	Frequency	Duration
FB01	Information about establishments	N/A	(FB04 and CA03) or (FB08 and CA06)	N/A	N/A
FB02	Safety management system (1)	CA02	FB10 and CA07	N/A	N/A
FB03	Safety report (1)	CA01 or CA02	(FB04 or CA02) and FB10 and CA07	≤ 5 years	5 years
FB04	Notification (1)	FB01 or CA03	*Will to modify establishment (1)*	N/A	N/A
FB05	Major accident prevention policy (1)	CA02	FB10 and CA07	N/A	N/A
FB06	Safety management system (2)	CA05	FB11 and CA08	N/A	N/A
FB07	Safety report (2)	CA04 or CA05	(FB08 or CA05) and FB11 and CA08	≤ 5 years	5 years
FB08	Notification (2)	FB01 or CA06	*Will to modify establishment (2)*	N/A	N/A
FB09	Major accident prevention policy (2)	CA05	FB11 and CA08	N/A	N/A
FB10	Feedback to monitor establishment (1)	FB02 and FB03 and FB05	N/A	N/A	N/A
FB11	Feedback to monitor establishment (2)	FB06 and FB07 and FB09	N/A	N/A	N/A
CA01	Approval of safety report (1)	CA03 or CA07	FB03 and CA02	N/A	N/A
CA02	Conclusions on safety report (1) examination	CA01	FB02 and FB03 and FB05	N/A	N/A
CA03	Approval of modification to establishment (1)	*Modify establishment (1)*	CA01 and FB04	N/A	N/A
CA04	Approval of safety report (2)	CA06 or CA08	FB07 and CA05	N/A	N/A
CA05	Conclusions on safety report (2) examination	CA04	FB06 and FB07 and FB09	N/A	N/A
CA06	Approval of modification to establishment (2)	*Modify establishment (2)*	CA04 and FB08	N/A	N/A
CA07	Actions to control establishment (1)	FB02 and FB03 and FB05	N/A	N/A	N/A
CA08	Actions to control establishment (2)	FB06 and FB07 and FB09	N/A	N/A	N/A

Regarding (e.g.) FB02 (i.e., "Safety management system (1)", cf. **Table 1**), instead, both FB10 (i.e., "Feedback to monitor establishment (1)", cf. **Table 1**) and CA07 (i.e., "Actions to control establishment (1)", cf. **Table 1**) shall be present: no safety management system is in place if no feedback or control is acting on the establishment.

3.1.2. *Temporal Relationships*

Temporal relationships explicate whether a SCS's element is dependent on time. An element may exist only at certain moments in time, or it may be characterized by a specific duration before disappearing. Thus, also temporal relationships have been detailed by two subtypes, i.e., "Frequency" and "Duration" (cf. **Table 1**).

Regarding the former, a temporal relationship of type frequency depicts every SCS's element that shall be provided repeatedly, following a rule that specifies its update every time a given period passes. It is the case of (e.g.) FB03 (i.e., "Safety report (1)", cf. **Table 1**) that, following the Seveso III Directive, must be provided at least every five years. Accordingly, FB03 has a frequency of emission of less than five years.

On the other hand, a temporal relationship of type duration details the validity of a SCS's element, if any. Accordingly, there can be rules stating that (e.g.) a feedback is valid only for a given time frame, making it non-existent after that time passes. For example, if considering FB03 (i.e., "Safety report (1)", cf. **Table 1**), again, the Seveso III Directive sets out its validity at five years – which is, indeed, the reason it shall be updated over and over.

3.1.3. *What about Agents?*

By looking at **Table 1**, it is possible to notice how only feedback loops and control actions have been included in it, and there is no track of agents. Indeed, the existence of an agent in a instantiation of the SCS has been considered strictly dependent on the existence of feedback loops and control actions they are actually receiving/sending in the instantiation. Whenever an agent is disconnected from the others, it is not meaningful for that specific instantiation of the model, even if it has been thought worthy at the model level.

For example, if FB04 (i.e., "Notification (1)", cf. **Table 1**) and CA03 (i.e., "Approval of modification to establishment (1)", cf. **Table 1**), or FB08 (i.e., "Notification (2)", cf. **Table 1**) and CA06 (i.e., "Approval of modification to establishment (2)", cf. **Table 1**) are not present, FB01 (i.e., "Information about establishments", cf. **Table 1**) cannot be sent in the instantiation. In other words, there should be a change from at least one establishment to be communicated to the European authorities to let FB01 be meaningful. Consequently, if the European authorities receive no feedback in the specific instantiation, they become, in turn, not meaningful for the STS representation.

4. Concluding Remarks

In this paper we argue that integrating additional data within the scope of a SCS is an added value for the STAMP implementation. This awareness emerged during the conduction of the RESET project, in which we are currently analyzing the STS described in the Seveso III Directive with respect to energy transition scenarios. STSs are – by definition – complex, and in the complexity domain it is difficult to comprehensively explain system behaviors (Snowden, 1999). However, STSs are often subjected to known rules (e.g., legislations, best practices, directives), which – somehow – affect their operations. This happens for the STSs described in the Seveso III Directive, which is – obviously – subjected to a set of known rules and prescriptions.

When analyzing the system by employing the STAMP, we noticed how such known rules are difficult to consider in the system SCS, leaving their inclusion to the subjectivity of the analyst. Considering additional information when developing the system SCS permits evaluating whether its elements exist or not under specific instantiations, eventually adding a sort of dynamic dimension to the traditionally static SCS representation. This dynamicity is related to the definition of specific triggers for the SCS elements' existence, i.e., causal and temporal relationships.

In practice, the inclusion of causal and temporal relationships is here – preliminarily – outlined in a tabular form as complement to the SCS representation. However, this information could alternatively be incorporated directly into the SCS as metadata, establishing links to its elements.

This integration could be achieved through various mode of implementation, such as (e.g.) using graphs for mapping the causal relationships, or employing time-dependent equations for representing temporal dynamics.

The need for dynamicity in STAMP had been already acknowledged in the literature, with Leveson (2018) stressing the need to apply STPA considering multiple stages of a system lifecycle to ensure its effectiveness. On this path, a common research stream relies on System Dynamics principles to study the dynamically changing relationships among causal factors (Dulac et al., 2005). Recently, leveraging STAMP to guide simulations emerged as a way to consider system dynamic behaviors in STPA applications (Simone et al., 2023). Nevertheless, none of these approaches ensure a dynamic dimension to be embedded in the SCS representation but only added afterwords.

Additional formalization is still needed to generalize the ideas presented in this paper, and their effectiveness should be better demonstrated with a more comprehensive case study. However, these early results include some interesting insights on the benefits – and even the need – to add a dynamic dimension to a SCS when behaving rules are known – which is the case of most real-life applications of STAMP.

Acknowledgement

The authors would like to acknowledge the support of INAIL (National Institute for insurance Against Accidents at Work). This work is funded through the project "RE-SET: Resilience Engineering for Safe Energy Transition" under the INAIL BRIC 2022 funding scheme.

References

Dulac, N., Leveson, N., Zipkin, D., Friedenthal, S., Cutcher-Gershenfeld, J., Carroll, J., & Barrett, B. (2005). Using system dynamics for safety and risk management in complex engineering systems. *Proceedings - Winter Simulation Conference, 2005*. https://doi.org/10.1109/WSC.2005.1574392

Emery, F. (2016). Characteristics of Socio-Technical Systems. In *The Social Engagement of Social Science, Volume 2*. https://doi.org/10.9783/9781512819052-009

Eskenazi, B., Mocarelli, P., Warner, M., Needham, L., Patterson, D. G., Samuels, S., Turner, W., Gerthoux, P. M., & Brambilla, P. (2004). Relationship of serum TCDD concentrations and age at exposure of female residents of Seveso, Italy. *Environmental Health Perspectives*, *112*(1). https://doi.org/10.1289/ehp.6573

European Council. (2012). Directive 2012/18/EU On the control of major accident hazards involving dangerous substances. *Official Journal of the European Union*, *L197*, 1–37.

Leveson, N. (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. (2012). Engineering a safer world: systems thinking applied to safety. In *Choice Reviews Online*. The MIT Press. https://doi.org/10.5860/choice.49-6305

Leveson, N. (2018). *STPA Handbook*. The MIT Press.

Patriarca, R., Chatzimichailidou, M., Karanikas, N., & Di Gravio, G. (2022). The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. *Safety Science*, *146*(105566). https://doi.org/10.1016/j.ssci.2021.105566

Simone, F., Akel, A. J. N., Gravio, G. Di, & Patriarca, R. (2023). Thinking in Systems, Sifting Through Simulations: A Way Ahead for Cyber Resilience Assessment. *IEEE Access*, *11*, 11430 – 11450. https://doi.org/10.1109/ACCESS.2023.3241552

Snowden, D. (1999). Liberating knowledge. *Liberating Knowledge 1*.