Integral Safety Layers for Residential System Development

Mohammad Rajabali Nejad
Department of Design, Production, and Management
University of Twente
Enschede, the Netherlands
e-mail: M.Rajabalinejad@utwente.nl

Chua Eu Chieh
Student of Mechanical Engineering
University of Twente
Enschede, the Netherlands
e-mail: chuaec2@gmail.com

***Abstract*—Integrally safe, or integral safety, is a challenge because safety is in different hierarchical layers across the entire life cycle for products and systems. Safety is beyond a specific layer, and challenges for safe integration are present through the complete chain of hierarchy. The system hierarchy helps to understand the system as a part of an integral whole, composed of components which interact with its environment. This paper provides an overview of integral safety, aiming to present an organisational view of the system's structure under consideration both internally and externally through the concept of safety layers. The paper builds upon the currently established hierarchical concepts and explains how the concept is applied in the tiny house project, where technology was successfully integrated with residential areas.**

Keywords - Safety layer; product safety; system integration; hierarchy.

I. INTRODUCTION

A hierarchy is an arrangement of items (objects, names, values, categories, etc.) in which the items are categorised as being 'above', 'below', or 'at the same level' as one another. According to the Oxford English dictionary, levels in a hierarchy may also represent authority, control or ownership of lower levels (command structure). It is important to note that the depth of the hierarchy is adjusted to fit the complexity of the system. Moreover, for the sake of efficiency, a system may focus on specific levels. Logical hierarchy, also known as a conceptual order, has uses in various disciplines, such as risk assessment or system governance as presented by [1]. Leveson had proposed the hierarchy model called the Systems-Theoretic Accident Model and Processes (STAMP) as an alternative safety incident investigation and to improve the performance analysis of a system [2].

The logic of hierarchy is closely related to the sequence of integration. In engineering practices, creation comes before integration. That is a logical approach where the functionalities are first identified, the systems and subsystems are designed, and then the components or subsystems are built and integrated. Systems engineering discipline pays extra attention to the importance of integration. It defines the purpose of the integration process as 'to synthesise a set of system elements into a realised system (product or service) that satisfies system requirements, architecture, and design', see [3]. This discipline mainly focuses on subsystems and integration. The concept of integration has been extended from just a technical integration in various literature, for example, [1] [4]. This study aims to propose a framework for integrating the technical and non-technical elements.

The rest of the paper is structured as follows. In section 2, we introduce the seven layers for safe integration introduced in [4], [5]. Then, in Section 3, we present its application to the LIFE project. And finally, in Section 4, we offer our conclusions.

II. LAYERS OF SAFE INTEGRATION

Through the concept of hierarchy, safe integration starts with the integration of components, where a combination of two or more parts or elements makes a subsystem. Then, integrating all the subsystems together with the human interactions results in the technical system. Integration of humans with the technical system is known as system integration. The integration of various systems is also known as systems integration or System of systems (SoS). SoS need to offer social services to function, and that leads to sociotechnical integration. National governments' control and monitoring of sociotechnical systems reflect the conformity with societal values regarding national norms, standards, and policies. And they also need to comply with regional, continental, or international regulations. Each integration layer applicable for safe products or systems is elaborated on below.

1) Safe integration of subsystems refers to a combination of two or more components or elements that make a subsystem. Subsystems or components are parts of a system and often do not function independently. Therefore, component integration or subsystem integration is often the earliest action in physical integration. The integration of components often occurs in the production or assembly stage.
2) Safe integration of technical system refers to the integration of components, elements or subsystems, or human interactions to realise a system that accomplishes the system objectives. In the system engineering community, a system is defined as 'an integrated set of elements, subsystems, or assemblies that cooperate to accomplish

 ISBN: 978-1-61208-943-0

a defined objective'. These elements include technological products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements, according to [6]. The Systems Engineering (SE) handbook defines integration as a technical process making integration of the elements of a system possible. In this context, successful system integration is a system that works and delivers the required functionalities without failures. The failures that happen in this process are seen as defects of a component or interface. At this level, the main focus is on components, subsystems, or interfaces. The SE Handbook does recognise that the integration of humans and systems is not a technical process and therefore recommends focusing on human systems integration (HSI) across the design or engineering of systems instead.

3) Safe integration of humans with technical system (HTSI) refers to the integration of the humans and technical systems. HTSI focuses on the human, an integral element of every system, over the system life cycle. It is an essential part of engineering systems, as it promotes a 'total system' approach that includes humans, technology (e.g., hardware and software), the operational context, and the necessary interfaces between and among the elements to make them all work in harmony, see [7].
   HTSI ensures consideration of the human in the system capability definition and system development. Here, the human is considered an element of the system; its integration with the system must be fully accomplished. It includes domains, such as human factors engineering (human performance, human interface, user-centred design), workload (regular and emergency), training (skill, education, attitude), personnel (knowledge, attitudes, career progression), working conditions and health (ergonomics, occupational standards, and hazard and accident avoidance), e.g. [6].
4) Safe integration of System of Systems refers to the integration of two or more systems. According to [8], a system of systems is a set of systems and system elements that interact to provide a unique capability that none of the individual systems ever could accomplish on their own. A system of systems is, in itself, wholly integrated. Also, it has elements that are managerially or operationally independent. Mo Jamshidi considers integration as the critical viability of any system made of systems [9]. To achieve optimal results, having shared objectives among organisations, co-creation of desired capabilities and co-integration of interoperable services are crucial to success, according to [10].
5) Safe integration with sociotechnical systems focuses on the integration of the system of systems or related services with society. In other words, a system of systems needs to be up-to-date with social demands in order to function optimally. A system of systems requires to conform to regulations, norms, values, and culture [11]. For example, the language of communication has an impact on the sustainable performance of the system of systems [12].
6) Safe integration with political system refers to the control or monitoring of sociotechnical systems by national governments and makes societal policies. Governments have the task of controlling sociotechnical systems while maintaining societal values and policies. Organisational chains of responsibility, authority, and communication ought to measure and control mechanisms to effectively drive the organisation and enable people to perform their roles and responsibilities, see [13].
7) Safe integration with global system refers to shared concerns of human societies which may, for example, be represented by international regulations. Globally essential considerations, such as the use of green energy, reducing the usage of fossil fuels, and minimising CO_2 emissions.

An illustration of the layers is provided via the application of the concept, which is described in Section 3.

III. Example application

A. Introduction to LIFE

The University of Twente, in 2019, initiated the 'Living project for Future Innovative Environments' project or more conveniently referred to with its acronym 'LIFE'. The project aimed to research the interplay between the technology, humans and the infrastructure system in supporting society's transition towards a future of low carbon footprint, climate-friendly living, and a circular economy [14]. Ten small-and-medium enterprises around the Twente region, known as the LIFE Project Partners, contribute to the project over the entire lifecycle, starting from conceptual design to equipment installation, support, maintenance and eventual disposal.

The aspiration is that the residential buildings become autarkic, meaning that they are self-sufficient in water and energy. Solar panels will be used to generate electricity and capture heat. A hydrogen system and batteries will act as electrical energy storage, charged and discharged cyclically. Heat is stored in an underground buffer and distributed via a heat pump throughout the house. Rainwater is harvested and treated before use. Used water is also treated and re-used wherever possible. The conceptual idea of LIFE can be seen in Figure 1.

The project will span over ten years, with six 'tiny house' units built initially as a pilot and function as 'living labs'. Energy generation and consumption data will be collected to enable researchers to evaluate the residents' interaction with installed technology.

B. Integration levels in the project

The hierarchy of integration for the LIFE project can be depicted in Figure 2. Various elements of the project residing at each hierarchy level are represented by dots. Lines connecting the dots suggest a direct influence, or interaction, between the elements. The elements within each hierarchy were identified simply from a brainstorming exercise.

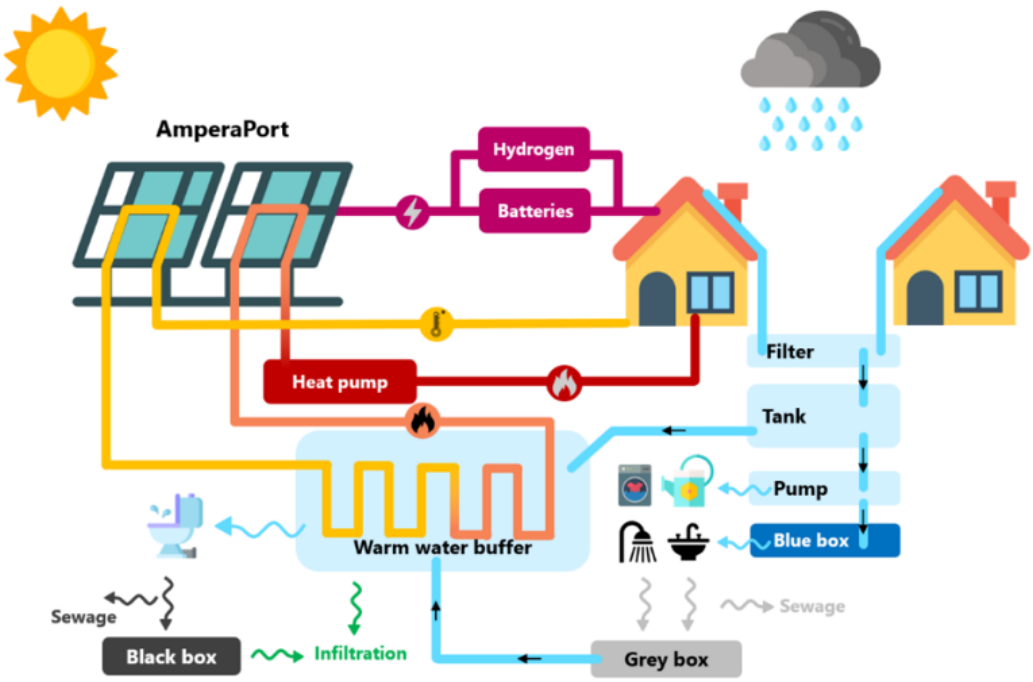

Figure 1. Conceptual depiction of the LIFE Project. Graphics from the LIFE project documents [14]

The inner-most box contains the various subsystems. Collectively, these subsystems are integrated to form the technical system, i.e., the 'tiny house'. The figure does not make a rigid distinction between components, subsystems, and systems. For example, the thermal energy subsystem consists of several components, of which a few are depicted in the figure. The electrical energy storage subsystems comprise several battery types and a hydrogen system. The hydrogen system can be broken down further into equipment and components used in hydrogen production and storage and the fuel cells.

The 'tiny house' technical system naturally has interfaces with human elements at the various asset lifecycle phases. For example, during the 'design' and 'construction' phases, the 'tiny house' has the most interaction with the building designer, builders and subsystem providers. In contrast, the homeowner, inhabitants and the facility manager come to the fore during the 'use' and 'disposal' phases.

Human systems integration is critical to ensure that the LIFE system's envisioned benefits can be realised. For example, human-related activities, such as misoperations and mistakes during maintenance, account for most hydrogen subsystems accidents [15]. Therefore, proper communication and systematic sharing of information among the relevant stakeholders are essential to reduce the human-factor failures during all phases of an asset lifecycle.

The 'tiny houses' exist within a more extensive system of systems, interacting with elements, such as the electrical, water and sewage network. Should a complete autarky design be impossible, the 'tiny houses' are connected to the local water, electricity, and sewage grid. Even if total autarky can be achieved, the 'tiny houses' must be connected to the University of Twente's emergency response system since it is considered a working laboratory. The laboratory administrators must comply with existing procedures for managing hazardous activities and the organisational structure of the emergency response.

The sociotechnical system integrates the social aspects with the system of systems. For instance, society's acceptance of 'tiny houses' is underpinned by the ability to satisfy environmental concerns and affordability while also providing a quality of living. Assurance is also needed that the novel technologies deployed, such as the electrical energy storage subsystems, do not endanger public safety. There is also the expectation that research organisations contribute to society's advancement by providing empirical data and being a catalyst for innovation. The LIFE project's 'living lab' concept enables researchers to collect information about society's energy consumption behaviour - from a small control group with above-average skills and capability in using novel technologies - when living in a building equipped with relatively state-of-the-art energy systems.

The political system balances the need to protect consumers, avoid the potential unintended consequences of technological disruption, and foster innovation. Government bodies create, maintain and enforce regulations in line with national policies and laws. Commercial bodies also are interested in trends that can impact their business model.

Following the example of energy storage subsystems,

 ISBN: 978-1-61208-943-0

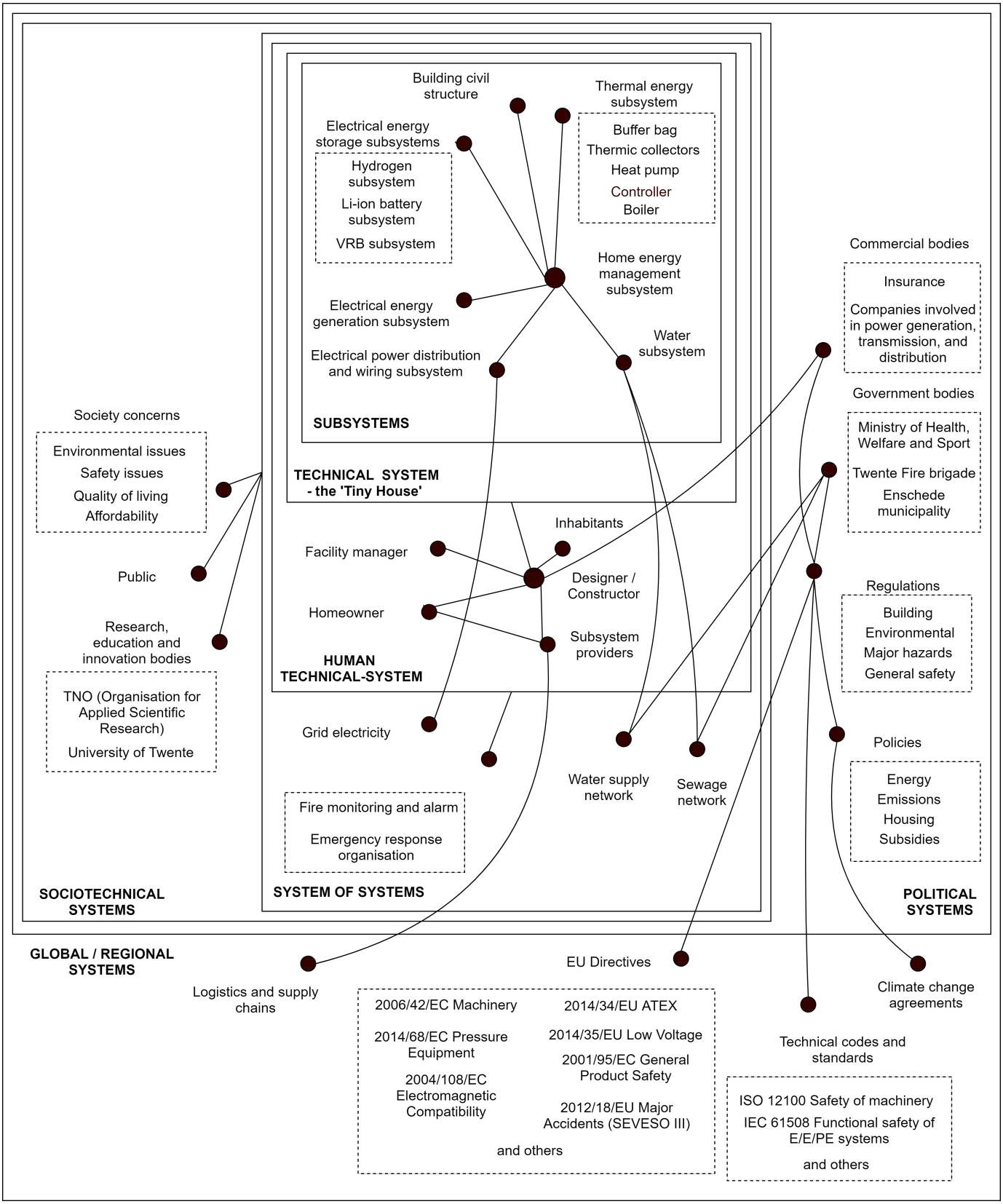

Figure 2. Hierarchy of integration of the LIFE project.

energy-related national policies and regulations should be aligned to remove implementation barriers. For example, hydrogen is considered an industrial gas subject to strict legal and safety requirements in the Dutch context. Therefore, the installation of hydrogen systems in residential zones would still require compliance with national legislation similar to that of industrial sectors, such as the 'Major accidents decree (BRZO), the 'Public Safety Decree' (BEVI), the 'Spatial Planning Act' (WRO) and the 'General Provisions Environmental Legislation Act' (WABO) [16]. On the other hand, regulations around using batteries in residential buildings are less restrictive, leading to situations where more guidance would help manage the associated safety hazards.

Commercial interests would also need to be considered. Insurance companies providing cover for buildings equipped with novel energy generation and storage technologies would naturally strive to balance profitability with risks by seeking more assurance of such equipment's safety levels. In addition, stakeholders involved in power generation, transmission and distribution would be interested in emerging trends that impact revenue and expenditures.

At the all-encompassing hierarchical level, global or regional systems represent the various concerns of the worldwide society. Internationally-adopted agreements, such as the Paris Agreement 2016, provide the impetus for changes in national policies around funding and technology deployment to reduce greenhouse gas emissions. Such a mandate makes a clear case for the need for energy storage technology. EU directives necessitate some changes in its member states national laws, while harmonised standards become references for national standards and regulations. According to van der Meer et al., the five EU directive that affects the deployment of hydrogen technology are the Major Accident Hazards Directive 2012/18/EU ("Seveso III"), ATEX Directive 2014/34/EU (the recast of "ATEX 95"), Industrial Emissions Directive (IED) 2010/75/EU, Strategic Environmental Assessment (SEA) Directive 2001/42/EC and the Environmental Impact Assessment (EIA) Directive 2011/92/EU [16]. In addition, Laumann et al. mentioned that hydrogen systems would need to obtain the 'CE' mark by complying with these directives: Machinery Directive 2006/42/EC, Low Voltage Directive 2014/35/EU, Electromagnetic Compatibility Directive 2004/108/EC, Pressure Equipment Directive (PED) 2014/68/EC and ATEX directives [17].

The technical standards can address safety, quality and cost concerns for designers, producers, installers, and end-users and reduce market barriers for products. For instance, the recently published NEN 4288 by the Royal Netherlands Standardization Institute is expected to provide clarity and guidelines around the safe use and operation of batteries storage technologies in homes by business providers. This standard, in turn, should help assure end-users of the safety of battery systems [18].

C. Discussion

The safety layers can describe how technologies are interrelated with individuals, organisations, other supporting systems, the society, and (inter)national authorities in a broad ecosystem. In general, all the layers for safe integration are mutually supportive of one another. For example, the acceptance of buildings conceptually similar to the LIFE project could be high if there is public trust in its safety and the perception that such a design can effectively reduce the carbon footprint of society's lifestyle.

It should be noted that the elements within each layer could be competing with one another (e.g., commercial versus society concerns) or setting constraints for others (e.g., regulations vs innovation). These interactions need to be evaluated during a product's conception.

By applying the safety layers to the LIFE project, we learned that a system integrator could use the hierarchy of integration to identify a stakeholder map to aid the communication and information flow between the various stakeholders and system elements. Safety hazards can be systematically identified through these interactions, and the risks assessed accordingly. The priorities and concerns of each stakeholder might differ and need to be considered. For example, the subsystem provider's most significant concern would be whether the supplied subsystems are inherently safe, while the first responders' foremost concern is personnel safety.

With this, we summarise our observations through the following propositions:

- From the methodological point of view, we find it necessary to distinguish between the 'technical system' and the 'humans' who interact with the system aiming for safe integration. Therefore, although it may sound trivial, we find it helpful to use 'human and technical system integration' instead of 'human system integration'. That makes the integration goals more transparent. In other words, as smart appliances and novel technology become more pervasive in our daily lives, we propose that the 'human and technical system integration (HTSI)' provides more transparency for achieving safe integration as practised in system safety discipline.
- We observed that integration at the technical system level is different from integrating humans with a technical system. Therefore, we propose that humans are not best described as a subsystem or an element of the system (as conventionally practised by systems engineering discipline) but are considered a separate category.
  We suggest that the conventional view may imply that technical tools are meant to provide a higher level of control when in principle, it should be humans that should dictate the manner of their interaction with technology. The latter perspective requires a different starting point of a technology's design philosophy, utilising a more diverse set of knowledge, tools, and methods.

 ISBN: 978-1-61208-943-0

IV. Conclusions

The seven layers for safe integration, described in this paper, create the 'big-picture' of the residential system development. The starting integration levels (e.g., technical system or system integration) align with the systems engineering standard practice. Yet, the proposed approach encourages the designer to look beyond the direct system stakeholders or system environment. The integration considerations beyond the technical system are rather critical for introducing new technologies.

We also observed that a clear distinction between the technical system and the humans in the system provides further transparency into what the LIFE project is meant to deliver.

The LIFE project was still in development at the time of this study, and the operational aspects of the project need further elaborations.

Acknowledgement

The authors acknowledge the support of all the collaborators for the LIFE project, including Y.Hajimolana, M.Winkler, G.Hoogsteen and the Project Partners, such as SuperB, HyGear and Volterion and Brandweer Twente. The co-author Eu Chieh was a Master's student at the University of Twente when this paper was written, but he has since graduated.

References

[1] N. Leveson, *Engineering a Safer World*. Cambridge, Massachusetts, London, England: Massachusetts Institute of Technology, 2012.

[2] N. Leveson, "A new accident model for engineering safer systems," *Safety science*, vol. 42, no. 4, pp. 237–270, 2004.

[3] D. D. Walden, G. J. Roedler, K. J. Forsberg, R. D. Hamelin, and T. M. Shortell, *Systems Engineering Handbook A Guide For System LiFe Cycle Processes And Activities*. International Council on Systems Engineering (INCOSE), 2015.

[4] M. Rajabali Nejad, L. Dongen, and M. Ramtahalsing, "Systems integration theory and fundamentals," *Safety and Reliability*, vol. 39, no. 1, pp. 83–113, 2020.

[5] M. Rajabali Nejad, *Safety by Design Engineering Products and Systems*. first ed., 2020.

[6] ISO, IEC, and IEEE, *ISO/IEC/IEEE 15288, First edition 2015-05-15, Systems And Software Engineering — System Life Cycle Processes*. ISO/IEC/IEEE 15288:2015(E), Switzerland: International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronics Engineers, Inc., 2015.

[7] ISO, IEC, and IEEE, *ISO/IEC/IEEE 29148 Systems And Software Engineering —Life Cycle Processes — Requirements Engineering*. Switzerland: International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronics Engineers, Inc., 2011.

[8] ISO, IEC, and IEEE, *ISO/IEC/IEEE/DIS 21840 Systems And Software Engineering — Guidelines For The Utilization Of Iso/Iec/Ieee 15288 In The Context Of System Of Systems (Sos) Engineering*. Switzerland: International Organization for Standardization, International Electrotechnical Commission, Institute of Electrical and Electronics Engineers, Inc., 2019.

[9] M. Jamshidi, "System of systems engineering new challenges for the 21' century," *IEEE Aerospace and Electronic Systems Magazine*, vol. 23, no. 5, 2008.

[10] A. M. Madni and M. Sievers, "System of systems integration: Key considerations and challenges," *Systems Engineering*, vol. 17, no. 3, pp. 330–347, 2014.

[11] D. M. Woo and K. J. Vicente, "Sociotechnical systems, risk management, and public health: comparing the north battleford and walkerton outbreaks," *Reliability Engineering and System Safety*, vol. 80, no. 3, pp. 253–269, 2003.

[12] K. Davis, T. Mazzuchi, and S. Sarkani, "Architecting technology transitions: A sustainability-oriented sociotechnical approach," *Systems Engineering*, vol. 16, no. 2, pp. 193–212, 2013.

[13] M. Cantor, "Cantor, m. 2006. estimation variance and governance. in ibm developerworks. accessed on 15 september 2011.," *IBM developerWorks. Available online at http://www.ibm.com*, vol. Available at http://www.ibm.com, 2006.

[14] E. C. Chua, *Management of safety hazards in residential buildings with multiple electrical energy storage systems*. Msc, University of Twente, 2021.

[15] Y. Suwa, H. Miyahara, K. Kubo, K. Yonezawa, Y. Ono, and K. Mikoda, "Design of safe hydrogen refueling stations against gas-leakage, explosion and accidental automobile collision," in *Proceedings of the 16th World Hydrogen Energy Conference*, vol. 139, Citeseer, 2006.

[16] J. van der Meer, R. Perotti, and F. de Jong, "Hylaw national policy paper for the netherlands," 2018.

[17] F. Laumann, F. Verbecke, A. Duclos, A. Zanoto, and L. Zhiyong, "Description of selected fch systems and infrastructure, relevant safety features and concepts, delivery 2.1," 2015.

[18] NEN, *NEN 4288:2020 Bedrijfsvoering van batterij-energieopslagsystemen - Aanvullende eisen op NEN 3140*. Vlinderweg 6, 2623 AX Delft: NEN - Royal Netherlands Standardization Institute, 2020.

 ISBN: 978-1-61208-943-0