A Systemic Approach for Safe Integration of Products and Systems

Mohammad Rajabalinejad
Department of Design, Production, and Management
University of Twente, Enschede, the Netherlands
Email: M.Rajabalinejad@utwente.nl

***Abstract*— Safe integration is an unresolved issue across different disciplines, and many problems happen due to improper integration of a product or system. Safe integration is beyond technical integration and requires both technical and nontechnical knowledge. This paper highlights the scope of integration challenges and sheds light on safe integration. It outlines a systemic view of safe integration and provides an example application for further clarification.**

Keywords - systems integration; safe integration; integration engineering; Safety Cube.

I. INTRODUCTION

Our society is becoming less tolerant to safety failures while it demands up-to-date technologies. People require seamless integration of new technologies with everyday life. We need products and services that are effortlessly usable in different contexts. Given the increasing complexity of high-tech systems, there is a need for new methods and techniques to support proper integration of newly developed systems or products. The challenge is far beyond technical installations and more than the integration of hardware, software, and human for a single product or system. The high pace of technological developments demands strategies that not only fulfil the technical requirements but also successfully address interoperability and dependability of systems, data integrity, security, or privacy matters. The main drivers and ingredients for safe integration are presented in Figure 1.

Integration creates a unique selling point for businesses. For example, Apple is conscious about seamless integration among its products aiming to deliver the ultimate use-experience for the users. In brief, proper integration is a prerequisite for a modern society. In the previous work [1], the author provides several examples of systems challenges for the rail industry. Yet, the scope of integration challenges crosses different industries.

The public is sensitive to integration failures imposing extra costs and resources [2]. Examples of needs for integration are across different disciplines and industries. Augmented Reality (AR) and its integration with human-life in the form of camera, wearables, games, or education are examples for the need for safe integration of technology with everyday life. Artificial Intelligence (AI) is another

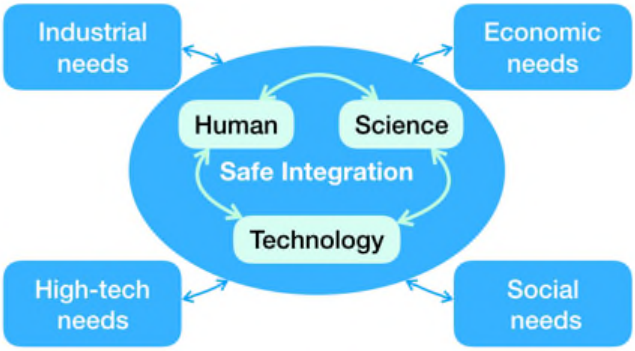

Figure 1. Drivers for safe integration

example where machines are being used to facilitate higher capabilities and performances. Here, safe integration is required at different levels. The first level of integration is superposition of components to make a product. If the components are properly put next to each other, then the product as a whole should be properly integrated and used. This is the second level of integration. For the third level of integration, the product has to be properly integrated into the environment and be safely used. Integration issues happen at all these levels, and the issues can go beyond technical matters. Figure 2 presents three different examples for the integration problem for bicycles. In all these three cases, the issues were dangerous to users and therefore the products were pulled out of the European market. Figure 2.A presents a city bike which was recalled under alert number A12/0134/19. The defect in the front mudguard may block the front wheel of this bicycle during the use and lead to an accident. Figure 2.B shows a children's bicycle where the nuts on the cranks have sharp edges, and they may harm children during the riding or maintenance of the bicycle. This product, which was recalled under the alert number A11/0066/17, is an example of faulty design with regard to human-product integration. The third example, Figure 2.C presents a bike which suffers from defective sealing for its batteries which may result in accumulation of humidity inside the battery and cause overheating and self-ignition. This is an example issue for integration of a product with its environment. This product was recalled under the alert number A12/0497/15.

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-698-9

(A) Recall of the product from end users in Europe (example of internal integration issues)

(B) Recall of the product from end users in Europe (example of product-user integration issues)

(C) Recall of the product from end users in Europe (example of product-environment integration issues)

In addition to highlighting the needs for integration, this paper reviews currently used tools and discusses the ingredients for safe integration. Section II provides a review of tools and techniques. The outcomes have been further discussed in Section III, where a systemic approach for safe integration is described. Section IV presents an example application for the safe integration of bicycles to the urban system. Conclusions are drawn in Section V.

II. SAFE INTEGRATION

Safe integration starts with a proper understanding of the stakeholders and their needs. Systems Engineering handbook highlights the human system integration (HSI). HSI considers domains such as human factors engineering (human performance, human interface, user centred design), workload (normal and emergency), training (skill, education, attitude), personnel (ergonomics, accident avoidance), working condition and health (hazard avoidance) [3]. These domains have direct links to safety. As a matter of fact, integration is similar to safety from several perspectives inheriting a multidisciplinary nature where different techniques and methods can be used for safe system integration. The Swiss cheese model of accidents developed by J.T. Reason presents a model for integration of different system layers in which the risk of a threat may become a reality [4]. The failure mode and effect analysis (FMEA) helps finding potential failure modes for hardware, software, or processes. The fault tree analysis is a systematic approach to present the possible faults related to a specific event. For analysing the operability problems, hazard and operability analysis (HAZOP) is used. The root cause analysis (RCA) focuses on the positive and negative consequences of events. ISO 12100, the reference standard for safety of machinery, pays special attention to safety matters during assembly of a machine or its integration with the surrounding environment [5]. IEC 61508 a seminal standard for functional safety delivered in several parts. Its first three parts focus respectively on general requirements, requirements for E/E/PE, and requirements for software for safety-related systems. Part 1 of this standard addresses issues on system safety validation and system integration (tests) including architecture, software, and PE integration tests. Part 2 addresses the module and system integration for safety-related systems, and Part 3 focuses on software testing and integration. Integration is comparable with safety inheriting multidimensional problems where stakeholders with shared goals need experience and technology to make proper decisions and remove, minimise, or control the risks. Technology readiness level (TRL), integration readiness level (IRL), safety by design and safety cubes are the methods to ensure better integration of products or systems.

As a result of reviewing these references, three common blocks have been identified for these as discussed earlier in [1]. Human (or people), system and environment are the

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-698-9

three building blocks for both of the design process and safety management process.

III. PRINCIPLES FOR SAFE INTEGRATION

One of the primary tasks for engineering design, systems engineering, or risk management is to ensure seamless and safe integration of a system with its environment. In this perspective, dealing with relations among the system, subsystems, environment, and people is of primary concern. These relations, or the so-called interfaces, represent one of the core issues for proper integration. Figure 3 schematically shows the main building blocks for safe integration and their relations. These are principles elements of the so-called safety cube, will be discussed in further details next.

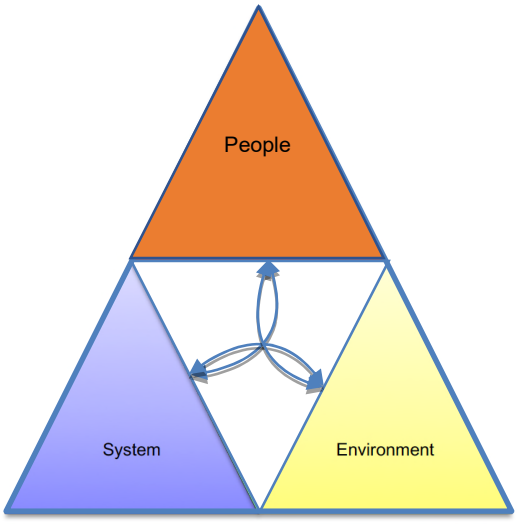

Figure 3. Elements of safe integration and the safety cube.

A. Human

Human or people in this context refers to individual or group of individuals who have connections to the system of interest. They can be stakeholders, designers, users, operators, owners, service providers, producers, or other humans who directly or indirectly have interest in the system and cooperate or compete with it. People have their own individual or organisational culture.

B. System

System refers to the system (or product) of interest that delivers the required functions. The system of interest is independent, and it can be a part of a system of systems. The system includes subsystems or components that form its structure to deliver the required functions under its specific behaviour. Equipment, facilities, and procedures for operation are parts of the system.

C. Environment

Environment includes the system of interest, the cooperating systems, and the competing systems which influence the system of interest. This excludes people which have been discussed earlier. Relevant regulations, industry standards, or supporting facilities are part of the system environment.

D. Human-system relation

Human can have different roles and consequently different relations with the system of interest. For a system, the user, stakeholder, operator, owner, or supplier may have different, competing, or even conflicting interests. This relation can be in the form of (physical) interface, operation, control, maintenance, or cognitive which can directly or indirectly influence the system. Operational and safety culture influences human-system relation.

E. System-environment relation

The system of interest connects to its environment. The relation between a system and its environment is often seen in the form of interfaces for technical installation under three categories of structure, information, and energy. It is important to note that the system is also under the influence of regulations, policy, and political interests of the environment.

F. Human-environment relation

Although, the relation between human and environment often falls out of the scope of system of interest in technological design, it has dominant influence on the system of interest. Change of regulations in a dynamic and competitive (geo)political context, policy making and governance are examples of human-environment relations. This often becomes very complex for systems where multiple stakeholders are involved.

To summarise, Table I provides an overview for the outcomes of this section. This is the information needed for forming a safety cube. The diagonals of this table specify the human, system, and environment for the system of interest where the other cells provide information about the connection between diagonals. The off-diagonals have to be read clock-wise in such a way that the associated row provides input for the associated column. For example, the

TABLE I. THE ELEMENTS OF SAFETY CUBE FOR SAFE INTEGRATION

	Human	*System*	*Environment*
Human	users, direct/indirect stakeholders, operators	human input for the system, intended use or misuse scenarios	human input for environment or its system of systems, use or misuse scenarios
System	system inputs, functions, malfunctions, or services for human	system of interest, its structure, functions, procedures, …	system input for environment, intended use or misuse scenarios
Environment	environmental inputs, functions, malfunctions, or services for human	environmental inputs, functions, malfunctions, or services for the system	cooperating or competing systems, physical environment, policy, regulations

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-698-9

human-system cell at the top row describes the human output as input for the system whereas the system-human cell at the second row describes the system output as input for human.

Table I summarises the system definition and provides an overview of the building blocks and their connections for safe integration. Although this is an important starting point and it is necessary to have a good understanding of the system and interaction between its elements, it does not focus on the system of interest. Therefore, there is a need to reorganise this information and move the focus to the system, subsystems, functions, structure, and behaviour. For this purpose, the points below need to be considered.

- The system of interest needs to be elaborated and relations between system, its subsystems, and super-systems need to be elaborated in further details.
- System of systems and environment can be merged. As result, the term environment refers to both system of systems and environments.
- Human is partly related to use and partly related to the environment of the system.

In order to address these points, Table II is produced representing the results of Table I with more focus on the system of interest. This presents the information for the so-called system safety cube. The rows of this table focus on the system of interest, its super system (or environment) and subsystems. The columns focus on requested functions (or malfunctions), physical structure, and the use (or misuse) scenarios. The questions below help to keep the focus per each column.

For the first column of Table II, the relevant questions are the following.

- Why does the (super/sub) system of interest exist?
- What is its purpose?
- What does it do?
- What are the requirements?
- What are the functions and services?
- What if it malfunctions or the services are interrupted?

For the second column of the table, one may ask the following questions.

- What are the elements of this (super/sub) system of interest?
- How do they connect?
- How is the energy provided?
- How is the information flow?
- What are the interfaces?
- How does it work?
- What if some components, subsystems, or interfaces fail?

For the third column of this table, or the use purpose, one may ask the following questions:

- Who are the people who have interest in the system?
- How do they influence the system?
- How do they use it?
- What are the foreseeable misuse scenarios?

TABLE II. SAFE INTEGRATION WITH FOCUS ON SYSTEM, THE SO-CALLED SYSTEM SAFETY CUBE

	System requirements, functions, and behaviour	*Physical system (system-SoS/environment relation)*	*Use/misuse scenarios (human-system relation)*
Environment and super systems	environmental requirements, policy, regulations	environmental/ super-system interfaces	user specifications/ interest, information for use, use/ safety culture
System	system requirements and functions. Modes of operation.	system level specifications: structure/ interfaces and subsystem failures	system level use/misuse scenarios, operation scenarios, accident history
sub-systems	sub-systems and components failures	sub-system level specifications structure/ interfaces and component failures	sub-system level use and misuse cases, intervention procedures

IV. EXAMPLE APPLICATION

This section presents an example application for safe integration of a bicycle to the urban environment. This is an interesting example because cycling is economic, healthy, and green for urban transportation. Yet, safety of cyclists is essential for making that a popular way of urban transportation. In the Netherlands, about 35% of people use frequently bicycles on a daily basis and this backs the public demand for safety. In 1970, people protested against a high number of child death on the roads and started the movement entitled "stop the child murderer" because of a high rate of casualties, especially on the cross-overs [6]. This demand influenced the government policy in the Netherlands perceiving bicycle as a critical means for safe

TABLE III. THE ELEMENTS OF SAFETY CUBE FOR SAFE INTEGRATION OF BICYCLES

	Human	*System*	*Environment*
Human	cyclist, other road users, regulators, service providers	traffic rules, quality & condition control, human-power input, steering	driving culture of e-bikes, cars, motorcycles, or other road users
System	safe, comfortable, economic, healthy, and enjoyable personal-transport	bicycle	visibility in day light, night, or at rain
Environment	traffic regulations, and traffic management system, climate requirements	bicycle (or safe) path, spare parts, fallen trees, snow or ice on the path, fallen trees or bushes	road, signs, curbs, markings, other road-vehicles, crossing, parking, climate, policy, regulations

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-698-9

TABLE IV. SAFE INTEGRATION WITH FOCUS ON SYSTEM, THE SO-CALLED SYSTEM SAFETY CUBE, FOR BICYCLES

	System requirements, functions, and behavior	*Physical system (system-SoS/environment relation)*	*Use/misuse scenarios (human-system relation)*
Environment and super systems	traffic regulations in Netherlands and Europe, control functions	bicycle path, roads, crossing, traffic lights, infrastructure, and natural environment	driving behavior of other users on bicycle path or adjacent roads
System	ergonomically safe, CE marking, meet the expected safety level, visible to other users	a two-wheels personal vehicle powered & steered by human	cyclist cycles in a (non) specified path at night, rain, or cross roads, cyclist uses unassigned paths (shortcuts)
sub-systems	components need to comply with standards	two wheels, frame, pedals chain, tires may go flat	cyclists sits on (side) saddle, inaccurate adjustment, stands on pedals, steers by one hand

transportation in urban areas. Along with geographical considerations, bike-friendly infrastructures and bike-friendly policy are the keys for the safe integration of bicycles into the system [7].

Here in this example, elements for safe integration have been described and listed through the approach introduced earlier in this paper. For this purpose, three elements of human, system, and environment are the starting points. Table III describes these three elements and their connections. This table shows what the needs are for creating safe cycling experience for users. It is far beyond a design of a safe bicycle and safe helmet requiring an integral view that combines proper infrastructures with supportive policy and embracing culture in order to achieve the optimum results.

Table IV represents this information with the focus on the system of interest, its subsystems, and super-system. It is important to note that the tables presented here for this example do not present all the detailed information for the safe integration of bicycles into urban areas.

In order to verify if the proposed approach can capture the essential elements of safe integration, a number of references have been reviewed as mentioned earlier in this section. The results confirm that the elements of safe integration have been captured in this approach. Yet, further elaboration is needed capture the details elements of safe design and their connections for safe integration.

V. CONCLUSIONS

For safe integration, one needs to pay attention to the system, its environment, and people who have connection to the system. As a matter of fact, the prerequisite of safe integration is proper system definition describing the system of interest, its structure, requirements and behaviour, people who influence it, its environment or super-system, and the relations. For safe integration, one needs to pay attention to use and misuse, function and malfunction, and components or interfaces as well as their failures. The proposed approach seems to be able to help for a quick verification and validation plan in early design phases, and this is a subject to further research.

REFERENCES

[1] M. Rajabalinejad, “System Integration: Challenges and Opportunities for Rail Transport”, System of Systems Engineering Conference, 2018, Paris, France.

[2] C. Perrow, “Normal accidents: Living with high risk technologies”, Princeton University Press, 2011.

[3] D. D. Walden et al., Systems Engineering Handbook - A Guide for System Life Cycle Processes and Activities, International Council on Systems Engineering (INCOSE), 2015.

[4] J. Reason, "Beyond the organizational accident: the need for "error wisdom" on the frontline," Quality and Safety in Health Care, vol. 13, no. suppl_2, pp. ii28-ii33, 2004.

[5] M. Rajabalinejad, "Incorporation of Safety into Design by Safety Cube" in Journal of Industrial and Manufacturing Engineering vol. 12, no. 3, WASET, International Scholarly and Scientific Research & Innovation, 2018.

[6] M. Wagenbuur "How Child Road Deaths Changed the Netherlands". *BBC World Service - Witness programme*. BBC World Service, November, 2013.

[7] "Cycling in the Netherlands", (Press release) The Netherlands: Ministry of Transport, Public Works and Water Management. Fietsberaad (Expertise Centre for Cycling Policy), 2009.

Copyright (c) IARIA, 2019. ISBN: 978-1-61208-698-9