Safe Integration for System of Systems: The Safety Cube Theory

Mohammad Rajabalinejad
Faculty of Engineering Technology
University of Twente,
Enschede, the Netherlands
Email: M.Rajabalinejad@utwente.nl

***Abstract*—This paper highlights the importance of integration in engineering practices and provides an overview for integration from two perspectives: system hierarchy and system behavior. Furthermore, the paper presents the Safety Cube theory for system of systems integration. Safety Cube simultaneously captures both hierarchical and behavioral perspectives required for integration in system of systems. An example application for the house hold robots has been presented through the paper.**

Keywords - systems integration; safe integration; system of systems integration; integration engineering; optimal integration, Safety Cube.

I. INTRODUCTION

We demand products, systems, and services for fulfilling our needs. We need them to function, to not harm any human, to neither damage properties nor the environment, and need them to perform the required tasks. We expect them to properly integrate with their related-environment and deliver optimal performances. For example, we expect the IoT devices to effortlessly connect to internet, seamlessly communicate with each other, and exchange data at the expected rate. Satisfaction to these needs is a fundamental economic driver for different industries.

On the other hand, it is a challenge to optimally integrate products with everyday life because of the high-pace of technological advancement and the dynamic of changes. Systems are often not any longer on the full control and need to adapt their services according to their environmental dynamics. Optimal integration of new technology with operational systems is becoming increasingly important, and resilient services are requested. Improper integration of new systems may expose extra costs to stakeholders, cause sub-optimal services, waste scarce resources, harm people, damage assets, or damage the environment. Improper integration causes redesign and reengineering of products or services which can become very expensive when issues are recognized at the end of a project lifecycle. A survey conducted by The Standish Group shows that risk mitigation through the operational phase can become up to 30 times more expensive than risk mitigation in the early design phase [1]. Brombacher shows that a high percentage of the consumer electronic products return to the manufacturer without any faults primarily because they do not meet users' expectations [2]. Example of integration issues for transportation sector have been presented for example in [3].

Therefore, engineers need to overcome integration challenges and properly design for integration because that limits the number of prototypes, reduces the number of tests, and demands less training especially for capital assets. Design for integration makes the products modular, reusable, upgradable, context aware, self-organizing, interoperable, and offers data driven capabilities. Engineers need to address integration challenges across the complete product lifecycle for safe and sustainable services.

This paper presents a brief review of integration in engineering practices, holistically addresses the integration maturity, and introduces the Safety Cube theory for a systematic approach for integration of systems. An example application is provided at the end of this paper.

II. INTEGRATION IN ENGINEERING PRACTICES

Integration is defined as "an act or instance of combining into an integral whole" or "behavior […] that is in harmony with the environment" according to dictionary.com. These two definitions highlight two different aspects of integration which are first being as an integral whole and second behaving in harmony with the environment. Most of engineering practices focus on the first aspect and less attentions are being paid on the latter. Best practices recommend tools and techniques for creating products or systems which are properly designed, flawlessly integrated, and the expected functionalities are optimally delivered. Being in harmony with the environment, however, has not been the focus for common practices. Next section explains this in more details.

978-1-7281-0457-7/2019/$31.00 ©2019 IEEE

A. Combined into an integral whole

In the engineering development, integration often appears after creation. This is a logical approach where first the functionalities are identified, the systems and subsystems are designed, and then the components or subsystems are built and then integrated [4]. The systems engineering (SE) community, which is one of the sources for sharing the best engineering practices, pays special attention to integration. It defines the purpose for integration process as "to synthesize a set of system elements into a realized system (product or service) that satisfies system requirements, architecture, and design" [5]. It recommends the V model, widely used across different industries, and the right side of this model highlights integration, verification, and validation. In this context, integration focuses on combining the system elements. Next subsections present a hierarchical view for integration for the levels of subsystem, system, and system of systems.

1) Subsystems integration

Here in this paper, the sequence of system, sub-system, and component is used for referring to the breakdown of a system into smaller parts. Therefore, subsystems integration refers to combination of two or more components. Subsystems integration is often among the earliest actions for integration. For example, the V model suggests starting integration from this level. Integration of components occurs often in production or assembly stage.

2) Systems integration:

Systems engineering handbook defines a system as "an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements" [5]. It defines integration as a technical process for integrating the elements of a system. In this context, a successful integration leads to a system that works and delivers the required functionalities without any failure. Here the focus is mainly on the subsystems or components. Through this approach, the integration of human and system becomes another issue because it is not a completely technical process.

The SE handbook recognizes that integration of human and system is a non-technical process and recommends focusing on human systems integration (HSI) across the design or engineering of systems. In that context, human is considered as an element of the system, and its integration with system must by fully considered. HSI considers domains such as human factors engineering (human performance, human interface, user centered design), workload (normal and emergency), training (skill, education, attitude), personnel (knowledge, attitudes, career progression), working condition and health (ergonomics, occupational standards, and hazard and accident avoidance) [5]. It is important to note that HSI focuses on the human needs within the scope of the system of interest.

3) System of Systems (SoS) integration

A "system of systems" (SoS) is a system whose elements are managerially and/or operationally independent systems according to [5]. As results, the interoperability of the integrated systems or subsystems usually is not achievable by an individual system alone. The relations among a system and other systems have been discussed for example by Mo Jamshidi in the context of System of Systems [6]. He considers integration as the key viability of any system of systems. This means that systems can communicate and interact through different interfaces e.g. hardware, software, etc. In this context, a system uses services from other systems or delivers services to other systems. This often requires collaboration among different organizations. For delivering optimal results, having shared objectives among organizations, co-creation of desired capabilities, and co-integration of interoperable services are key factors to success [7, 8]. The effects of a system and its behavior on the related-environment have been discussed through a variety of literatures for example around the subject of sociotechnical systems.

B. In harmony with environment

According to the definition of integration, a system is properly integrated when it behaves in harmony with its environment. Environmental-wise, however, the SE models do not focus on the environment of the system of interest. For example, the famous V model guides toward developing a system that delivers the expected functionalities and meets the formulated requirements. However, this model does not directly motivate its users to explore the system environment, investigate the relevant history, or share/use the relevant knowledge or experience about it. The related environment can impact the system. In his book named Normal Accidents, Perrow explains how integration of coupled systems can lead to unexpected behavior [9]. The Swiss cheese model of Reason represents integration of different aspects in which the risk of a threat may become a reality [10]. For example, flaw in software, fault in the hardware, stress on the operator, and operation under specific circumstances may lead to unexpected results and unpredicted behavior. Next subsections discuss three categories for maturity of integration: operational, safe, and optimal.

1) Operational integration

Operational or functional integration is the basic level of integration for enabling a system to technically deliver its required functionalities. Numerous studies have been conducted to address the maturity of a component technology or an interface for proper integration. Metrics are available for TRL (technology readiness level), SRL (system readiness level), and IRL (Integration readiness level) for software, hardware or interfaces to assess the maturity [11, 12]. However, a combination of two mature technology components is not always mature and flawless. Issues may emerge related to for example user-friendliness, high costs, or sustainability problems which may impact the system performances or result in safety related consequences.

2) *Safe integration*

Safety is “freedom from those conditions that can cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment” [13]. Safe integration is the condition that the integration of a system with its environment does not cause death, injury, occupational illness, or damage to or loss of equipment or property, or damage to the environment. A safely integrated system compliances with regulations. Regulations often target safe integration too. For example, the European Directives for Railways benchmarks for the safe integration of new rolling stocks [12, 15]. IEC 61508 a seminal standard for functional safety delivered in several parts. Part 1 of this standard addresses issues on system safety validation and system integration (tests) including architecture, software, and integration tests [16]. 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 [17]. It is important to note that these conditions are not limited to a specific phase in the life-cycle.

3) *Optimal integration*

A system that is optimally integrated offers its services safely and at the optimum level of performances. At this level, there is a balance between cost, quality, and delivering of services. This is the desired level of integration which mobilizes the full system capabilities. There is a variation in the definition of optimal integration across different maturity models. For example, optimal integration for software, hardware, or interfaces have been defined differently. Literatures mostly focus on the subsystem and system level integration, and further research is required for defining the optimal integration for system of systems. A comprehensive study has been done by the Open Group resulting in Open Group Service Integration Maturity Model (OSIMM). The OSIMM maturity matrix provides guidance on how to achieve certain levels of service maturity.

III. SAFE SYSTEMS INTEGRATION

A. *Principles*

One of the primary objectives for engineering design, systems engineering, or risk management is safe integration of the required functionalities into the operational environment. In this perspective, dealing with the system, human, environment, and relations among them are fundamentally important for safe integration [18, 19]. The following subsections explain the fundamental views required for safe integration in the context of human, system, and environment.

1) *System of interest*

System of interest (SoI) is the system whose lifecycle is under consideration [20]. The ISO standard for railway safety defines the system as “a set of elements which interact according to a design, where an element of a system can be another system, called a subsystem and may include hardware, software and human interaction” [21]. The SE handbook defines a system as “an integrated set of elements, subsystems, or assemblies that accomplish a defined objective. These elements include products (hardware, software, firmware), processes, people, information, techniques, facilities, services, and other support elements” [5].

2) *Human*

Human or people refer to individual or group of individuals who have connections to the system of interest in the form of for example stakeholders. They can be users, operators, owners, service providers, producers, or other humans who directly or indirectly have interest in the system. They may cooperate or compete with the system of interest, monitor, regulate, manage, maintain, replace, or dispose it. People have their own individual or organizational culture. Not only the relations among human and system but also relations among human and human may influence the system of interest.

3) *Environment*

Environment consists of all relevant parameters that can influence or be influenced by the system of interest in any lifecycle phase. One may refer to the related environment as context, surrounding, or super-system. Relevant regulations, industry standards, or supporting facilities in the course of normal or specific operational conditions are part of the system environment. Functional safety and railway safety standards define human as a part of environment whereas the systems engineering practice considers human as a part of the system [5, 16, 21].

4) *System – Environment*

The system of interest has relations with its environment. The relation between a system and its environment can be physical or non-physical. A physical relation is often realized through technical installations. Non-physical relations are e.g. laws, regulations, policy, market demands, or political interests that have influence or are influence by the system.

5) *Human – System*

Human can have different roles and consequently different relations with the system of interest. The relation can be physical, logical, emotional, etc. This relation can influence or be influenced by the system of interest. Human factors, operational and safety culture fall under the category of human-system relation.

6) *Human – Environment*

The human-environment relation often falls out of the scope of system of interest in the technological design, but it may have dominant influence on the system of interest. Change of regulations in a dynamic and competitive political context or policy-making that influence the system of interest are examples of human-environment relations for the system of interest. These relations often become very complex for systems where multiple stakeholders are involved.

B. The Safety Cube Theory

The Safety Cube Theory formulates six fundamental views for safe integration. It underlines that these views are fundamentally important for safe integration. They are about the system of interest, human who have relation or are associated with the system, the related environment of the system, human-system integration, system-environment integration, and human-environment interfaces that influence the system. Figure 1 shows these six fundamental views for safe integration through six faces of Safety Cube. The three-dimensional visualization of Safety Cube is presented by Figure 2.

Safety Cube can capture both hierarchical and behavioral aspects of integration. The reason for that is that the hierarchical perspective can be presented through the system or system-environment views, and the behavioral perspective can be presented by human-system and system-environment views. However, this requires further research and elaboration. The author experience shows that Safety Cube can help designers to see the system not in isolation but also as a part of the people and/or environment context required for safe integration [22]. In fact, Safety Cube demands for knowledge from systems engineering, risk management, and safety engineering disciplines which are prerequisites for safe and optimal integration. In this perspective, integration maturity ultimately meets sustainability where a system remains in harmony with the environment.

Figure 1. This picture provides the six views of Safety Cube.

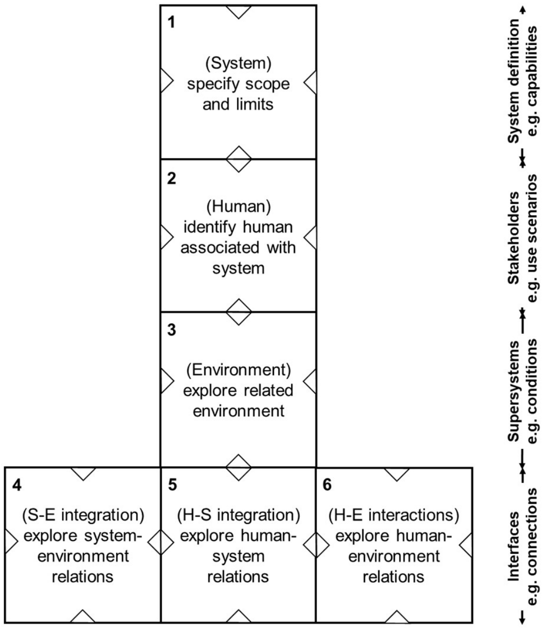
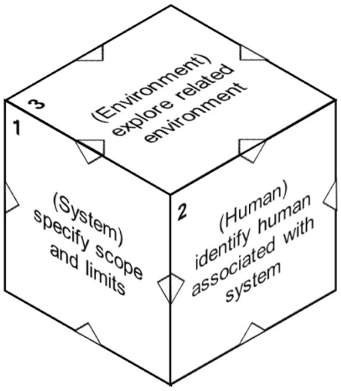

1
(System) specify scope and limits
2
(Human) identify human associated with system
3
(Environment) explore related environment
4
(S-E integration) explore system-environment relations
5
(H-S integration) explore human-system relations
6
(H-E interactions) explore human-environment relations
System definition e.g. capabilities
Stakeholders e.g. use scenarios
Supersystems e.g. conditions
Interfaces e.g. connections

Figure 2. Visualization of Safety Cube. Six fundamental views for safe integration are presented through the six faces of Safety Cube.


3
(Environment) explore related environment
1
(System) specify scope and limits
2
(Human) identify human associated with system

IV. Example application

This section provides an example application for the use of Safety Cube for the integration of house hold robots. Household robots can offer many services for their owners such as cleaning, entertainment, telepresence, preparing food, offering companionship, aiding with health care, etc. However, integration of these services into the everyday life raises many concerns such as safety or security issues. In other words, they can become a source of hazards if not properly designed, used, operated, maintained or dismissed. These concerns should be dealt through the design phase and before they become operational in houses.

Table 1 summarizes several important system-level considerations for the safe integration of house hold robots. The diagonals of this table specify the human, system, and environment. The other cells provide information about the relations between diagonals. The off-diagonals must be read clock-wise in such a way that the associated row provides input for the associated column. For example, the human-system cell in the top row describes the human input for the system whereas the system-human cell in the second row describes the system input for human. In this table, numbers refer to the faces of Safety Cube explained in the previous section.

V. Conclusions

People are becoming less tolerant for safety failures while they demand up-to-date technologies seamlessly integrated with their everyday life. The increasing complexity of high-tech systems raises the needs for supporting tools for proper integration of newly developed technologies. The challenge is far beyond technical matters and more than the integration of hardware, software, and human for a single product or system. Next to an integral whole, the system needs to behave in harmony with its environment.

Safety Cube formulates the principal views for safe integration. Its six faces present six fundamental perspectives

TABLE 1. THE ELEMENTS OF SAFETY CUBE FOR SAFE INTEGRATION

	Human	*System*	*Environment*
Human	1. users, owner, direct/indirect stakeholders, operators	5. human input for the system, intended use or misuse scenarios	6. human input for environment or its, use or misuse scenarios
System	5. system inputs, functions, malfunctions, or services for human	2. house hold robots, specified functions, procedures, operational conditions, etc.	4. system input for environment, intended use or misuse scenarios
Supersystem or Environment	6. environmental inputs, functions, malfunctions, or services for human	4. environmental inputs, functions, malfunctions, or services for the system	3. cooperating or competing systems, physical environment, policy, regulations

for safe integration. Safety Cube seems to be able to simultaneously cover both hierarchical and behavioral aspects of integration. In addition, it helps engineers and designers to remember the six principal views required for safe integration of system of systems.

ACKNOWLEDGEMENT

The author acknowledges the support of Dutch Railways (NS), ProRail and HTSM (Holland High Tech) through the framework of the SIRA (Systems Integration for Railways Advancement) project [23]. Furthermore, the author would like to acknowledge the peer reviewers for their feedback led to improvement of this paper.

REFERENCES

[1] Y. Bijan, J. F. Yu, J. Stracener, and T. Woods, "Systems requirements engineering-State of the methodology," (in English), *Systems Eng,* vol. 16, no. 3, pp. 267-276, Fal 2013.

[2] A. C. Brombacher, "Maturity index on reliability: covering non-technical aspects of IEC61508 reliability certification," (in English), *Reliab Eng Syst Safe,* vol. 66, no. 2, pp. 109-120, Nov 1999.

[3] M. Rajabalinejad, "System Integration: Challenges and Opportunities," presented at the System of Systems Engineering, Paris, France, 2018.

[4] G. Pahl, W. Beitz, J. Feldhusen, and K.-H. Grote, *Engineering Design A Systemmatic Approach*. Springer, 2007.

[5] 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.

[6] M. Jamshidi, "System of Systems Engineering New Challenges for the 21' Century," *IEEE Aerospace and Electronic Systems Magazine,* vol. 23, no. 5, 2008.

[7] M. Rajabalinejad and L. v. Dongen, "Framing Success: the Netherlands Railways Experience," *International Journal of System of Systems Engineering,* vol. 8, no. 4, pp. 313-329, 2018.

[8] R. L. Stroup and K. J. Kepchar, "Enterprise Integration: A Framework for Connecting the Dots," 2012.

[9] C. Perrow, *Normal accidents: Living with high risk technologies*. Princeton University Press, 2011.

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

[11] S. Ross, "Application of System and Integration Readiness Levels to Department of Defense Research and Development," Defense Acquisition University, July 2016 2016, vol. 23.

[12] R. A. Martin, "International Standards for System Integration," presented at the INCOSE International Symposium, 2005.

[13] *MIL-STD-882E: 2012 Department of Defense Standard Practice System Safety*, 2012.

[14] *Directive (EU) 2016/798 of The European Parliment and of the Council of 11 May 2016 on Railway Safety,* E. Parliment L 138/102, 2016.

[15] *Directive (EU) 2016/797 of The European Parliment and of the Council of 2016 on the Interoperability of the Rail System Within the European Union,* T. E. P. A. T. C. O. T. E. UNION, 2016.

[16] *IEC 61508-1 Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: General requirements*, 2010.

[17] *EN-ISO 12100:2010 Safety of machinery - General principles for design - Risk assessment and risk reduction*, 2010.

[18] M. Rajabalinejad, "A Systemic Approach for Safe Integration of Products and Systems," presented at the The Ninth International Conference on Performance, Safety and Robustness in Complex Systems and Applications, Valencia, Spain, March 24 - 28, 2019.

[19] M. Rajabalinejad, "Incorporation of Safety into Design by Safety Cube," *Industrial and Manufacturing Engineering,* vol. 12, no. 3, 208.

[20] *ISO/IEC/IEEE 15288, First edition 2015-05-15, Systems and software engineering — System life cycle processes*, 2015.

[21] EN, "EN 50126 Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process," 2015.

[22] M. Rajabalinejad, "Safety by Design," *Journal of System Safety,* vol. 54, no. 2, p. 3, 2018.

[23] SIRA. (2018). *Integration Engineering* [Online]. Available: https://integration.engineering/.