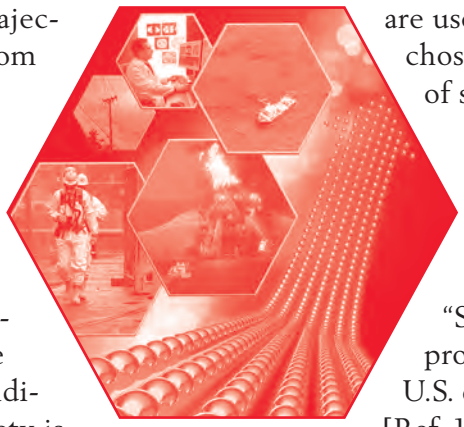
‘Technical Safety’ or ‘System Safety’? Why Names Matter

by Sergio Oliva and Ricardo Lopez
Houston, Texas

By providing safety and risk management consulting services, we have the opportunity to be regularly involved with clients from a number of different industries. We often interact with professionals of varied trajectories and backgrounds, many of whom have never received comprehensive training in system safety. Those individuals are by no means less competent in their jobs; however, their schooling in system safety often comes from a senior colleague or mentor who held a safety-related position during a long career in a single industry. More often than not, the individual’s understanding of system safety is reduced to his or her limited exposure to this rich and diverse field.



A few months ago, we were involved in an offshore project for an oil and gas client. We visited the client’s office for a project presentation. The meeting was on a normal course until we brought up certain system safety issues that required our attendee’s review. These issues were under the label of “technical safety,” which in hindsight was a mistake. We were soon challenged to offer a definition of technical safety, which in our view was no different than system safety. This gentleman argued that technical safety was different from the other “safeties” such as system, functional or operational safety. Coincidentally, a few weeks later in a meeting with a different group of clients, we mentioned that our expertise included system safety. One of the meeting participants immediately asked: “What system?”

The preceding experiences made us consider how safety professionals may use tools, techniques or mental constructs that were developed in different industries, and originally labeled under different names. It is a matter of fact that familiarity with equipment, processes or activities in a technical field favors the use of unique terminology to the point of developing a professional jargon that is intelligible only to insiders. The constant repetition of a term by specialists in an industry without a clear definition of that term’s meaning creates a false sense of universality. The terminology used by industry experts frequently differs from the terms used by colleagues in other industries, despite the fact that similar, if not identical, methods, ideas and contraptions are used by all. This is extensive to our chosen profession and to the actual field of system safety.

System Safety in All Its Flavors

After the previous experiences with our clients, we questioned our own understanding of the subject. “System safety” may be traced to the production of ballistic missiles in the U.S. during the decade after World War II [Ref. 1]. The first system safety practitioners developed methods to assess risks and controls of the hazards related to the rapidly changing technologies they were facing. Some of the new quantitative methods were highly favored by the emerging computerization taking place in military technology. Analyses were initially time consuming, limited and restricted to a few classified reports. In time, the proven success of the methodology became known worldwide. System safety as a professional field was thereafter established.

Variations of the concept of system safety have been offered by experts, but the almost 40-year-old definition remains up to date: *“The application of engineering and management principles, criteria and techniques to optimize all aspects of safety within the constraints of operational effectiveness, time and cost throughout all phases of the system life cycle”* [Refs. 2 & 3]. The completeness and broad scope of system safety is manifest when the term “system” is subsequently defined [Ref. 4]: *“An integrated composite of people, products and processes that provide a capability to satisfy a stated need or objective. “*

We are personally aware that the aforementioned definition of system safety is accepted and in use in several industries, such as aerospace, defense, mass transit and medical device manufacturing. We are also aware that some areas of the body of knowledge of system safety have acquired their own specific names. Colleagues in various industries have attempted to define

Table 1 — System Safety Under Different Names

Name	Most Accepted Definition	Industry	Reference
Functional Safety	Part of the overall safety relating to the Equipment Under Control (EUC) and the EUC control system, which depends on the correct functioning of the electric/electronic/programmable electronic safety-related systems, other technology safety-related systems and external risk reduction facilities	Electronics, Oil & Gas	[5]
Operational Safety (Management)	The systematic management of the risks associated with flight operations, related ground operations and aircraft engineering or maintenance activities to achieve high levels of safety performance	Civil Aviation, Railway, Nuclear, Oil & Gas*	[6]
Process Safety (Management)	The proactive identification, evaluation and mitigation or prevention of chemical releases that could occur as a result of failures in process, procedures or equipment.	Oil & Gas, Chemical	[7]
Technical Safety (Requirements)	The limits, controls and related actions that establish the specific parameters and requisite actions for the safe operation of a (nuclear) facility.	Nuclear, Oil & Gas Upstream**	[8] [9]

* The use of "operational safety" has been adopted by these industries, civil aviation notwithstanding, without any formal definition. The reader may refer to [10] for more on the topic.

** No definition of "technical safety" for Oil & Gas is provided in [8], despite its title.

these safety areas, with limited success. Table 1 shows a list of definitions based on the authors' experience.

One may argue that since people have always been part of the system, occupational safety is therefore embedded in system safety. Perhaps for pragmatic reasons, the safety of workers in the workplace has been historically addressed by specialists with little experience in system safety. By the same token, system safety practitioners are often unaware of all the intricacies and requirements that compliance with workplace safety and labor laws demands from our occupational colleagues. This is especially true when the manufacturing, testing and deployment of a system imply managing people with different cultures and languages, and in compliance with laws in workplaces scattered around the globe.

Specialized scientific knowledge often spins off in time into a new field of science. The contributions of its practitioners propel the development of the new field with its ultimate acceptance by the scientific community and the general public. Process safety may be one of these cases as defined in Table 1. Any plant safety aspect related to a potential chemical release is now typically under the label of process safety. Its practitioners customized system safety methods in the 1980s, and even created new techniques to address the unique issues of the process industries, more specifically in petrochemical facilities. Layers of protection analysis (LOPA) and safety integrity levels (SIL) are examples of that effort. At best, these techniques match the capabilities of fault and event tree analysis. However, that does not change the fact that LOPA and SIL are central to process safety, and are often the first quantitative tools of choice for practitioners in that field.

The use of preceding modifiers to the term "safety" is customary in many industries and mostly useful to characterize a specialization within the broad professional field of safety. The modifier identifies the specialty to make a clear distinction from others. "Patient safety," "radiation safety" and even "system safety" are examples of that use. Therefore, the names in Table 1 suggest that those areas of safety are somehow different from system safety, and indeed perceived by many as disconnected from our chosen profession. Some may argue that the specialized knowledge required in those industry niches deserves specific designations within the safety profession. Time will tell, but a false sense of uniqueness is portrayed in the meantime. As long as no clear definition of those specialties is provided and the use of system safety methods continues, system safety practitioners are affected. Professionals and others with little exposure to system safety tend to believe that the meth-

odologies used in Table 1 specialties were developed within, or for, those industries alone. Managers and other decision-makers are often doubtful of methods and tools applied by outsiders, let alone of hiring system safety practitioners from a different industry. It may take years for a risk assessment technique to be tested and adopted outside its industry of origin [Ref. 11]. The frequent re-labeling of methods once they migrate to different industries compounds the detrimental effect. New practitioners are prevented from finding the original association, and often remain uninformed of concurrent breakthroughs by peers in other industries.

Conclusion

Despite the issues discussed here, world-class organizations are working to close the gap among professionals on issues related to safety and risk assessment. In the Internet age, a professional forum is relatively inexpensive to create, and the benefits may be accessed by colleagues worldwide. The International System Safety Society is an example, for its outreach to foster communication among professionals of different industries across the globe.

As technologies and systems continue evolving, and capital projects remain fraught with risks, system safety will have an important place in project management. System safety practitioners will certainly have an important role in the optimization of all aspects of safety. This role will be fostered if it is derived from a cooperative effort among professionals in every industry — or it will likely be hindered by the atomization of our chosen profession.

About the Authors

Sergio Oliva until recently was a senior safety and risk consultant at ERM in Houston, Texas. He currently works for Wild Well Control, Inc. Sergio has more than 17 years of multi-industry experience, and holds a master's degree in engineering from Texas A&M University at College Station. He is a certified safety professional (CSP) who is also experienced in system safety, reliability and quantitative risk assessment. He has authored reports and professional publications, including peer-reviewed technical papers in renowned scientific journals. He is a member of the International System Safety Society.

Ricardo Lopez is a principal consultant in safety and risk management within ERM's Houston office. He has more than 30 years of experience in civil engineering and a master's degree in environmental science from the University of Houston at Clear Lake. Ricardo has led efforts on reliability, availability and maintainability (RAM) analyses, financial risk, building site assessments and quantitative risk analyses of capital projects for major oil and gas companies.

References

1. Vincoli, J. W. *Basic Guide to System Safety*, John Wiley & Sons, 1993.
2. Department of Defense Standard Practice for System Safety. "MIL-STD-882D," February 10, 2000.
3. "System Safety Links," International System Safety Society, accessed September 13, 2013, http://www.system-safety.org/links/
4. Air Force Safety Agency, Kirtland Air Force Base. "*Air Force System Safety Handbook* (AFB NM 87117-5670)," July 2000.
5. International Electrotechnical Commission. "Functional Safety of Electrical/Electronic/ Programmable Electronic Safety-related Systems," IEC 61508 International Standard, Part 4.
6. Civil Aviation Authority. "Safety management systems for commercial air transport operations," CAP 712, April 2002.
7. U.S. Department of Labor Occupational Safety and Health Administration. "29 CFR 1910.119 Federal Regulation, Process safety management of highly hazardous chemicals," July 2011.
8. Norwegian Oil Industry Association (OSL). "Technical Safety," NORSOK Standard S-001, Edition 4, February 2008.
9. U.S. Department of Energy Nuclear Regulatory Commission. "10 CFR Part 830 Federal Regulation, Nuclear Safety Management," January 2011.
10. Salter, M. "Managing the Operational Safety Case in High-Risk Systems," MS Thesis, University of York, Department of Computer Science, September 2006.
11. Stamatelatos, M. and H. Dezfuli. "Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners (NASA/SP-2011-3421)," Second Edition, Office of Safety and Mission Assurance NASA Headquarters, December 2011.