**SYSTEM SAFETY ENGINEERING FOR A HIGH-PRESSURE EXPERIMENTAL RESEARCH FACILITY**

**Simon P Philbin PhD MBA**

Programme Director, Institute of Shock Physics and

Visiting Fellow, Imperial College Business School

Imperial College London

London SW7 2AZ, United Kingdom

Phone (+44) 20 7594 8605, Email [s.philbin@imperial.ac.uk](mailto:s.philbin@imperial.ac.uk)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract**

*This paper will discuss system safety engineering through a case study investigation of an engineering project at Imperial College London, involving a new high-pressure experimental research facility. As part of the establishment of the Institute of Shock Physics, Imperial College is partnered with an industrial organization to create this new facility that will allow research to be undertaken in the area of understanding how materials behave under high strain rates. In order to achieve this objective, new purpose built equipment has been designed and is scheduled to be delivered and installed in 2010. Before the new facility can become operational there is a need to develop a robust safety case and to initiate a new safety management system. To achieve this goal, a set of technology and systems management processes have been employed in order to ensure safety engineering best practice is utilized early in the system lifecycle. The process methodologies adopted include systems design visualizations, such as systems architecting and safety control structure diagramming; failure modes and effects analysis (FMEA); multidisciplinary teaming; benchmarking and enterprise management. The paper will describe these processes, initially through a review of supporting literature and then from the case study investigation, highlighting the merits of the processes as well as any difficulties encountered. The paper will then conclude with a set of recommendations on improving safety management for engineering projects.*

**Key Words**

System safety engineering; facilities management; systems engineering; FMEA; architectures.

**Introduction**

The Institute of Shock Physics was established in 2008 with the objective of undertaking research in the area of shock physics, which involves research on the behavior of materials under high strain rates (Isbell, 2005). In order to achieve this goal, it was decided to direct significant funding into a new high pressure experimental research facility that would allow materials to be investigated at pressures on a gigapascal (GPa) scale.

The research facility was jointly funded by Imperial College London in the UK and an industrial partner. The resulting facilities development project has been reported previously (Philbin, 2008) and this study provided a discussion of the use of systems engineering to help facilitate the project’s planning and management. The new purpose built high-pressure equipment and supporting laboratory services have now been designed and are scheduled to be installed in 2010. However, before the new facility can become operational, there is a need to develop a robust safety case through undertaking system safety engineering of the facility. Therefore, the focus of this new study is to describe how technology and systems management processes have been employed in order to ensure safety engineering best practice is utilized early in the facilities system lifecycle. Moreover, the study will highlight how management tools can be effectively deployed so that engineering design is optimized whilst ensuring safety and wider organizational risks are minimized. The process methodologies adopted include systems design visualizations, such as systems architecting and safety control structure diagramming; failure modes and effects analysis (FMEA); multidisciplinary teaming; benchmarking; and enterprise management.

The paper has the following structure. After the introduction there will be a literature review of system safety engineering, which will include discussion of some key techniques and processes. There will then be discussion of the process tools and methodologies that have been adopted, involving a case study investigation of the high-pressure research facility. The paper will conclude with a set of recommendations for system safety engineering.

**System Safety Engineering**

**The Systems Context**

System safety engineering can be regarded as the need to obtain a level of assurance that the system in question is safe for all the people, equipment and the surrounding environment (Bahr, 1997). Incorporating safety studies within systems engineering is logical since the systems focus encourages a holistic treatment of safety risks (Reason, 1997). Furthermore, where safety management is part of a wider program and systems engineering is being implemented in order to reduce technical and business risks, then systems safety engineering allows best practice management to be implemented early in the system lifecycle. Related to safety management are the areas of reliability and risk assessment, which can be employed to determine different combinations of factors (or faults) that may give rise to reduced safety (Andrew and Moss, 1993).

Ultimately the system safety engineering approach needs to develop from a defined set of requirements for a system where potential hazards are identified, which may become risks that are evaluated and mitigated against. This allows the system to then be modified (if possible) so that the risks can be reduced. In this regard, risks can be viewed as being a combination of the probability of a particular hazard occurring and at a certain level of severity or magnitude. Moreover, the ability to ensure that hazards are effectively and adequately contained, through the use of risk assessments and supporting methodologies as part of the design stage, has been standardized across a number of industries, such as within the chemical process sector (Kletz, 1998) and the construction industry (Jannadi and Almishari, 2003). Developing structured methodologies, which can accommodate technology and systems complexity, can therefore be framed in the context of enhancing decision support tools, which can support the engineering design process (Liu and Boyle, 2009). Ultimately, of course, achieving optimized design through delivering the system requirements and whilst minimizing safety risks is of major importance for all facilities initiatives.

**Decision Support Tools**

The application of decision support tools, such as risk assessments, has been investigated widely and Crossland et al. (2003) have described a whole-life cost-benefit uncertainty model that can be used to assess design uncertainties. Here engineering design takes account of safety risks as well as other technical risks that may affect the reliability of the engineering system, which can then impact on overall business performance.

Engineering system design can be improved through the use of both failure mode avoidance (Clausing, 2004), leading to enhanced reliability as well as from various quality assurance and management techniques (Taguchi, 1993). In the former case there are two main causes of failure modes and these are a lack of robustness and mistakes, where both mistakes and design decisions can eventually lead to a lack of system robustness and resulting potential failure modes. Consequently, an adequate focus on detecting and subsequently managing any failure modes for the engineering design will help lead to a robust and reliable engineering system. On this matter, Clausing and Frey (2005) have examined the failure mode avoidance (FMA) technique through the use of an operating window approach to detect the failure modes for a jet engine turbine blade. Incorporating this kind of approach into the engineering design for the turbine blades indicates how robustness of the blade (i.e. ‘effective life’) could be improved. In a different area, Henshall and Campean (2009) have applied FMA in the automotive industry, through the adoption of widely used tools, such as function fault tree analysis, P-diagrams and design verification, in order to improve product design and development.

Focusing down on specific tools leads to the failure modes and effects analysis (FMEA) approach, which is a quality and risk assessment tool. FMEA can be used to capture potential failure modes and the causes of failure, together with the required process controls. This analysis can then be used to modify the engineering design, so that any identified failure modes are removed, or the likelihood of impact for the failure mode is reduced. Furthermore, Teoh and Case (2004) have described how FMEA is a generic methodology that can be applied to different industries. Although they also point to a need to develop modeling approaches, which can handle different quantities of engineering knowledge.

The FMEA process requires a system function diagram to guide the analysis, where failure modes are identified for each subsystem or component in the diagram. In this regard, different visualization techniques have been used, including fuzzy cognitive maps, which are supported by fuzzy set theory and which allow qualitative information to be captured (Peláez and Bowles, 1996). Such an approach highlights how causal effect modeling can be adapted for different circumstances, thereby allowing varying levels of knowledge to be accommodated within the system. Other diverse applications of FMEA include evaluation of risks of failure in terms of the cost for the development of electromagnetic and permanent magnet systems for particle accelerator applications (Spencer and Rhee, 2004) as well as automated evaluation of electrical system failures for vehicles (Price et al., 1995).

An approach that seeks to move beyond purely safety risk analysis is called STAMP (safety-theoretic accident modeling and processes), which includes all elements of risk, including technical, organizational and social (Leveson, 2004). This more comprehensive approach builds on systems theory, where safety is viewed as a control issue and safety management is a control structure within an adaptive socio-technical system. As part of the methodology, a safety control structure diagram is developed, which illustrates the control actions as well as the system hierarchy in respect of both system development and system operations. The STAMP process has been investigated for different applications, including safety evaluation for space and missile systems (Leveson and Dulac, 2005) as well as safety assessment of the ballistic missile defense system (Pereira et al., 2006).

**Research Facility Case Study**

The case study investigation involves application of a series of system safety engineering methodologies to the development of a new high-pressure experimental research facility at Imperial College (the university), which is expected to be commissioned in early 2010. This initiative represented a significant undertaking for the university, involving the design of a complex set of mechanical and electrical (M&E) services together with supporting construction works. The facilities development project was required so that an existing laboratory could be upgraded to accommodate the new high-pressure equipment. The project had a number of design risks, since both the design of the laboratory services and the design of the equipment were undertaken in parallel.

Many of the technical risks for the facilities development project related to the systems integration between the services and the corresponding engineering components and structures of the equipment. This is because an inability to adequately control these integration points could compromise the robustness of the engineering system and decrease the performance of the equipment. Furthermore, there were significant safety risks to manage as the equipment is required to generate pressures on a gigapascal (GPa) scale through the use of pressurized gas. Consequently, in order to help alleviate some of these design and safety risks, it was decided that structured management techniques would be deployed. This would allow engineering management best practice to be utilized within the project and the systems engineering approach would help to relate the facilities project to the wider system-of-systems context, i.e. in relation to other partially federated systems at the university and elsewhere.

**(i). Systems Design Visualizations**

Initial visualization was undertaken using a viewpoint-oriented SADT (structural analysis and design technique), which allowed a system architecture to be developed for operation of the facility (Philbin, 2008). Exhibit 1 overleaf provides the system architecture that was initially developed. This was used to guide the preliminary FMEA studies as part of the design process.

In order to develop a more comprehensive view of the safety engineering system, it was decided that a safety control structure diagram would also be developed. This would provide a visualization of how the facility relates to broader considerations, such as university management structures, safety legislation, equipment design, operation and maintenance issues. This is required since all these factors need to be considered during the engineering design process so that the required levels of robustness and reliability can be achieved. Exhibit 2 overleaf provides the safety control structure diagram for the high-pressure research facility (adapted from Leveson and Dulac, 2005).

Formulating the system safety engineering through a safety control structure diagram helps to identify the dependencies between the different safety-related activities. The diagram is built on the premise that the required control of safety cannot be achieved without consideration of both system development as well as system operations. This is especially relevant for the high-pressure research facility, since there was an extended design stage that lasted over a year, during which there were a series of modifications to the equipment and facility design. These modifications had to take account of the eventual operation of the facility as well as performance requirements in terms of the desired pressure levels and corresponding shock physics parameters.



**Exhibit 1**. System architecture for operation of high-pressure equipment (Philbin, 2008)



**Exhibit 2**. Safety control structure diagram for high-pressure research facility

Others features of the diagram include a recognition of the control processes in terms of both social and technical parameters as well as the hierarchical control structures which collectively contribute to the required level of safety robustness.

**(ii). Failure Modes and Effects Analysis**

The FMEA process was carried out using the systems design visualizations described previously to guide the overall analysis. Exhibit 3 overleaf provides a representative FMEA worksheet that was produced by this exercise. This was a design (or specification) level FMEA and one of the benefits of adopting this approach is that the process can be repeated for different phases of activity for the project, such as the equipment transportation and delivery phase, installation and commissioning phase as well as the operational phase. This approach thereby allows all the potential risks that may arise throughout the facilities project to be identified and mitigated.

The use of FMEA was a crucial part of the system safety engineering for the new facility. This is because it provided a mechanism to capture individual design criteria that were required in order to produce a robust and reliable equipment and facilities design.

As the worksheet highlights, the identified fault with the highest RPN (risk priority number) was a failure of the pressure vessel or pipework. The identification of such faults and the ability to rank them according to RPN was an instructive process, as it allowed the project to ensure most attention was focused on mitigating these failure modes. However, due to the importance of the project, it was decided that all the required action points would be acted on and not just the ones relating to faults with an RPN above an arbitrary number.

The FMEA process and supporting worksheet allows identification of the following safety parameters:

* Potential mode of failure for the system function or requirement.
* Potential effects of failure (which determines severity level).
* Potential causes of failure (which determines occurrence level).
* Required process controls (which determines detection level).
* Risk priority number and criticality number can be calculated.
* Required action.

The eventual safety parameter to be established by the process is the required action. Although the required actions for this activity have been determined to contribute and improve the facilities design, it should be noted that there are also action points that relate to the equipment operations. Therefore, when the FMEA is undertaken for the operations phase, these points need to be included.

The FMEA process proved to be highly beneficial in contributing to the optimized design of both the high-pressure equipment and the supporting laboratory services and infrastructure. It also provided an effective mechanism for capturing the technical information generated and decisions that were taken. This had been a previous issue in the early stages of the project, when there had been a number of team meetings at which safety and design matters were discussed but unfortunately there was a lack of an overall framework to capture the information generated and decisions made. The use of the FMEA process and worksheets remedied this situation through providing structure to the discussions as well as an actual record of the safety analyses and supporting decisions.

The use of a multidisciplinary (or cross-functional) team was an essential part of the FMEA process and this will be discussed next. In fact one of the main shortcomings of FMEA can arise when there is an insufficiently wide perspective brought to bear on the analysis. Alternatively, problems can occur when the FMEA is undertaken only by quality or management professionals without the input of technical or engineering design professionals. It is therefore crucial that there is technical input to the process from staff who have the relevant technical expertise and experience to identify and comment on the potential failure modes.

**(iii). Multidisciplinary Teaming**

The use of multidisciplinary teams to undertake initiatives is viewed as attractive since when a group comes together that includes representatives from all the relevant areas, the outcome of the discussions or decisions will more likely include the range of different perspectives and issues that may impact on the success of the initiative (Van Der Vegt and Bunderson, 2005). Areas where there can be particular benefits from the multidisciplinary team approach include new product development as well as construction projects (Fong, 2003). In the latter case, the unique case of construction projects in terms of design, constraints and construction is well suited to analysis and implementation through a range of different perspectives.



**Exhibit 3**. FMEA Worksheet for high-pressure facility

However, the very characteristic that promotes a broader consideration of issues within multidisciplinary teams can also act as a possible limiting factor (Ratcheva, 2009). This is because differences in approaches to decision-making and professional language could potentially hinder team building. Therefore to address this issue, it has been suggested that new multidisciplinary teams need to develop their own ways of working as a consequence of the team coming together and working intensively on the initiative in question. This emerging working practice from the team then allows any differences in professional language or culture to be overcome.

In terms of the system safety engineering case study of the new high pressure facility, multidisciplinary teaming was used throughout the overall facilities project and as a way to guide the safety activities. The multidisciplinary team, which was called the working group, included the following personnel:

* Project director: Responsible for overall direction of the project; liaison with senior management; establishing a safety code of practice for the Institute.
* Project manager: Management of the project, including project planning, cost control and scheduling project tasks.
* Safety auditor: Guidance on safety legislation and university safety procedures; specialist safety expertise.
* Technical authority: Industry partner representatives who provided technical design advice, shock physics and diagnostics input.
* Academic leader: Academic input on shock physics applications.
* Laboratory manager: Responsible for developing the technical safety case, including laboratory safety code of practice documentation.
* External advisers: M&E (mechanical and electrical) and structural engineering external contractors who provided specialist technical advice.

The above list of key personnel involved in the system safety engineering activities highlights that there were a diverse collection of different viewpoints. This proved to be an asset to the project. The multidisciplinary team met periodically throughout the project design stage and as part of the design, the safety case developed in parallel. This was so the outputs from the individual safety activities could contribute to a more robust and reliable design for both the laboratory infrastructure and supporting services as well as the actual high-pressure equipment itself.

Problems did occur initially when the team first came together, particularly as the more technical-focused members of the team had a different set of terminology for the initiative compared to the general management and safety staff. This gave rise to a certain level of conflict that required careful management by the project director and project manager. However, once the team had met a number of times, the conflict dissipated. This was due to the team learning to work together and also from the team members developing a common understanding of the technical issues.

The multidisciplinary team approach was also particularly effective in contributing to the FMEA process. This was from analysis of the potential faults through consideration of the system architecture as well as from generating the actual technical information for the FMEA worksheets.

**(iv). Benchmarking**

Benchmarking is a recognized business management practice that involves a planned assessment of management best practice with a view to achieving continuous improvement. Benchmarking has been applied to a number of different areas of management and there have been some studies in the literature where safety best practice has been benchmarked. Henson (2006) has described a number of benchmark drivers for safety effectiveness within an organization, ranging from executive involvement, employee participation, teamwork and process improvement through to assimilation of safety practice into standard organizational processes.

Obtaining safety best practice information from the perceptions of key personnel presents a challenge, as this can represent tacit knowledge that is difficult to codify. Consequently, Ramírez et al. (2004) have developed a qualitative benchmarking system for the construction industry, which found that safety performance was strongly related to organizations having superior planning and control systems, quality management, cost control as well as subcontract management procedures. Benchmarking has also been used to assess safety climates in hazardous environments (Mearns et al., 2001), where the strength of an organization’s safety climate was found to influence its risk management abilities; therefore highlighting the benefit of encouraging a positive safety climate.

The case study investigation involved the use of benchmarking to assess safety management systems utilized by collaborators in the shock physics area at other universities. This benchmarking exercise had the following objectives:

* To identify the procedures and management structures used at other universities, which had already been developed for shock physics applications and where best practice could be identified.
* To identify supporting technical information that had been generated for risk assessments and safe operating procedures, which could be used to compare across the different university organizations.
* To start building a community of link-minded professionals, who collectively sought to raise the standards for safety management.

The safety management benchmarking provided valuable information to help inform the development of the facilities safety case at the university. The actual benchmarking activities mainly centered on structured meetings with collaborative partner universities, where information was shared on the different aspects of safety, together with the exchange of key safety documentation. The success of such meetings was, however, highly contingent on there being an existing good working relationship with the partner (benchmark) university, so that technical information could easily be shared between the institutions.

**(v). Enterprise Management**

The adoption of the enterprise management viewpoint has been explored across different organizational domains, such as through enterprise resource planning and architecture development for IT operations integration (Stephenson and Sage, 2007) as well as the development of improved corporate risk management (Coffin, 2009). This approach, involving integration of different organizational functions within the enterprise, can offer clear benefits, such as enhanced control and governance, effective communication, improved risk management, etc. Application of enterprise management thinking to safety management is clearly highly relevant to the aforementioned benefits. On this matter, Law et al. (2006) has used the analytic hierarchy process (AHP) methodology to identify key criteria for safety management systems, such as the need for clear client requirements, insurance company requirements and employee requirements.

As part of the case study investigation, systems level planning, through the visualization methods described previously, allowed wider dependencies to be identified. More detailed technical activities focused on specific safety risk issues to be managed and which provided granularity to the system safety engineering. The resulting safety case for the new experimental research facility is being brought together as part of a code of practice document for the high-pressure laboratory. This will be a single source of safety information, procedures and guidance for the safe operation of the new facility. The documentation builds on the decisions taken during the design stage of the preceding facilities development project, which in turn was informed by the system safety engineering activities, such as systems architecting and FMEA. This code of practice is required to be to be linked to the wider enterprise and therefore a new code of practice is also being developed for the Institute of Shock Physics, which in turn will need to relate to corporate safety documentation and procedures for the university. This integration of the safety procedures and documentation (as detailed in the previous safety control structure diagram) is a deliberate attempt to ensure effective enterprise management, so that safety risks are minimized and controlled.

**Conclusions**

System safety engineering has been explored through an analysis of some of the available tools and techniques that can help identify and manage safety risks, which include risks to the project and business performance and not just the traditional interpretation of safety risk. This holistic treatment of safety is consistent with a systems view that seeks to determine the wider implications of design risk. A literature review has elaborated on the fundamental role of engineering design and the potential that system safety engineering, through methods such as failure mode avoidance, has to improve the design process. This literature review has extended to consider a selection of decision support tools, such as FMEA and STAMP.

The case study investigation of system safety engineering for a high-pressure experimental research facility involved deployment of a range of decision-support tools. Structured technology and systems management processes have ensured that as the designs for the new equipment and facilities have matured, safety and operational risks have been mitigated through an overall adoption of failure mode avoidance. Moreover, the use of systems visualization techniques helped to identify the primary and supporting functions of the facilities system as well as the dependencies.

The systems level view was significantly enhanced through the generation of a safety control structure diagram for the high-pressure research facility. This has helped the project to address system-of-systems considerations and ultimately ensure delivery of a robust and reliable design.

**Recommendations**

Through consideration of the studies reported in this paper, it is possible to formulate the following recommendations for system safety engineering:

* Engineering design can be enhanced through failure mode avoidance, which allows the eventual design to include the countermeasures for the identified failure modes.
* FMEA is an effective tool to identify the specific information behind the potential failure modes, probable causes and countermeasure options. Potential visualization techniques that can be used to support FMEA include systems architectures, function trees, fault tree analysis diagrams, boundary diagrams and system state flow diagrams
* Safety-related control processes for a given system will depend on the hierarchies within the system as well as the constraints imposed by such hierarchies. Safety control structure diagramming is an effective technique to ensure these control processes are identified and to also consider social and technical dimensions.
* Adoption of system safety engineering is reliant on there being a supportive and knowledge-based environment, so as to enable effective use of the decision-support tools and communication between the key stakeholders. In this regard, multidisciplinary teaming, benchmarking and enterprise management can provide such an environment.
* System safety engineering programs require adequate support from senior management and there also needs to be the required funding in place.

**Acknowledgments**

The author would like to acknowledge various colleagues from Imperial College (especially Julia Cotton and Stephen Johnson) as well as technical staff from the partner company.

**References**

Andrew, J. D. and Moss. T. R., *Reliability and Risk Assessment*, Longman Scientific & Technical (1993).

Bahr, Nicholas J., *System Safety Engineering and Risk Assessment: A Practical Approach*, Taylor & Francis (1997).

Clausing, Don P., “Operating Window: An Engineering Measure of Robustness”, *Technometrics*, Vol. 46, No. 1 (2004), pp. 25-31.

Clausing, Don P. and Frey, Daniel D., “Improving System Reliability by Failure-Mode Avoidance Including Four Concept Design Strategies”, *Systems Engineering*, Vol. 8, No. 3 (2005), pp. 245-261.

Coffin, Bill, “The Way Forward: Rethinking Enterprise Risk Management”, *Risk Management*, Vol. 56, Issue 3 (2009), pp. 36-40.

Crossland, R., Sim Williams, J. and McMahon, C., “The practical application of design risk assessment models”, *Proceedings of the Institute of Mechanical Engineers – Part B – Engineering Manufacture*, Vol. 217, Issue 2 (2003), pp.227-234.

Fong, Patrick S. W., “Knowledge creation in multidisciplinary project teams: an empirical study of the processes and their dynamic interrelationships”, *International Journal of Project Management*, Vol. 21, Issue 7 (2003), pp. 479-486.

Henson, L. “Benchmarking Organizational Safety Strategy”, *Professional Safety*, Vol. 51, Issue 11 (2006), pp. 50-57.

Henshall, Ed and Campean, Ioan, “Implementing Failure Mode Avoidance”, in *Reliability and Robust Design in Automotive Engineering*, SAE World Congress and Exhibition, Detroit, MI, USA (April 2009).

Isbell, William M., *Shock Waves*, Imperial College Press (2005).

Jannadi, Osama A. and Almishari, Salman, “Risk Assessment in Construction”, *Journal of Construction Engineering and Management*, Vol. 129, Issue 5 (2003), pp. 492-500.

Kletz, Trevor, *Process Plants: A Handbook for Inherently Safer Design*, Taylor & Francis (1998).

Law, W. K., Chan, A. H. S. and Pun, K. F., “Prioritising the safety management elements: A hierarchical analysis for manufacturing enterprises”, *Industrial Management & Data Systems*, Vol. 106, issue 6 (2006), pp. 778-797.

Leveson, Nancy, G., “A New Accident Model for Engineering Safer Systems”, *Safety Science*, Vol. 42, No. 4, (2004), pp. 237-270.

Leveson, Nancy, G. and Dulac, Nicolas, “Safety and Risk-Driven Design in Complex Systems-of-Systems”, *1st NASA/AIAA Space Exploration Conference*, Orlando, FL, USA (2005).

Liu, Shaofeng and Boyle, Iain M., “Engineering design: perspectives, challenges and recent advances”, *Journal of Engineering Design*, Vol. 20, No. 1 (2009), pp. 7-19.

Mearns, Kathryn, Whitaker, Sean M. and Flin, Rhona, “Benchmarking Safety Climate in Hazardous Environments: A Longitudinal, Interorganizational Approach”, *Risk Analysis*, Vol. 21, No. 4 (2001), pp. 771-786.

Peláez, C. Enrique and Bowles, John B., “Using Fuzzy Cognitive Maps as a System model for Failure Modes and Effects Analysis”, *Information Sciences*, Vol. 88 (1996), pp. 177-199.

Pereira, Steve J., Lee, Grady and Howard, Jeffrey, “A System-Theoretic Analysis Methodology for a Non-advocate Safety Assessment of the Ballistic Missile Defense System”, *Proceedings of the 2006 AIAA Missile Sciences Conference*, Monterey, CA, USA (14-16 November 2006).

Philbin, Simon P., “Managing Projects Through Systems Engineering Methodologies”, *Proceedings from the 29th Conference of the American Society for Engineering Management (ASEM),* West Point, NY (12-15 November 2008).

Price, Christopher J., Pugh, David, R., Wilson, Myra S. and Snooke, Neal, “Flame system: Automating electrical failure mode and effects analysis (FMEA)”, *Proceedings of the Annual Reliability and Maintainability Symposium*, (1995), pp. 90-95.

Reason, James, *Managing the Risks of Organizational Accidents*, Ashgate Publishing Company (1997).

Ramírez, Ricardo R., Alarcón, Luis Fermando C. and Knights, Peter, “Benchmarking System for Evaluating Management Practices in the Construction Industry”, *Journal of Management in Engineering*, Vol. 20, Issue 3 (2004), pp. 110-117.

Ratcheva, Violina, “Integrating diverse knowledge through boundary spanning processes – The case of multidisciplinary project teams”, *International Journal of Project Management*, Vol. 27, Issue 3 (2009), pp. 206-215.

Taguchi, G., *Taguchi on robust technology development*, ASME Press, New York (1993).

Teoh, P. C. and Case, K., “Modelling and reasoning for failure modes and effects analysis generation”, *Proceedings of the Institute of Mechanical Engineers – Part B – Engineering Manufacture*, Vol. 218, Issue 3 (2004), pp. 289-300.

Spencer, Cherrill M. and Rhee, Seung J., Comparison Study of Electromagnet and Permanent Magnet Systems for an Accelerator Using Cost-Based Failure Modes and Effects Analysis”, *IEEE Transactions on Applied Superconductivity*, Vol. 14, No. 2 (2004), pp. 413-416.

Stephenson, Stephen V. and Sage, Andrew P., “Architecting for enterprise resource planning”, *Information Knowledge Systems Management*, Vol. 6 (2007), pp. 81-121.

Van Der Vegt, Gerben S. and Bunderson, J. Stuart, “Learning and performance in Multidisciplinary Teams: The Importance of Collective Team Identification”, *Academy of Management Journal*, Vol. 48, No. 3 (2005), pp. 532-547.

**About the author**

Dr. Simon P. Philbin received his PhD from Brunel University in the UK on the chemistry of energetic materials. He also holds an MBA (with distinction) from the Open University Business School and a BSc in chemistry from the University of Birmingham. He is presently Programme Director for the Institute of Shock Physics at Imperial College London and Visiting Fellow of Imperial College Business School. He is a program management professional who also conducts research on technology and project management as well as systems engineering. He has worked at Imperial College for six years and was previously with the UK Ministry of Defence for nine years.