1 Scope of the Document

This is the report of the Short-Term Scientific Mission (STSM) granted by Cost Action IS1304 to Michele Compare (Politecnico di Milano, Energy Department), hosted by Prof. Ahti Salo (System Analysis Laboratory of Aalto University School of Science) for the period 2015 August 17-28.

2 Research Context

A fundamental outcome of engineering risk analysis is the identification of risk reduction measures to be installed throughout the system, which seek to curtail the occurrence and impact of accident scenarios. In this context, the research issue of interest is to develop a methodology to establish sound quantification processes in order to characterize, on rational basis, the magnitude of risks for personnel, environment, or continuity of business operations after the implementation of risk mitigation measures. For application in industrial practice, these processes of quantification must rely on statements that are elicited from experts.

Moreover, the final objective of engineering risk analysis is also that of finding cost-effective sets of possible solutions. For this, the research interest is also on positioning the issue of installing risk reduction measures within the Portfolio Decision Analysis (PDA, [1]) framework, to find cost-effective solutions.

3 STSM research activities

During the visiting period at Aalto University School of Science, the research activities have been carried out through two main, inter-dependent pathways:

1. Literature review. Many works have been reviewed, which both propose approaches to properly install risk reduction barriers throughout a system (e.g., [2]-[9]) and describe methodologies to represent and propagate the uncertainty in the expert statements (e.g., [10]-[12]).
2. Meetings. The outcomes of the literature review have provided the basis for making brain-storming meetings aimed at envisaging possible modelling solutions to estimate the amount of reduction in risk brought by the installation of a set of risk reduction barriers, and assess this reduction against some possible conflicting criteria such as the cost, the complexity, etc. The envisaged modelling approaches have then been cross-checked with respect to the available scientific literature, also authored by Prof. Salo (e.g., [13]-[14]), in an iterative approach.

These activities have yielded a preliminary problem framing, which is summarized in the next Section.

4 Preliminary problem framing

From a broad perspective, assigning a value to risk reduction measures can be framed as the problem of estimating the performance of safety barriers to be introduced in a process or system. This concept is at the basis of the Defence-In-Depth (DID) principle, which has been introduced in the nuclear industry to fulfil very stringent safety constraints ([7]). Positioning the research problem at hand in the DID context brings an undoubtable added value: we can exploits the findings, procedures, methodologies, etc. of a sound and mature risk analysis framework. The steps to be taken to do this re-positioning can be summarized as follows.

1. Barrier grouping and rating. In industrial practice, there exist a huge number of possible devices, technical solutions, etc. to be installed as barriers in different situations, scenarios, etc. On the contrary, working with a limited number of possible alternatives is fundamental for the methodological framework to be general. Thus, a preliminary grouping or classification of the barriers is required, together with a rating of their effectiveness of the barrier in acting on the accidental scenario. Some works of the literature reviewed during the STSM (i.e., [3], [4], [5]-[7]) provide a sound basis for developing a methodology for barrier grouping and rating.
2. Risk reduction estimation. Within the DID reference framework, events and barriers before an accident are distinguished from those after an accident. In the former case, the barriers aim at preventing deviations from nominal conditions, whereas in the latter case the barriers aim at mitigating the consequences. If the accident prevention succeeds, the event is only an incident (near-miss). Otherwise, an accident happens and the effectiveness of accident mitigation barrier determines the level of consequences. This way of framing the aim of the barrier into two classes (prevention and mitigation) well fits with the BowTie approach, which is a simple and pragmatic method widely used in industrial practice (e.g., [15]). For this reason, BowTie approach is adopted in the methodology outlined during the STSM. Namely, BowTie is first used to model the risk of the system in its current configuration. Then, combinations of different barrier types and ratings are introduced into the BowTie model to estimate the effect in risk reduction.

   In particular, to take account of the possibly different magnitudes of deviations, the events considered within the BowTie scheme need to be modelled as multi-state events (e.g., 'very large gas release', 'large gas release', 'small gas release', etc.), instead of binary (e.g., 'gas release' or 'gas contained'), with a probability mass distribution associated to every event to describe the uncertainty in its realization. Against this background, the Bayesian Belief Network (BBN, [16]) methodology seems to be a promising approach to cope with this multi-state BowTie, as it provides a sound modelling framework to propagate the effects of both failure events and barrier actions with corresponding uncertainties.

   Two main issues need to be addressed by the emerging modelling framework:

a) The rules to propagate the effects of combinations of events need to be elicited from experts. In particular, in the BBN framework we need eliciting both unconditional and conditional probability values. This elicitation activity is expected to pose some challenges, such as how to avoid making complex questions (e.g., with many antecedents) especially for conditional probabilities, how to reduce the number of questions, how to check the consistency of the answers, etc.
b) The statements of the experts are expected to be qualitative (e.g., 'given that a large gas release occurred and that mitigation Barrier A was not very effective, the probability of having a very good mitigation by Barrier B is large'). The methodology to be developed to guide the installation of barriers must be able to accommodate the imprecision and uncertainty in the available information, while avoiding to introduce biases. In particular, uncertainty and incomplete information will affect the conditional and unconditional probability values entering the BBN model, which need to be correctly represented and propagated through the network. To address this issue, different theoretical framework to represent and treat imprecision have been investigated ([17]-[18]), and evaluated also with respect to their applicability to the BBN-based risk model.

3. Barrier portfolio optimization. Once we have a risk model capable of mapping a given combination of barriers into the value of risk reduction, we can use it to find portfolios of barriers, which are optimal with respect to conflicting objectives such as:

I. Minimize the risk related to the operation of an engineering system or process.
II. Minimize the installation cost of the barriers.
III. Maximize the system availability. In fact, the larger the number of activated barriers based on monitoring, the larger the probability of triggering false alarms that may stop the production.
IV. Maximize the diversity of the barriers: the larger the diversity of the barriers (physical principles they are based on, different energy sources, etc.), the smaller the probability of having common cause failures.
V. Fulfil the constraints on the risk acceptability.
VI. Fulfil the constraints on the applicability of the barrier to the specific case.

To find optimal portfolios of barriers in the presence of imprecise values of risk reduction benefit, installation cost, etc. the Robust Portfolio Modelling (RPM, [19], [20]) technique will be considered and adapted to the needs of the peculiar research context. RPM also allows considering possible synergies and inter-dependencies among the barriers included in the portfolio, which may represent an important factor to drive the selection of optimal portfolios.

5 Research activities post-STSM

The objective of the STSM was that of pave the way to a fruitful research collaboration between the involved Institutions (i.e., Aalto University, School of Science and Politecnico di Milano, Energy department). The preliminary problem framework is at the basis of the actual development of the methodology, which is being carried out by a PhD student under the supervision of Profs Ahti Salo and Enrico Zio, and Dr. Michele Compare.

6 Other STMS activities

During the STSM, Michele Compare had the possibility of giving an informal seminar focused on previous research works to the members of the System Analysis Laboratory at the School of Science. This has given the possibility of identifying possible future research collaborations on other research topics.

7 References

[1] Salo, A., J. Keisler, A. Morton, An invitation to portfolio decision analysis. A. Salo, J. Keisler, A. Morton, eds., Portfolio Decision Analysis, vol. 162. Springer, New York, 2011.

[2] ISO:13702 Petroleum and natural gas industries—Control and mitigation of fires and explosions on offshore production installations—Requirements and guidelines International Organization for Standardization, Geneva, 1999.

[3] Skelt, S. Safety barriers: Definition, classification, and performance, Journal of Loss Prevention in the Process Industries, 19(5), pp. 494–506, 2006.

[4] Guldenmund, F.W., Hale, A.R., Goossens, L.H.J., Betten, J., Duijm, N.J. The development of an audit technique to assess the quality of safety barrier management. Journal of Hazardous Material, 130 (3), pp. 234–241, 2006.

[5] De Dianous, V., Fiévez C.,ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance. Journal of Hazardous Material, 130 (3), pp. 220–233, 2006.

[6] IEC 61508-1, Functional safety of electrical/electronic/programmable electronic safety-related systems. 2010.

[7] IAEA-TECDOC-626, Safety related terms for advanced nuclear plants, IAEA-TECDOC-626, International Atomic Energy Agency, Vienna, 1991.

[8] INSAG-10, Defence-in-depth in nuclear safety. International Atomic Energy Agency, Vienna, 1996.

[9] Neogy, P., Hanson, A. L., Davis, P. R., Fenstermacher, T. E. Hazard and barrier analysis guidance document, Rev. 0. US Department of Energy (DoE), 1996.

[10] Helton, J.C., Johnson, J.D., Oberkampf, W.L. An exploration of alternative approaches to the representation of uncertainty in model predictions. Reliability Engineering and System Safety, 85, pp. 39-71, 2004.

[11] Dubois, D., Prade, H. Possibility theory, probability theory and multiple valued-logics: A clarification. Annals of Mathematics in Artificial Intelligence, 32, pp. 35-66, 2001.

[12] Baudrit, C., Dubois, D., Guyonnet D. Joint Propagation and Exploitation of Probabilistic and Possibilistic Information in Risk Assessment. IEEE Transactions on Fuzzy Systems, 14 (5), pp. 593-608, 2006.

[13] Vilkkumaa, E., Liesiö J., Salo, A. Optimal strategies for selecting project portfolios using uncertain value estimates. European Journal of Operational Research, 233, pp. 772-783, 2014.

[14] Kangaspunta, J., Salo, A. Expert Judgments in the Cost-Effectiveness Analysis of Resource Allocations: A Case Study in Military Planning. OR Spectrum, 36(1), pp. 161-185, 2014.

[15] Duijm, N.J. Safety-barrier diagrams as a safety management tool. Reliability Engineering & System Safety 94, pp. 332-341 (2009).

[16] Jensen FV, Nielsen TD. "Bayesian networks and decision graphs," 2nd ed., New York, Springer, 2007.

[17] Simon, C., Weber, P., Evsuko, A. Bayesian networks inference algorithm to implement Dempster Shafer theory in reliability analysis. Reliability Engineering and System Safety, 93 (7), pp.950-963, 2008.

[18] Zhai, S., Lin, S. Bayesian Networks Application in Multi-State System Reliability Analysis, Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13).

[19] Liesiö, J., Mild, P., Salo, A., "Preference programming for robust portfolio modeling and project selection", European Journal of Operational Research 181 (3), pp. 1488-1505, 2007.

[20] Liesiö, J., Mild, P., Salo, A., "Robust portfolio modeling with incomplete cost information and project interdependencies", European Journal of Operational Research 190 (3), pp. 679-695, 2008.