OVERVIEW OF FINE EXACT METHODS OF SAFETY ENGINEERING

Dana PROCHAZKOVA

Abstract: The safety, security and risk engineering are systematic use of general findings, engineering knowledge and experiences for: ensuring safe object from internal hazards (risk engineering); from internal and external hazards (security engineering); and, in present, for optimising the protection of human lives, environment, property and economic affairs (safety engineering). Taking a comprehensive view, one needs to examine all potential conditions that could threaten the favourable operation of a given system in all stages of its life cycle, and identify the capabilities for overcoming them by prevention, preparedness, response and renovation. It uses tools, methods and techniques that indicate how we could lay out the problem in text; determine what we ought to solve; collect and create data sets so they might have a clear evidence to a given problem; select a method for data processing so outputs might be relevant to a given problem; and interpret the outputs in given conditions. Therefore, it uses a family of exact methods, tools and techniques; this paper presents a survey of fine exact methods and suggests their systemization.

Keywords: Risk engineering, security engineering, safety engineering, risk, methods, tools, techniques.

Introduction

The human system safety represents a well-ordered set of measures and activities that provides human system security and sustainable development; by analogy it holds for other systems.[1] In practice the system security (the security of system) is reached by tools of security engineering.[2] High-powered tool represented by engineering of the safety called "safety engineering" does not only deal with technical problems but it respects public assets in the system vicinity, is a branch applying the methods, tools and techniques (hereafter "the MTT") and it is based on engineering and managing approaches by way in order that the system might be safe for all public assets during the whole its life cycle.[3] The both engineering type predecessor was the risk engineering the standards and norms of which started to be developed in the middle of last century.

INFORMATION & SECURITY. An International Journal, Vol.28, No. 2, 2012, 167-178.

The ensuring of such comprehended safety management is particularly marked from the risk management viewpoint by these characters: sitting – designing – construction – project with risk reduction; operation with integration of early warning systems and of procedures for management of acceptable level of risks; and defeating the abnormal, emergency and critical conditions at operation and at putting out of operation. However, the safety engineering conception was just expressed by technical terms, it holds at other domains that are important for safe human system with sustainable development; only there is necessary to use suitable transformation of terms in order that it might be comprehensible for specialists of partial disciplines that are only adapted to actual terminology.[4]

Safety Engineering

Safety engineering is a branch that solves problems, i.e. it uses the MTT that indicate how we ought to: texturize the problem; determine what we would solve; collect and create data sets in order that they might have a clear evidence to a given problem; select real method for data processing in order that outputs might be relevant to a given problem; and interpret the outputs in given conditions. From the professional view it goes on process seeking the all potential conditions that could threaten favourable operation of a given system in all stages of its life cycle, and identifying the capabilities for their defeating by prevention, preparedness, response and renovation. In a present concept the safety engineering is based on system interpretation, and therefore, in addition to a standard methodology it also uses the *system methodology* that includes: system analysis; system design; implementation of solution; and system operation.[5]

Safety engineering is based on the key concepts:

1. The approach to a problem is based on risk with rule that intensity of work and documentation are adequate to risk level;
2. In professional procedure respecting the solved problem logic there must be considered critical attributes of quality and critical parameters of process;
3. The problem solution is directed to critical items, i.e. the topics are monitoring and management of critical aspects of technical systems ensuring the operation consistence of systems;
4. Certified parameters of quality must be included in project proposal for problem solving;
5. It puts emphasis on quality engineering procedures which means that the correctness of selected procedures in given conditions must be demonstrated;

6. During the whole life cycle there is aiming to safety upgrade (by help of safety management systems), i.e. it goes on continually improving the processes with use of analysis of root causes of defects and failures.

For above given principles respect there must be used relevant data sets and only verified methods that provide outputs with designated testified competence. Because, in group of cases there is not well coped with vagueness in data, there are used in practice the procedures designated as good practice procedures / good engineering practice procedures. It goes on modus operandi procedures in individual domains that on the basis of experience lead to a good result. The given procedure is used in cases in which there was not approved any unified procedure. It is often used at measurements in laboratories, negotiation with humans etc.

Good engineering practice (good engineering procedure) is then defined as a set of engineering methods and standards that are using during the life cycle of technical system with aim to reach appropriate and cost- efficient solution. It is supported by fit documentation (conceptual documentation, diagrams, charts, manuals, testing reports etc.).

In a given context the engineering expertise is expression of capability to: apply knowledge of mathematics, science and engineering; propose and realize experiments; analyse and interpret data; propose components or whole system according to requirements and under the frame of realistic limitations identify, formulate and solve engineering problems; ensure the effective communication; comprehend impacts of engineering solutions in broader context; use the advanced tools and methods in engineering practice; adhere professional and operational responsibilities and ethics; lead the interdisciplinary team.

Safety Engineering Methodology

The safety engineering methodology at problem solving considers that all processes are under way in dynamically variable universe, and therefore, there must be used a special apparatus that is created by a set of used research procedures for optimum risk management. With regard to rating the accessible data sets, existing uncertainties and vagueness at these data the practice separates the tasks that may be solved deterministically, stochastically and or only heuristically.[6] It uses by integrated way qualitative and quantitative approaches to risk and to system security and in a general ground it consists of next given steps: definition of system and its vicinity; identification of danger; *determination of hazards from extreme events (beyond design disasters*); risk assessment; proposal of corrective and remedial measures and actions according to safety criteria with aim to ensure acceptable security; and verification of risk accept-

ability. In all missions it uses the MTT that are dependent on quality of disposable data and on goals of safety management.

The word “exact” in safety engineering and in risk engineering is apprehended as strictly scientific, i.e. the facts are found out by texturized, precisely described and reproducible way from validated data, i.e. data hold appreciated uncertainties, vagueness and testified competence to a given problem.

The system safety management inserted in safety engineering is then discipline (branch) applying the MTT based on engineering and managing approaches with aim to ensure in order that the system and its vicinity might be safe. It leans on risk management to which there is included the precaution principle. In the case of complex safety management it goes on management of complex (integral) risk. This management type is then the discipline (branch) for the SoS (System of Systems) safety management.[7]

Risk and Its Aspects

The risk is for engineering practice expressed as probable size of losses, damages and harms on followed assets that are caused by a given disaster with specified size and that are rescheduled for certain time unit (usually 1 year) and certain territory unit that is in agreement with the EU standard under preparation.[8] At advisement in practice we distinguish whether the risk realisation goes on steadily by same way or variously in dependence on immediate site and time conditions of assets. In the first case we determine a sort of mean value, and its validity for use in practice is connected with a condition that it is determined for much worst case (this case we can find in norms and standards based on deterministic approach). The second case corresponds to a variable reality - there are determined the variant scenarios of risk realisation and their occurrence probabilities; from these data by clear mathematical approach the mean value and its dispersion are determined (we can find it in norms and standards based on probabilistic approach). At present practice for complex cases there are used precisely defined heuristic procedures that are considered at preparation of groundwork for strategic management.

The principal attributes of each risk are *uncertainty and vagueness*. Their sources we divide into three groups, namely to variations originating at: usual system process life cycle at normal conditions in vicinity (uncertainties); real changes of system process life cycle in time and space that affects occasional extreme values occurrences – we consider normal and abnormal conditions (uncertainties and vagueness); variable system process life cycle that is caused by process changes in time and space induced by outside causes or by critical conditions (vagueness).

Data uncertainty relates to dispersion of observations and measurement. It may be included into assessment and prediction by mathematic statistics apparatus. The vagueness relates to both, the lack of knowledge and information and the natural variability of processes and actions that caused disasters. For processing the vagueness the mathematic statistics apparatus in insufficient and , therefore, it is necessary to use recent mathematical apparatus that offers e.g. extreme values theory, fuzzy set theory, fractal theory, dynamic chaos theory, selected expert methods and suitable heuristics.

The data vagueness follows from reality that data are incomplete, inhomogeneous (i.e. their accuracy depends on their size or on time of occurrence) and non-stationary, i.e. data have massive dispersion and are encumbered by random and sometimes also by systematic errors, the distribution functions of which cannot be usually determined. Because nothing is absolutely precise we must generally considered data uncertainties and vagueness at each quantity that we investigate. Therefore, both the safety engineering and the risk engineering require in order that the quality of data set ought to be verified from the viewpoint of their credibility with regard to a given task.

In risk engineering being a predecessor of safety engineering [9] there were for risk determination used further given principles: risk is determined after design of system; risk determination is directed to a level of system and its components, i.e. there is not considered outer vicinity and protection of public assets; there are only required knowledge of system and processes, i.e. there are not require knowledge of outer vicinity and protection of public assets; and if risk exists then it is determined and solved but the lack is that there are not possible to remove risks connected with inappropriate solution for given site and system.

The risk engineering leans on risk management and it searches problem solution by way that it individually considers disaster after disaster and requires coping all risks the occurrence probability of which is equal or higher than 0.05. Usually it only includes disasters the sources of which are within the system and hence it very often only solves technical aspects of problem.

Safety engineering uses at risk determination the following principles: risk is determined during the given system whole life cycle, i.e. at sitting, designing, building, operation and putting out of operation, and eventually at territory bringing in original condition; the risk determination is directed to user's demands and to level of provided services; risks are determined according to criticality of impacts on processes, provided services and on assets that are determined by public interest; and unacceptable risks are mitigated by tool for risk management, i.e. according to technical and organisational proposals, by standardisation of operating procedures or by automatable check-up.

Safety engineering leans on risk management from all possible disasters at a stroke and it searches an optimum problem solution applying the All Hazard Approach (i.e. it considers all possible disasters without respect whether their source are within or outside a given system and it uses the precaution principle). It uses tool "safety management", i.e. risk management supporting the human system security in which it is also included sustainable system development. In technical slang we speak that safety management forms inherent safety of human system against to design disasters and by implementation of precaution principle we upgrade resistance against to unacceptable impacts of beyond design disasters the occurrence of which is so low probable that it is unforeseeable. In practice there are introduced principles as fail safe; carry out only determined functions, e.g. if you cannot fulfil the aim, do not do anything.

Exact Methods, Tools and Techniques of Safety Engineering

From above given facts it follows that safety engineering is the branch that solves problems, i.e. it uses the MTT that indicate how to: texturize problem; determine what might be solved; collect and create data set in order that it might give evidence to a given problem; select method for data processing in order that outputs might be relevant to a given problem solution aim; and how to interpret outputs of data processing from the view of human system safety that includes functionality and reliability of a given system.

From the given facts it follows that at selection of the MTT we must respect that safety engineering is multi-branch and cross-section discipline that uses both, the general and specific methods, tools and techniques. The specific ones are either simple or complex.[10] The complex ones represent use of several general or simple MTTs. Individual MTTs respect reality that aimed complex safety management of each system cannot be only reached by technical or knowledge items but by combination of possible and accessible branch tools of human activity, i.e. they must be used the MTT logic, technical, finance, managerial and arbitrary because integral part of safety engineering is decision-making on technical problems, human factor, costs and on time schedule etc. It means that for solution of present tasks of safety engineering that requires non-trivial problem solving to use the multi criteria MTTs in which we must respect that assets and risk source have different natures that are roots of criteria incommensurability and at their selection we must respect data quality, structure of solved problem and requirements on output quality; and specially verify both, the data quality (correctness, completeness, testified capability to problem) and also the expert competences (IAEA, OECD, USA, WB etc. have strict criteria for expert qualification verification).

In terms of data acquisition we separate safety engineering MTTs into:

Empirical. The survey of facts is made by inquiries and questionnaires. These are used at data collection on human behaviour and human society behaviour in sociology but also at acquisition of impact distribution in the case of earthquake, wind storm or other disasters in territory. In exact sciences there are used for their rapidity and modesty. Accuracy of such data is lower than those obtained by instrumental measurement but qualified statistical processing gives good and reliable information for decision-making and management.

Theoretical. They create findings, hypotheses, theoretical constructions on the basis of general science procedures, i.e. they are based on use of algorithms that lead to solving all tasks of a given type.

Expert. They use professional (professionals) for activity that requires special knowledge. They are used in many situations the common feature of which is necessity of professional (expert) judgement of problem and of its further development in future. They are also used if there is necessary to eliminate local view on a given problem and to judge it independently in new, broader or more specialised frame.

Regarding knowledge acquisition, we distinguish the following MTTs:

- *procedures for acquisition of fundamental (usually individual) knowledge* – as discovery of properties and behaviour of a given substance, behaviour of nanomaterials under different physical and chemical conditions, etc.;

- *procedures for solution of simple practical tasks* – as allocation and application of fundamental knowledge in practice, e.g. typical earthquake impact scenario for earthquakes from one focal region in a given region; way of response to chlorine release from a given building etc. In this case we must also solve at data acquisition whether we are dependent or independent on phenomena recurrence (e.g. measurement of natural events is non-reproducible) and how inaccuracies in fact acquisition may influence uncertainties and vagueness in data and by that also in knowledge;

- *procedures for solution of tasks of strategic nature* – as discovery of basic knowledge for support of capability to solve effectively present and future problems of a given object, e.g. connected with security and sustainable development of human system, with human society development in a given region. In this case we must solve how at data acquisition we are dependent on fact whether followed processes are or are not stable in space and time (e.g. processes of occurrence of floods, earthquakes etc. are not stable in time – extreme phenomena occur rarely and irregularly in time and space) and how inaccuracies in data acquisitions might influence uncertainties and vagueness in data and by that also in knowledge, and what follows from it for prediction and consecutively for management; i.e. it goes on qualified selection of

optimum variant from a set of variants offering different combinations of followed parameters for problem solving.

Examples of Methods, Tools and Techniques used in Safety Engineering

There are dozens of MTTs used in safety engineering. Some are broadly known, e.g. methods of arithmetic, algebra, geometry, logic, etc. Then there are methods of mathematic statistics, cluster and factor analysis, application of time series, methods of operating research, network analysis methods, specific methods for decision-making support, and specific methods for safety engineering including those for risk engineering.

Examples of general MTTs include analytical hierarchy process (AHP); event tree analysis; analysis of causes and consequences; cost-effectiveness analysis; cost-benefit analysis; cost-minimize analysis; cost-utility analysis; thought map application; problem tree application; benchmarking; fuller method; Gordon method; heuristic methods for problem structuring (e.g. stakeholders analysis; boundary analysis; event analysis; brainstorming; brainwriting; why-why diagram; fishbone diagram); dimensional analysis; hierarchy analysis; causal loop models; classificatory analysis; mind maps; problem tree; technology assessment); Ishikawa diagram; causal analysis; risk quantification; risk matrix; marginal analysis; mathematic programming; responsibility matrix; methods of aimed prognosis; Delphi method; ALO-FUL; extrapolation method; main component method; goals achievement matrix; method of variants judgement; method of marginal valuation; fuzzy set; Monte Carlo; management by objectives; methods of operation analysis, like operation research; methods for multicriteria assessment; methods for determination of weights of variants or criteria (e.g. swing method, antipathy to changes, Macbeth and holistic method; methods for problem structuring: macro block scheme, Pareto diagram, affinity diagram, Ishikawa diagram, how-how diagram, priority matrix, decision-making matrix; network analysis methods (e.g. CPM (critical path method); MPM; PERT (program evaluation and review technique); RAMPS; GERT, Petri nets (colour Petri net, fuzzy colour net etc.); tree relevancy methods (examples: PATTERN, QUEST, SEER); modelling; panel discussion; PCDA (plan-do-check-act); Saaty method; SWOT analysis; system methods (e.g. application of analysis of changes, HAZOP, FMEA, What-If, FTA, ETA, dependability analysis; survivability system analysis; vulnerability analysis, resilience analysis; function analysis, technique for human error analysis); analysis of risks connected with facility(PSA, event and barrier function, discrete event analysis); application DSS technique; criteria weight determination technique (e.g.: allocation of points; application of point scale; theory of extremes (e.g. hazard assessment according to enormous number theory, application of Probit function; theory of games.[11]

Among the *examples of specific or specially adjusted MTTs* are:

- Methods for risk analysis and risk assessment (*traditional ones as*: check list; safety audit; What – If analysis; Preliminary Hazard Analysis; HAZOP analysis (Hazard Operation Process Analysis); QRA (Process Quantitative Risk Analysis); ETA (Event Tree Analysis); FMEA (Failure Mode and Effect Analysis); FTA (Fault Tree Analysis); HRA (Human Reliability Analysis); FL-VV (Fuzzy Set Method); RR (Relative Ranking); CCA (Causes and Consequences Analysis); PSA (Probabilistic Safety Assessment); *specialised ones as:* CRAMM (CCTA Risk Analysis and Management Methodology – see standards CSN ISO/IEC 13335 and ISO/IEC 17799), COBRA, MELISA.; methodologies: *@risk* (based on Monte Carlo Methods); *RiskPAC*; *RiskWATCH.*[12]

- Set of adapted methods for assessment of disasters and for risk management such as: method for determination of relevant disasters in a territory; method for determination of maximum expected disaster size (it has to modifications: root of hazard is only one source of disaster; and root of hazard is several sources of disaster); method for determination of attenuation of disaster impact size with distance from source of disaster; methods for determination anomalies in territorial distribution of disaster impacts; method of determination of unacceptable disaster impacts; method for assessment of potential damages on property caused by unacceptable disaster impacts; method for determination of optimum corrective measures for expected disasters in a given territory; method for implementation of corrective measures for ensuring the property renovation in a given territory; method for determination of database of corrective measures to individual disasters; method for determination of parametric relation between cost for renovation vs. disaster size; method for determination of financial reserve for recovery. Examples can be found in the experience of the US FEMA; the Swiss PLANAT programme for public administration, the Netherlands, UK, etc.

- Methods for *investigation of interdependencies in systems of systems* (SoS). For study of the SoS, their behaviour and failure there are apart from analytical methods, traditional methods of risk analysis, scenarios, deterministic and probabilistic analysis of safety, security analysis of networks, reliability analysis, expert appraisals, decision matrixes (risk matrix, criticality matrix), Monte Carlo, etc. there are often used specific methods for model compilation, namely: Bayesian Method, Bayesian Network, Mixed Bayesian Network, Fuzzy Bayesian Network Model, Bayesian Reliability Model, Fuzzy Rule-based Bayesian Reasoning (FuRBaR); Petri Nets (PN), Coloured Petri Nets (CPN), Stochastic Petri Nets (SPN), Coloured Stochastic Petri Nets (CSPN); Case Study (CS); Multi-Attribute Utility Theory (MAUT); Multi-Criteria Analysis (MCA); Weighted Sum Approach (WSA); Concordance, Discordance Analysis (CDA); Technique for Order Preference by Similarity to Ideal Solution

(TOPSIS); Ideal Point Analysis (IPA); Aggregation Preferences (AGREPREF), Preference Ranking Organisation Method; for Enrichment Evaluations (PROMETHEE); Markov Chain (MC); Multi-Objective Genetic Algorithm (MOGA); Multiplicative Intuitionist Linear Logic (MILL), etc.

- *Engineering working methods* include MTTs used for: *disaster assessment* (i.e. site, maximum expected size, occurrence probability or occurrence frequency, distribution and size of impacts); *hazard assessment* (determination of normative disaster size – the most frequently design disaster = centennial disaster); and for *risk assessment* (in a given site according to hazard size, the amount and vulnerability of assets). Generally it must be for each investigated object or specific site determined: size of the maximum expected hazard from a given disaster; set of phenomena that will be caused by occurrence of disaster with size equal to maximum expected hazard; so called secondary impacts and followed impact levels (cascade chain of impacts) with regard to: site fundament structure, construction of followed building, technology located in a given building and according to recent findings also to a number of humans being in the given site; assessment of secondary impacts; size of secondary impacts and harms and losses caused by them; and to consider security stand-by.

Then there are the MTTs as:

Resistance / resilience certification, i.e. the technique of proof that followed risks are managed by equipment construction, building construction and by safety systems, i.e. the required safety is ensured. It is created by set of calculations, tests, analogies, judgements by which there is possible with certain level of credibility to determine that followed item and its parts are resistant up to determined level of disasters.

Safety certification, i.e. the technique of proof of safety that starts from disasters - All Hazard Approach,[13] i.e. not from set of risks determined because this set needs not be complete.

Both mentioned certifications are in design and operation documentation and in documentation as: Safety Program, Safety Report and Safety Certificate.

The negotiation with risk as a technique by which we separate the risk copying into categories - part of risk: the realisation of which is averted by preventive measures and activities; mitigated by preparedness, i.e. by warning systems, training and education of possible afflicted population and rescue units, alternative solutions (e.g. preparation of sites for relocation of important industry in advance); the repayment of expected damages is shifted to insurance office; for which there is prepared response and renovation and their knowledge, personnel, materially technical and financial base; contingency plan for part of risk that is uncontrollable (because no knowledge

and capabilities), low frequent occurrence or too expensive. In the process management there is a rule that all involved participated in risk copying and that real risk copying is assigned the subject that is well prepared. These rules are the basic part of safety engineering.

Among the examples of safety engineering tool are the strategic safety management of territory (processes as the DSS) and the application of SWOT analysis and case study methodology.[14]

Conclusion

To reach aims and human dreams we must qualifiedly manage the risks. Therefore, the safety engineering requires to: apply all hazard approach at risk identification; determine correct size of hazard; analyse and assess correctly the size of risk (that is only possible if relevant data and qualified MTTs are used); cope with risks correctly (i.e. measures and activities for risk reduction and mitigation to perform in details and connections in order that it might not get to new risk origin or to grow of risk in other part of human system); follow system and its processes continuously and to revise with regard to new knowledge and experiences. In all activities there is necessary to think in connections (human intellect is a repository of tacit knowledge), to use qualified data, qualified MTTs and by correct way to use experiences (good practice principles are very useful).

Because the safety management of each object is dependent on risk management quality that is predetermined by quality of data and their processing the MTT knowledge is very important and because it demands interdisciplinary and multidisciplinary data processing the special methodical education in universities seems to be very useful.

The judgement of practical problem solutions shows that for advanced solutions of safety engineering problems we need concept of reality that is represented by system with several mutually interconnected assets being dynamically variable. This new concept is ambitious not only on various nature data but also on their processing with known witness capability.

Acknowledgement

The research was supported by the Ministry of Regional Development, Ministry of Interior, Ministry of Agriculture of the Czech Republic, the Czech Technical University, Faculty of Transport Science, Institute for Security Technologies and Infrastructures and by the project FOCUS (with funding from the EU Seventh Framework Programme—FP7/2007-2013—under grant agreement n°261633. For more information visit the project website at www.focusproject.eu).

Notes:

[1] Dana Prochazkova, *Human System Safety* (Ostrava: SPBi, 2007), – in Czech.

[2] Ross J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems* (Indianapolis, IN: John Willey, 2008).

[3] Harold E. Roland and Brian Moriarty, *System Safety Engineering and Management* (New York, NY: John Willey, 1990).

[4] Dana Prochazkova, "Methodology for Selection of Optimum Model of Strategic Territory Safety Management," in *Požární ochrana 2010* (Ostrava: SPBi, 2010), 260-265; Dana Prochazkova, *Strategic Management of Safety of Territory and Organisation* (Praha: Karolinum, 2011). – both in Czech.

[5] Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*; Roland and Moriarty, *System Safety Engineering and Management*.

[6] Dana Prochazkova, *Risk Analysis and Risk Management* (Praha: Karolinum, 2011). - in Czech.

[7] See the referenced works of the author.

[8] *Risk Assessment and Mapping Guidelines for Disaster Management*. EU draft standard (Brussels, December 2010).

[9] ESRA: *Reliability, Risk and Safety: Theory and Applications* (Leiden: CRC Press, 2009); the referenced works of the author.

[10] Prohazkova, 2011; H.J. Pasman, "Developments in loss prevention/ process safety / risk assessment methodology: layer of protection analysis," 15th International Congress on Chemical and Process Engineering, Praha, 25-29 August 2002.

[11] For details see Prochazkova, *Methods, Tools and Techniques for Risk Engineering*.

[12] More than 1000 specialised methods that are supported by software are accessible at www.riskworld.com. They have been developed for specific cases; hence, before their use it is necessary to verify if the conditions for technology transfer are met.

[13] *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101 (Washinton, D.C.: Federal Emergency Management Agency, 1996).

[14] Dana Prochazkova, "Application of SWOT Analysis and of Selected Types of Case Studies at Selection of Model for Strategic Territory Safety Management," in ENVIRO, STRIX ann. Gillian, 2010. – in Czech.

DANA PROCHAZKOVA – see the CV on p. 36 of this volume.