- neglecting the assessment of investor financial capacity in granting the relevant authorizations.

3. Inadequate legislation:
   - insufficient public administration supervisory power,
   - insufficient legislation governing the design of SCPS (too general, incomplete, allows for several interpretations,
   - insufficient enforceability of the right to safety, employee protection, public protection and the environment.
4. Other:
   - the State has not professional institution which has been able to professionally assess the process of making the SCPS in all aspects,
   - haste in design and construction due to pressure from politicians,
   - the State has not developed a system of supervision under design of SCPS,
   - the State did not have criteria for assessing the accuracy of the design of SCPS,
   - contractor and investor did not cooperate with the public administration during the design of the SCPS,
   - natural disaster occurrence as: earthquake; landslide; flood; fire,
   - occurrence of phenomena as: corruption; insider´ attack; hackers´ attack; terrorist attack.

5 Risk Management Plan

The risk management plan for design process is after prevention principles the second important tool for the SCPS design. For creating this top-quality safety management tool, they are considered both, the current knowledge and experience on risks associated with SCPS and their surroundings summarized in [12], and the new real knowledge, which were obtained from study of compiled original database of SCPS failures and accidents, among the causes of which they were found defects in the area of design; totally 521 cases were identified.

The aim of risk management plan is to ensure the SCPS coexistence with surroundings. Two actors are considered - public administration, which supervises activities in the territory including the SCPS with aim to ensure the safety of territory and citizens, and designer, who is responsible for the safety of design of SCPS, which also includes the protection of the surroundings and inhabitants. It is prepared in the form of table; Table1 shows example for designing; complete table is are in [12].

Table 1. Risk management plan for SCPS designing directed to coexistence of operated SCPS with surrounding.

Risk area	**Risk description**	**Probability of occurrence Risk impacts size**	**Risk mitigation measures**
Public administration	As a result of absence of a State strategy on SCPS design focused on safety, it is possible to enforce current political interests, requirements of coercive groups or the failure to cope with extreme political situations (war, terrorist attacks), which in turn leads to reduction in human living standard and safety of citizens, economic instability, etc.	Probability: Large Impacts: Large	***Measures:*** To develop the relevant State strategy and adapt the Building Act ***Execute:*** Prime minister ***Responsibility:*** Parliament chairman
	Due to lack of competence of public authority in overseeing the SCPS design there is an extension of construction, problems in commissioning, accidents accompanied by enormous expenditure from the public budget, disruption of citizens security.	Probability: Large Impacts: Large	***Measures:*** To adapt the Competence Act and the laws associated with it. ***Execute:*** Prime Minister ***Responsibility:*** Parliament chairman
	……..		
	As a result of errors in the authorized designer selection, the project is of poor quality, which sooner or later will disrupt the construction or operation and lead to accidents accompanied by enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	*Measures:* Change of designer *Execute:* Authorized investor worker *Responsibility:* Investor director
Future operator	…….		
	As a result of a poor estimate in the field of supplier – customer relations, the project is based on unrealistic data, which sooner or later will lead to disrupts the construction or operation of a SCPS, enormous expenditure, disruption of citizens safety and problems with public administration.	Probability: Medium Impacts: Large	*Measures:* To force investor to perform remedy *Execute:* Authorized future operator worker *Responsibility:* Future operator director
Authorized designer	…….		
	As a result of a poor quality or non-cooperative team of project processors, the project is of poor quality and it leads sooner or later to disruption of construction or operation, enormous expenditure, citizens safety and problems with public administration. …….	Probability: Medium Impacts: Large	***Measures:*** To introduce rules for team cooperation ***Execute:*** Authorized designer team worker ***Responsibility:*** Authorized designer team director

Table 1 serves for protection against problems that impede to building permit issue. Table shows that big role plays the human factor, namely at way of execution of critical tasks of designing (terms of references compilation, use of knowledge on compilation of safe design etc.) and at professionality of supervision performed by the public administration directed to public interest.

Risk management plan was tested with success at six medium SCPS [25]; their site-specific compilation and application in practice are ambitious on experts´ knowledge and time, and it requires the access to detail SCPS and public administration documents, which is connected with respecting the certain legal rules.

6 Procedure of SCPS risk-based design generation

Based on the above facts, we have compiled a procedure for SCPS risk-based design compilation to respect applicable standards, practices of good practice and the above principles for working with risks. Since in many cases it is necessary also to consider the opposite criteria when deciding on a problem, we used both simple methods (linear and tree) and multicriteria tool – the DSS in the work [36] when working

with risks, for each component, the process of production and the entire power plant.

When deciding on specific items, we used both partial risks of critical components and systems and their interconnection, as well as integrated process risks and integral risk of the whole. We considered all the risk sources listed in chapter above, determined their sizes for the above items that had the parameters required by the standards. For all relevant risk sources (in accordance with focus, we have considered the eight most common combinations of external risk sources) we have identified the threat size for the 1000-year interval for quiet sites (the size of risk sources of all kinds is acceptable and calculated in all construction and design standards), places at risk (with one to two larger sources of risk not foreseen in building and design standards) and critical sites (multiple sources of major risks , which is not foreseen in building and construction standards).

In the case of the second and third cases, the designer needs to think as follows:

1. Can I eliminate the hazard?
2. Can I reduce the size of this hazard?
3. Cannot I create a new hazard with the proposed measures to manage this hazard?
4. What technical and control systems are required to manage the hazard that is left?

In order to manage the SCPS safety according to [12,19] within the design it is necessary to create:

- conditions for shaping the culture of safety in the operation of the SCPS, which is implemented by: compliance with safety rules and procedures; the responsibilities of the managers; workplace running reporting systems; workplace audits; communication with employees; a proactive approach to risk management; taking care of a safe workplace, communications on safety, and training the employees.,
- the right loss prevention policy implemented by safety management (higher priority than reliability),
- a clear division of responsibilities (consistency between competences and responsibilities is important),
- the distribution of equipment, components and systems according to criticality,
- operating regulations for normal, abnormal and critical conditions,
- correct modes for the operation of equipment, components and systems, especially critical ones,
- summary of critical assets - their limits and conditions and requirements for risk-based inspections (RBI),
- maintenance plan (preventive and forecasting for critical equipment, components and systems),
- modernization and renewal of equipment, components and systems, especially critical ones,
- a program of non-destructive tests of critical equipment,
- emergency (contingency) plans,
- a continuity plan that ensures the survival of the SCPS (mainly its critical items) under extreme conditions.

On the basis of above knowledge and experiences from practice [25,37], the technique for compilation of a risk-based design we propose by such way:

1. To establish a list of components and systems that comply with the standards and will be combined into sub-units.
2. For all items in the list of components and systems (point 1), to determine the limits and conditions from the point of view of their operation in a particular territory with regard to: the material from which they are made; demands on uptime; the working mode in which they will work; human factor; and possible other risks (internal fire or explosion and external risks).
3. For all items in the list of components and systems (point 1), to determine for the site-specific sources of risks determined by considering the All-Hazard-Approach, the sizes and characteristics of the partial risks.
4. For all risk sources (point 3) to determine impact scenarios; and when some risk impacts are not acceptable, it is necessary to increase the material and construction requirements so that these risks may be acceptable.
5. To establish the component interconnections and model of their interconnections, which meets standards and inherent safety requirements.
6. For all interconnections (point 5) to determine the limits and conditions from the point of view of their material composition, method of execution (loose, tight, or complex), methods of interconnection (welds, screws, rivets, seals, etc.) and the realization of possible other risks (internal fire or explosion, human factor and external risks).
7. For the risk sources (point 3) to determine impacts scenarios of partial risks for all interconnections and integrated risk for whole made up from jointed components; when the partial risks and integrated risk of whole made up from jointed components are not acceptable, it is necessary to increase requirements on material and construction of components interconnections so that these risks may be acceptable.

8. For the risk sources (point 3) to determine for the entire production process the process impact scenarios showing the integrated risk manifestation. In the case that the integrated risk is not acceptable, to increase the demands on design of: components of production process; working regime; and operators, so that the risks may be acceptable.
9. For the risk sources (point 3) to determine integral risk. If the risk is only conditionally acceptable (ALARP), then make modifications to the technology that will allow an immediate quality response that will ensure a return to normal state. In case of unacceptable risk, it is necessary to return to the adjustment of partial risks of components, systems and their interconnection (planned and even those that arise in the realization of sources of major risks) and the introduction of the principle of fail safely.
10. Considering the risk sources (point 3) to specify requirements for the steering system, that is for both, the I&C and the operators under normal, abnormal and critical conditions.

The above procedure of generation of SCPS risk-based design was tested with success at seven medium SCPS [25,37].

7 Conclusion

The quality of SCPS design predetermines its safety throughout the operation. Examples from practice show that some errors, such as underestimation of foundation conditions or some errors in terms of references, cannot be removed after the construction completion and commissioning. They pose a danger under certain conditions (e.g. at flood or earthquake) and can only be mitigated by organizational measures that entail additional costs and do not have the ability to ensure safety level as correct measures at design stage [13,14,25].

The above-summarized knowledge and results of study of SCPS accidents and failures show that basis for ensuring the facilities safety at required life cycle is knowledge of: regulations (legislation, norms, standards) in context; risks in the site to which the technical facility is placed; technical system, which constitutes a technical facility; models and theories associated with accidents; methods of analysis, management and settlement of risks; and way of management that operator might use after commissioning (finance, human resources, organization, technology, innovation...).

Furthermore, it is necessary for all those involved to respect the public interest, to participate in building the safety culture and for managers to motivate employees to do quality work, even by their own example, as shown by the so-called "golden rules of safety" [29]. The grounds need to be inserted into the design.

An analysis of environmental development as well as development of political, social and economic situation in the world shows the need to be prepared for the resolution of cases and actions that will cause critical situations with impacts intensities higher than these today. In order to manage realization of risks which are inherent in present world using the adequate forces, resources and means, it should be had: principles for managing the emergencies and critical situations, especially those of a large range; allocation of resources; and allocation of responsibilities. The risk management plan is tool that gives overview on measures, the person who execute them and the responsible person for execution.

Since the design of a SCPS is complex, the Process Safety Management (PSM) should be required for rational management of each process and for complete management is required the Safety Management System (SMS) [13,16,29] for rational management of each process. For practice, twelve methodologies for public administration are presented at work [33].Most of these methodologies can also be used for SCPS in the event of external risk sources. For internal sources of risk, specific investigations should always be carried out or procedures should always be applied to analogue SCPS where the conditions for technology transfer are met [38].

The results of the study [12,36,37] show that designer´ competences are very important for: the application of the results of methods of risk analysis and evaluation; implementation of the methodology for analysing and assessing the risks adapted to the problem; emergency and crisis management; analysis of situations / activities / accidents; the transformation of policy into a real action; the conversion of accident statistics into action plans; strategic planning; hierarchy of problems; finding the right information and learning; critical analysis; designing the right solutions; communication; carrying out synthesis and adapting the wording intended for the public; and ethics.

At each decision in favour of safety it should be remembered: all factors and processes that can be dangerous and how often they can occur; how large their impacts can be; how the size of the impacts or frequency of occurrence can be reduced; whether the proposed measures cannot be a source of new hazards; and which technical and control systems can be controlled by hazards that cannot be prevented.

Finally, it should be noted that, in line with the results at work [14], it is essential what is the political will to create a system to protect against unacceptable impacts of harmful phenomena, i.e. natural and other

disasters. An analysis of environmental development as well as the development of the political, social and economic situation in the world shows the need to prepare for the resolution of cases and actions that will cause critical situations by the intensity of impacts, and these are phenomena that do not today have such cruelty (severity) in the followed territory. Therefore, in terms of human security, the development of the human system, the existence, stability and development of the State, the concept of human safety and the subsequent concept of development must be codified and implemented through the management of safety into practice. In order to manage the realization of the risks, which are inherent in the present world using adequate forces, resources and means, it should be had: management principles for managing emergencies and critical situations, especially those of a large range; allocation of resources; and allocation of responsibilities.

The research showed that:

- each SCPS design has a certain danger. The designer art is to select such solution that is optimal, i.e. it is sufficiently safe and it is possible to realize with regard to investor and public administration options. The near the same holds for manufacturer´ skill (craftsmanship) at realization,
- impressive and low robust designs with insufficient safety margins often fail sooner or later,
- wrongly determined limits and conditions for critical technical facility parts lead to frequent disturbances up to serious accidents; they are not able to react to condition changes.

The analysis of accessible legislations [25] revealed that rules in force do not require to follow operation process safety in designing, and this occasionally leads to problems at operation, which is revealed e.g. in [19]. Based on authors´ experiences from practice [25,37], they compiled procedure for generation of SCPS risk-based design. There is continued the procedure implementation in practice and its improvement.

Acknowledgement: Authors thank for the EU grant; project RIRIZIBE-CZ.02.2.69/0.0/0.0/16-018/00026 49.

References

[1] ALE, B., I. PAPAZOGLOU and E. ZIO, *Reliability, Risk and Safety*. London: Taylor & Francis Group 2010, 2448p.

[2] BEER, M. and E. ZIO, *Proceedings of the 29th European Safety and Reliability Conference.* Singapore: ESRA 2019, e:enquiries@ rpsonline. com.sg

[3] BÉRENGUER, C., A. GRALL and C. GUEDES SOARES, *Advances in Safety, Reliability and Risk Management*. London: Taylor & Francis Group 2011, 3035p.

[4] BRIŠ, R., C. GUEDES SOARES and S. MARTORELL, *Reliability, Risk and Safety. Theory and Applications.* London: CRC Press 2009, 2362p.

[5] CEPIN, M. and R. BRIS, *Safety and Reliability – Theory and Applications.* London: Taylor & Francis Group 2017, 3627p.

[6] HAUGEN, S., J. VINNEM, A. BARROS, T. KONGSVIK and A. VAN GULIJK, *Safe Societies in a Changing World.* London: Taylor & Francis Group 2018, 3234p.; https://www.ntnu. edu/esrel2018.

[7] IAPSAM, *Probabilistic Safety Assessment and Management Conference.* Helsinki: IPSAM & ESRA 2012, 6889p.

[8] NOWAKOWSKI, T., M. MLYŇCZAK, A. JODEJKO-PIETRUCZUK and S. WERBIŃS- KA-WOJCIECHOWSKA, Safety *and Reliability: Methodology and Application*. London: Taylor & Francis Group 2014, 2453p.

[9] PODOFILLINI, L., B. SUDRET, B. STOJADINOVIC, E. ZIO and W. KRÖGER, S*afety and Reliability of Complex Engineered systems: ESREL 2015*. London: CRC press 2015, 4560p.

[10] STEENBERGEN, R., P. VAN GELDER, S. MIRAGLIA and A. TON VROUWENVEL- DER, *Safety Reliability and Risk Analysis: Beyond the Horizon*. London: Taylor & Francis Group 2013, 3387p.

[11] WALLS, L., M. REVIE and T. BEDFORD, *Risk, Reliability and Safety: Innovating Theory and Practice: Proceedings of ESREL 2016*. London: CRC Press 2016, 2942p.

[12] PROCHAZKOVA, D., J. PROCHAZKA, J. LUKAVSKY, V. BERAN and V.

SINDLERO-VA, Management of Risks of Processes Connected with Manufacturing and Commissioning Technical Facility. Praha: ČVUT 2019, 207p. http://hdl.handle.net/ 10467/84466

[13] PROCHAZKOVA, D., *Safety of Complex Technological Facilities.* ISBN 978-3-659-74632-1. Saarbruecken: Lambert Academic Publishing 2015, 244p.

[14] PROCHAZKOVA, D., *Principles of Management of Risks of Complex Technological Facilities* (in Czech). ISBN 978-80-01-06180-0, e-ISBN 978-80-01-06182-4. Praha: ČVUT 2017, 364p. http://hdl.handle.net/ 10467/72582

[15] PROCHÁZKOVÁ, D., *Critical Infrastructure Safety* (in Czech). ISBN 978-80-01-05103-0. Praha: ČVUT 2012, 318 p.

[16] PROCHÁZKOVÁ, D., *Principles of Management of Critical Infrastructure Safety* (in Czech). ISBN 978-80-01-05245-7. ČVUT, Praha 2013, 223 p.

[17] PROCHAZKOVA, D., *Challenges Connected with Critical Infrastructure Safety.* ISBN: 978-3-659-54930-4. Saarbruecken: Lambert Academic Publishing 2014, 218p.

[18] PROCHÁZKOVÁ, D., *Risks Connected with Disasters and Engineering Ways of Their Management.* ISBN 978-80-01-05479-6. Praha: ČVUT 2014, 234 p.

[19] PROCHÁZKOVÁ, D., PROCHÁZKA, LUKAVSKÝ, J., DOSTÁL, V., PROCHÁZKA, Z., OUHRABKA, L., *Management of Risks of Processes Connected with Technical Facilities Operation during Life Cycle*. ISBN 978-80-01-06675-1. Praha: ČVUT, 465 p. http://hdl.handle.net/10467/85867 doi:10.14311/BK.9788001066751

[20] PROCHAZKOVA, D., *Analysis and Coping with Risks Connected with Technical Facilities*. Praha: CVUT 2018, 222p. http://hdl. handle.net/10467/78442

[21] FEMA, *Guide for All-Hazard Emergency Operations Planning*. State and Local Guide (SLG) 101. Washington: FEMA 1996.

[22] RAUSAND, M., *Reliability of Safety-Critical Systems: Theory and Applications*. John Wiley & Sons 2014.

[23] EPSTEIN, W., Not Losing to the Rain: What I Learned when I Learned about Onagawa. In: *Safety and Reliability of Complex Systems*. London: Taylor &Francis Group 2015, pp. 365-371.

[24] REASON, J., *Human Error*. Cambridge: University Press 1990.

[25] CVUT, *Database on World Disasters, Technical Entities Accidents and Failures – Causes, Impacts and Lessons Learned.* Praha: CVUT 2020.

[26] EU, *Council Directive 82/501/EEC of 24 June 1982 on the Major-Accident Hazards of Certain Industrial Activities*. Brussels: EU 1982.

[27] IAEA, *Safety Guides and Technical Documents*. Vienna: IAEA 1954–2020. www.ns.iaea.org/ standards

[28] COMAH, *Safety Report Assessment Manual: COMAH*. London: UK – HID CD2 London 2002, 570 p.

[29] OECD, *Guidance on Safety Performance Indicators. Guidance for Industry, Public Authorities and Communities for developing SPI Programmes related to Chemical Accident Prevention, Preparedness and Response*. Paris: OECD 2002, 191p.

[30] HEIKKILÄ, A., M. *Inherent Safety in Process Plant Design. An Index-Based Approach*. Helsinki: VIT 1999, 132 p.

[31] KLETZ, T., *Process Plants: A Handbook for Inherently Safer Design* CRC. London: Taylor &Francis Group 1998.

[32] INSAG, Defence in Depth in Nuclear Safety. *INSAG-10*. Vienna: IAEA 1996.

[33] PROCHAZKOVA, D., *Methods, Tools and Techniques for Risk Engineering*. Praha: CVUT 2011, 369p.

[34] ZAIRI, M., *Total Quality Management for Engineers.* Cambridge: Woodhead Publishing Ltd. 1991.

[35] ISO, *Risk Management – Principles and Guidelines.* ISO 31000:2009.

[36] PROCHAZKOVA, D., PROCHAZKA, J., *Risk Management at Technical Facilities Designing, Building and Commissioning.* ISBN 978-80-01-06716-1. Praha: ČVUT 2020. dspace.cvut.cz . http://hdl.handle.net/10467/87491,

https://doi.org/10.14311/BK.9788001067161

[37] PROCHAZKOVA, D., PROCHAZKA, J., Tool for risk reduction at specific component aircraft engine welding. *Proceedings of International European Safety and Reliability Conference, ESREL2018*. ISBN 978-0-8153-8682-7. London: Taylor & Francis Group 2018, pp. 3135-3142; https: //www.ntnu. edu/esrel2018

[38] PROCHÁZKOVÁ, D., Examination of Core of Complaints and Conflicts Concerning Technical Solutions (in Czech). *Kontrola MSK ČR 1992*. MSK ČR Praha, 95p.