Application of STAMP to Improve the Evaluation of Safety Management Systems

Robert J. de Boer, Raymon van der Maarel

Aviation Academy
Amsterdam University of Applied Science
Weesperzijde 190, 1097DZ, Amsterdam
The Netherlands
rj.de.boer@hva.nl
Raymon.van.der.Maarel@hva.nl

1 Background

Although Aviation safety is continuously improving and has reached an all-time low in 2013 [FM 14], [ICAO 13], further efforts are still required to maintain absolute safety levels in periods of growth, and to improve safety levels in those niches of the air transportation system that have poor safety performance. One development to support continuous improvements in safety is the compulsory implementation of Safety Management Systems (SMS) [ICAO 13b], [CAA 14]. The adoption of Safety Management Systems to warrant aviation safety differs significantly from conventional safety assurance. Safety Management Systems acknowledge that any human endeavour cannot be completely free of hazards and risks, including those due to human activities and errors. An appropriate balance needs to be maintained between production and protection (cf. [H 14]). Safety is an "emergent", dynamic property of the complex, open aviation system so that safety risks needs to be continuously assessed and mitigated. The objective of the SMS is to maintain safety risks "under an appropriate level of control" [ICAO 13b]. In contrast, conventional safety assurance focuses on compliance to rules.

The change from a compliancy-based to a risk-based safety management requires a modification in oversight from compliance oversight to performance oversight [W 13]. However, evaluation of safety performance is not enough: although improved safety performance is a stated objective, SMS allow companies to achieve "an acceptable level of safety while balancing the allocation of resources between production and protection" [ICAO 13b]. Companies will always have to comply with a minimum set of regulations, but company management has some leeway in deciding what they consider to be an acceptable level of safety and how they allocate resources to mitigate risks. Therefore, the oversight of SMS cannot be entirely based on objective or numerical safety performance. It is therefore interesting to investigate whether and how the European aviation regulatory system is coping with this new challenge. For instance, one development is the guidance material for the national regulatory authorities to assess the implementation of SMS at the company level. The Safety Management International Collaboration Group (SM-ICG, consisting of representatives from industry and regulatory authorities) has generated such

guidance for the oversight of SMS, in the form of an evaluation tool for SMS [SMICG 12].

STAMP is a relatively new hazard analysis method based on system thinking rather than on component thinking [L 11], [L 13]. It is based on the principle that the sum of the safety of each component of a system is not necessarily equal to the safety of the whole system. One will need to look for conflicting interactions or safety constraints among components in order to guarantee safety. In a system, components could be physical components as well as organisations or persons within organisations. Applying STAMP to management systems is even more unique and has barely done before (cf. [dB 14]). There is a need for more knowledge about this hazard analysis method and its practical application to supervisory socio-technical systems.

2. Purpose

To identify the value of applying STAMP to the European aviation regulatory system in identifying risks that have not previously been identified for the change from a compliancy-based to a performance-based oversight. The scope of the current study is limited to aviation maintenance as it is vulnerable for complex and inefficient regulatory systems since maintenance companies are relatively small. Besides, the decreasing number of aircraft crashes resulting in an increasing level of in-flight safety forces the industry to pay more attention to on-ground hazards [OSZ 13].

3. Approach

The current study has applied a modified five-step STPA methodology [L 13], [dB 14]: (1) Hazards and safety requirements; (2) Functional control structure; (3) Control actions; (4) Allocation of safety requirements to components; and (5) Control loop effectiveness. The results of the analysis is compared to the currently known hazards described in the most recent EASA annual report [EASA 12]: (1) Inadequate provision of resources in relation to existing and new tasks (extension of the remit) of the Agency; (2) Unaddressed safety issues at the time of certification, validation, approval of flight conditions resulting in a crash of an aircraft. (3) Unaddressed safety issues resulting in a catastrophic consequences due to non-issuance of an airworthiness directive or insufficient corrective actions, inadequate compliance time specified by an Airworthiness Directive; and (4) Inadequate occurrence reporting system and ineffective processing of occurrence reports discrediting continuing airworthiness of products and leading to preventable accidents or serious occurrences.

4. Results

The main goal of the European aviation regulatory hierarchy system applied to maintenance service providers is to create an environment in which legislation is drawn

up and reformed according to the latest knowledge, occurrences and developments; and this legislation is provided to the industry in such a way that aviation maintenance is carried out properly and timely in order to maintain or reduce the number of incidents, accidents and losses caused by technical failures. Taking into account this goal, a generic hazard has been established which conflicts with the aforementioned goal. The system-wide hazard is that maintenance is carried out in such a way that the aircraft does not function as intended and crashes or causes economic or environmental impact as a result of at least one technical failure. This system-wide hazard can be split up in more specific and better understandable hazards, which apply to different areas of the system. These hazards are: (1) Regulations are not prescribed resulting in unsafe operations of maintenance organisations on its turn resulting in incidents or accidents; (2) Maintenance organisations do not comply with prescribed regulations resulting in unsafe operations of maintenance organisations on its turn resulting in incidents or accidents; (3) Risks, other than the risks mitigated by prescribing regulations, are not identified and thus not mitigated resulting in unsafe operations of maintenance organisations on its turn resulting in incidents or accidents; and (4) Feedback on the functioning of the regulatory system is not provided resulting in a not completely effective regulatory system in terms of preventing the three aforementioned hazards from happening resulting in unsafe operations of maintenance organisations on its turn resulting in incidents or accidents. Each of these is hazards is translated into constraints iteratively in discussions with EASA, see Van der Maarel [vdM 14] for a full account.

Figure 1: Control structure for the European aviation maintenance regulatory system

In the European aviation maintenance regulatory hierarchy, organisations are involved which (1) carry out maintenance and have to comply with the prescribed regulations, (2) national authorities which enforce regulations to maintenance organisations and audit compliancy and (3) European authorities which draw and adapt regulations and enforce them to Member States. The control structure for the European aviation maintenance regulatory system is shown in Figure 1.

Susequently, it is established what control actions exist in the control structure. This is based on Part-M and Part-145 regulations together with documents from several European Institutions. The first constraint is: 'Risk control in the form of regulations shall be in place at any level'. This constraint can be translated basally into the control action 'command to make, enforce or comply with the regulations'. The second constraint is: 'A system which properly oversees and enforces regulations shall be in place'. This constraint can be translated basally into the control action 'command to provide information related to auditing compliance or to perform audits to check compliance of organisations'. The second constraint is: 'A system which properly oversees and enforces regulations shall be in place'. This constraint can be translated basally into the control action 'command to provide information related to auditing compliance or to perform audits to check compliance of organisations'. The fourth constraint is: 'Feedback on the functioning of the system shall be provided'. This constraint can be translated basally into the control action 'command to provide feedback related to the functioning of the system or other relevant input'.

5 Conclusion

Three potential hazards have been identified in the capability of the regulatory hierarchy to evaluate the SMS effectiveness. EASA has no appropriate powers to directly address national aviation authorities. The EASA can either provide guidance material or they have to issue through the Commission which is seen as a heavy and time-consuming measure. Furthermore the Commission has political interests and opinions which could influence the decision-making process, whereas EASA has the most knowledge in the aviation regulatory work field and is politically neutral.

There is no proper risk-management capability assessment tool. Now, competent authorities mainly have to audit compliancy which is considered as a 'black and white' process. After the implementation of SMS, authorities will be required to audit risk-management competences of the maintenance service provider, which is harder and more time-consuming to do. Ongoing discussion is expected about the acceptable level of risk and an acceptable level of safety with the introduction of Safety Management Systems. It is not defined neither measurable what exactly is considered as an acceptable level of safety or as an acceptable level of risk.

Due to the financial crisis, governments have less leeway in their budgets. Whereas previously a compromise between safety and economics was never been made in the disadvantage of safety, now we see more well-considered and tight allocation of (financial) resources. The law prescribes the government to designate a competent authority and provide it with sufficient resources, which is a subjective requirement. Taking into account that SMS are required to be implemented in various kinds of aviation organizations, which in turn requires more work for the competent authority in initial approval and oversight, this leads to a potential hazard.

These findings are quite different to the currently known hazards described in the most recent EASA annual report [EASA 12]. We conclude that the STAMP analysis is a useful

addition to contemporary safety analysis tools, and look forward to further studies to identify its strengths and weaknesses. In particular, we expect to be able to study its value in comparison to currently available guidance material for the national regulatory authorities to assess the implementation of SMS at the company level [SMICG 12].

References

[CAA 14] CAA-UK, "SMS Implementation Dates," 2012. [Online]. Available: https://www.caa.co.uk/default.aspx?pageid=11558. [Accessed: 22-Apr-2014].

[dB 14] R. J. de Boer, "Using STAMP to Predict Safety: Application at a Ground Service Provider," Saf. Sci., accepted, 2014.

[EASA 12] EASA, "Annual Report 2012," Cologne, Germany, 2012.

[FM 14] D. Fouda and I. Maragakis, "Significant improvements for Global Aviation Safety in 2013." EASA, Cologne, Germany, 2014.

[ICAO 13] International Civil Aviation Organization, "Safety Report," Montreal, 2013.

[ICAO 13b] International Civil Aviation Organization, "Safety Management Manual (SMM)," Montreal, 2013.

[H 14] E. Hollnagel, "The ETTO principle as ETTOing – or Occam ' s Razor redux," 2012.

[L 11] N. G. Leveson, Engineering a safer world: Systems thinking applied to safety. Cambridge, MA: MIT Press, 2011.

[L 13] N. G. Leveson, "An STPA Primer," Cambridge, MA, 2013.

[vdM 14] R. van der Maarel, "Using STAMP to Analyse the Effectiveness of the European Regulatory System," Amsterdam University of Applied Sciences, 2014.

[OSZ 13] C. V. J. Oster, J. S. Strong, and C. K. Zorn, "Analyzing aviation safety: Problems, challenges, opportunities," Res. Transp. Econ., vol. 43, pp. 148–164, 2013. [SMICG 12] Safety Management International Collaboration Group, "Evaluation Tool," Cologne, Germany, 2012.

[W 13] C. Wassink, "The Netherlands - Implementation SSP & SMS."