Application of STAMP to Facilitate Interventions to Improve Platform Safety

How to apply the STAMP framework to safety management

Robert J. de Boer, Scott de Jong
Aviation Academy
Amsterdam University of Applied Sciences
The Netherlands
rj.de.boer@hva.nl

***Abstract*—This study aims to predict the relation between safety management and safety performance for a Ground Service Provider using the STAMP framework, to enhance its safety performance, and to adapt the STAMP framework if and where necessary. Airplane turn-around activities on the airport platform contribute disproportionally to a lack of safety in aviation, and these activities turn out to be difficult to improve. The STAMP framework applies complex system thinking and may therefore be suitable to identify lapses in safety management that are a cause for a lack of safety. This paper reports on a longitudinal single case study approach at a Ground Service Provider that investigates the use of STAMP to assess safety management and correlate this with safety performance. The results show that the STAMP framework, suitably modified, is a useful evaluation tool for safety management, and that its assessment correlates with safety performance.**

Keywords: platform safety, safety management system, STAMP,, Line Observation Safety Audits

I. Introduction

Although Aviation safety is continuously improving and has reached an all time low in 2013 [1], 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 such area where safety records are less than average is platform operations [2]. Platform activities account for more than a quarter of aviation incidents [3]. These incidents lead to aircraft damage and associated costs, risk of injuries, and can potentially impact in-flight safety.

Platform safety is a difficult issue to address. Platform staff generally work in a hostile environment and it is difficult for supervisors to monitor task execution due to the geographic spread. The work requires limited qualifications and is less well paid than other jobs within aviation, yet the pressures to achieve a quick turn-around can be high. Platform service providers experience fierce competition that is aggravated by the economic crisis, and job security is limited. Temporary workers generally constitute a large fraction of the labor force. Oversight of platform operations by regulatory authorities is not as strictly regulated as other aviation activities, and achieved though aircraft operator and/or aerodrome operators.

In an effort to improve platform safety and curb incidents, a Ground Service Provider at a major European airport has recently implemented Line Operations Safety Assessments for platform operations (ramp-LOSA) [4], [5]. This approach has been effective in identifying the level of adherence to safety regulations. Some regulations (e.g. speed limits) are consistently trespassed in over 80% of the observations. On average, over 30% of the regulations in force are not complied with at each turn-around. Naturally, the results of the LOSA observations are being reported back to senior management of the Ground Service Provider. There was an initial shock at the severity of the numbers, and a realization that this mirrored their unease about platform safety. However, contradictory to what was expected, a very limited improvement in safety performance has been realized over the last twelve months despite the magnitude of the infringements. This stagnation in the improvement of platform safety inspired the search for a methodology that would identify the flaws in the management of safety at this and other Ground Safety Providers.

The traditional safety enhancement tools are limited in their effectiveness within this challenging domain. Safety culture surveys may identify areas of weakness but have limited diagnostic capability, and the correlation between safety culture factors and safety performance "still awaits a fundamental scientific underpinning" [6]–[8]. Efforts to improve safety culture on the platform are at odds with the lack of supervision, lower qualification levels of employees, and the lack of job security. Hale [9], [10] suggests that both a top-down and bottom-up coordination is required to ensure the application and optimization of rules, and enable their enforcement. Increasingly, a systemic approach to safety is being advocated to identify safety risks that are a result of the interaction between components of the system under scrutiny rather than the failure of individual components [11], [12]. One such methodology is the STAMP framework [13], [14], that has been applied successfully to identify system safety hazards [15]–[19]. Organizational aspects have been included in each of these studies, illustrating its effectiveness in identifying safety management flaws in each specific instance. However, as yet the studies have not generated a generic prediction or theory on the relation between safety management and safety performance even though this is highly desirable [20], probably because the method is quite demanding and requires prior experience [14]. In particular the identification of the causes for unsafe control is challenging, requiring input from several domain experts.

The STAMP method is appealing because it is based on control theory using feedback. In control theory, the purpose of the feedback loop is to maintain the output close to the set point under dynamic conditions [21]. An effective feedback loop will manage a change in the set point, dampen short-term distortions (noise), and will counter a change of the controlled process such as a gradual degradation or drift of the organizational defenses over time [22]. A system with feedback is essentially resilient to internal or external distortions, which mirrors the aim of safety management.

The first aim of this study is to develop a prediction or theory on the relation between safety management and safety performance for a Ground Service Provider using the STAMP framework. The second aim is to use this prediction for a specific Ground Service Provider to enhance its safety performance. The third aim is to adapt the STAMP framework if and where necessary to support the diagnostic capabilities of the framework.

II. Description of the Framework

The STAMP framework describes socio-technical systems, in which safety constraints, if adequately enforced, eliminate one or more hazards [13]. A hazard is defined as “a system state or set of conditions that together with a worst-case set of environmental conditions, will lead to an accident (loss)” [14]. The safety constraints are enforced through control loops.

A. Control loop components

The generic components of a control loop are discussed below. The supervisory control system may comprise multiple hierarchical loops. The controlled process of any loop constitutes the controller for a subordinate loop.

The *controlled process* is the process that is under supervision. In the example of ground services, this is the process of positioning, unloading, cleaning, loading and pushing back aircraft. The controlled process has inputs (arriving aircraft, baggage and passengers to be loaded, information, etc.) and outputs (departing aircraft, unloaded baggage and passengers, information, etc.).

It is the aim of the socio-technical system to maintain control over this process, i.e. to keep the output within specified margins of the *set point* despite varying inputs and process conditions. In ground service safety, the set point will be determined by an explicit or implicit safety target from higher management levels. For a given system there is (or should be) only one set point, even in case of multiple hierarchical control loops. A system cannot thrive for multiple values of the same parameter simultaneously.

The *sensors* generate data on the output performance of the controlled process and deliver this in meaningful form to the controller. In technological process control, this will include temperature, flow, etc. sensors. In a human supervisory loop as in Ground Services, sensors are less evident. The sensors in this context include management reporting systems, the ears and eyes of supervisors walking the floor, audits and such. After the implementation of LOSA at a Ground Services Provider, this can become the main source of safety performance data.

The *controller* is the entity that is tasked with supervisory control of the controlled process. In technological control loops this may be an automated system. In case of a human-dominated controlled process as in ground services it is difficult to envisage that this could be anything but a human controller, i.e. the supervisor at the next hierarchical level. The controller – to be able to fulfill the control task – requires at least a model of the controlled process (the *process model)* and a *control algorithm*. The process model is required to interpret the output performance data from the sensors into a representation of the current state of the process. In the example of ground services, the supervisor might conclude based on his process model that a particular infringement of procedures is caused by a lack of training rather than production pressure.

The control algorithm generates control signals based on the gap between the current process state and the set point. In this example, the supervisor may decide to increase the off-site training effort (effectively increasing production pressure on the remaining workers). Both the process model and the control algorithm need to be recalibrated periodically to maintain consistency with the controlled process [14, p. 19].

Actuators translate the control signals into interventions at the process level. In technological process control this will include physical actuators, valves opening or closing, etc. In a human supervisory loop as in ground services, actuators are less evident. The actuators in this context include e-mails, face-to-face instructions, schedule interventions, etc.

B. Unsafe control actions and flaws

An important foundation of the STAMP framework is the identification of unsafe control actions and flaws in the control loop. Leveson [14] identifies five types of *unsafe control actions*: (1) An unsafe control action is provided that creates a hazard; (2) a required control action is not provided to avoid a hazard; (3) a potentially safe control action is provided too late, too early, or in the wrong order; (4) a continuous safe control action is provided too long or is stopped too soon; and (5) a control action required to enforce a safety constraint is provided but not followed. In the context of ground services, it can be easily understood that for instance not providing a safety training, prematurely discontinuing supervision of novice employees or giving inappropriate instructions will constitute unsafe control actions.

Unsafe control actions arise from *flaws* in the control loop. A multitude of possible flaws have been identified in the literature, both from theory and in the actual application of STAMP to incidents. In our intended use of STAMP as a diagnostic tool, the systematic categorization of flaws serves as a basis for the methodical identification of organizational strengths and weaknesses. Flaws can occur in each of the components discussed earlier. Flaws in the sensor (labeled A for use in the results section) are defined as any cause that leads to a lack of correct, complete and timely information at the controller. This includes missing feedback, delays in feedback, measurement inaccuracies etc. Flaws in the process model (B) are defined as any cause that leads to a lack of a correct, complete and timely representation of the current state of the process, assuming the correct, complete and timely input of feedback information at the controller. This includes wrong interpretations of the feedback, delays in interpretation, etc. Flaws in the set point (C) are defined as any cause that leads to a lack of correct, complete and timely target values for the output, including specified margins. This may include lack of management direction, or contradictory targets. Flaws in the control algorithm (D) are defined as any cause that leads to a lack of correct, complete and timely generation of control signals based on the gap between the current process state and the set point (assuming both are available and correct). This includes the generation of insufficient, too severe or untimely control signals, etc. Flaws in the actuators (E) are defined as any cause that leads to a lack of correct, complete and timely control signals at the controlled process (assuming that the control signals have been generated correctly). This includes missing or distorted control signals, delays in control etc. Unsafe control actions can also arise from large and unforeseen disruptions in the controlled process (F), including unforeseen conflicting control inputs from other controllers. These may offset the controlled process so far outside the specified margins that the control loop is not able to regain the set point within a reasonable time. By definition these disruptions have not been taken into account in the design and implementation of the control loop, either because they were not recognized, or because they were considered sufficiently improbable to be ignored. Examples are excessive disturbances like extremely bad weather, a great number of missing or malfunctioning resources, and conflicting control actions from other controllers for which no procedures or work instructions are in place. A control flaw that has been added to the original STAMP documentation is cognitive resistance (G): the capacity of humans to endure salient stimuli that are contradictory to the current mental model [23], marking a hesitation to switch from automaticity to effortful thinking even when this is "appropriate" for the current situation [24], [25].

C. *Control Actions*

The control actions that can be attributed in a safety management loop are necessarily generic rather than specific. Six generic management activities have previously been identified [26]–[28] that are congruent with normal system behavior and the emergent characteristics of safety [11]: (1) set goals and direction; (2) establish work processes and standards; (3) staff, schedule and train; (4) manage facility and equipment; (5) allocate financial resources; and (6) monitor and evaluate performance. These activities are suggested to form the repertoire with which the safety constraints can be enforced.

Note that each of these activities require a complete and effective control loop. For instance, staff allocation cannot be effective if feedback from the controlled process is not heeded to identify any gaps between the plan and reality, and to modify the staffing plan accordingly. Similarly, the monitoring and evaluation of performance not only requires feedback from the controlled process, but may also entail the application of control signals to prepare the workforce for the evaluation, or instill them to contribute to the monitoring of performance. Therefore, although these activities are associated with management by name and convention, in fact within the STAMP framework they are sets of tasks throughout the control loops that are necessary for the enforcement of the safety constraints. As an example related to ground services: the habit to violate the speed limit could be due to a lack of direction, unclear procedures, insufficient training, vehicles not equipped with a speed limiter, no financial consequences for the violation, too little oversight, or a combination of the above.

To enforce the safety constraints at the Ground Service Provider, the controllers at each hierarchical level will need to ensure that each of the management activities have been defined, are adequately divided into tasks for each control loop component, and are properly executed. In our implementation of STAMP, the division of tasks over the elements allows us to make a more detailed diagnosis of the organization's strength and weaknesses.

III. METHOD

This study is conducted using the STPA methodology described by Leveson [13], [14], [19] applied to a Ground Services Provider. The method is described first, followed by the application of the methodology to the case. Two moments in time have been chosen to apply the methodology to the company: a retrospective study of the situation at the Ground Service Provider in the period up to 2011, and a study of the current situation at the Ground Service Provider.

A. *Risk analysis using STPA and the STAMP framework*

The methodology to apply the STAMP framework to identify system safety risks has developed over time. The most recent description dates from 2013 [14]. In this study we apply this methodology, using the following breakdown: (1) Hazards and safety requirements (encompassing from the guide the establishment of the system engineering foundation for the analysis and for the system development, scoping of relevant losses, identifying the hazards associated with these, and specifying the safety requirements / constraints); (2) Functional control structure (encompassing the description of the control structure for the system under consideration part of the system engineering foundation); (3) Control actions (in which we identify all relevant control actions, not just those that are unsafe); (4) Allocation of safety requirements to components (mirroring the identification of unsafe control actions to create safety requirements and constraints); and (5) Control loop effectiveness (in which we determine how each potentially hazardous control action could occur).

B. Case study

A longitudinal single case study approach was chosen for the current research to test for a relation between control loop effectiveness and safety performance [29]. Qualitative data was collected for two moments in time with differing safety performance and control loops: the situation at the Ground Service Provider in the period up to 2011, and the current situation. Control loop effectiveness is determined by the efficacy of each of the components of the control loop and the information flows between them across the six management tasks. Safety performance is determined by to the number of incidents leading to airplane damage and/or employee injury, operational errors that damage the company's reputation, and significant customer audit findings. The data for the case study was derived from semi-structured interviews, and the experience of the junior researcher as a platform employee of the Ground Service Provider. The interviewees were the Platform Supervisor (first interview), and the Quality & Safety Manager and Officer (second interview, together). Each interview lasted over two hours and was organized around the control structure that was drawn up in preparation. The interview results and the hands-on experiences were used to fill a matrix of control loop components versus control actions (see the results section for details).

IV. RESULTS

A. Retrospective Analysis (2011)

The first analysis is a retrospective study of the situation at the Ground Service Provider in the period up to 2011.

1) Hazards and safety requirements

In our application of STAMP at a Ground Service Provider, the System Engineering Foundation for the current case has been developed previously through our earlier work to implement Line Observation Safety Audits (LOSA) [4], [5]. The regulatory baseline against which platform performance is assessed is an extensive rule base, consisting of the original LOSA suggested regulations, all the company operational regulations, the aerodrome regulations, and the airline requirements for the airplane being serviced. Each of these can be considered a safety constraint, violation of which creates an aviation safety hazard and/or an occupational health hazard. Note that in contrast to traditional STAMP applications [13], [14], [19], in this specific case we have not taken the effort to write out the specific hazards – we assume for the purpose of this study that an appropriate hazard analysis underlies the set of regulation. We will elaborate on this in the discussion section.

2) Functional control structure

The initial control structure for the ground services provider is shown in Figure 1. The controlled process is the aircraft turn-around process, including the disembarkation of passengers, offloading of baggage, fueling and cleaning, restocking supplies, loading baggage and passengers. The process is executed by platform employees working a two shift system. Two separate groups can be identified: a number of experienced, less well educated employees and a group of students who work on the platform besides their day study at one of the local universities.

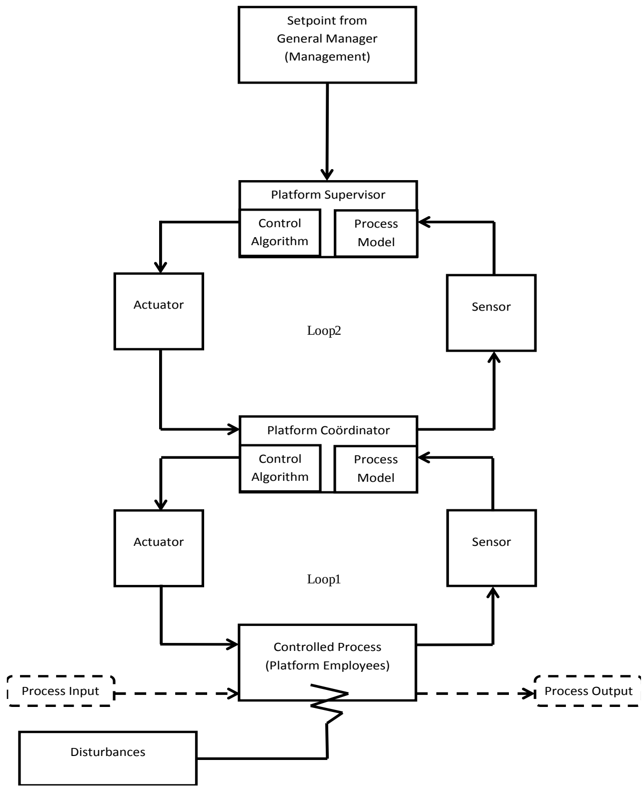

Figure 1: Retrospective (2011) Functional Control Structure for the Ground Services Provider

The procedures to be applied in the execution of the turn-around have been documented and trained, and are clear to all employees. The process is robust against most common disturbances such as bad weather, aircraft delays and sudden incapacitation of individual resources. Back-up arrangements have been made with the airport authorities in case of difficulty. For instance, the number of turn-around bays is geographically limited, so it is expected that process execution will remain in control even in case of a large number of aircraft diverging to the airport. Information about the performance and execution of this process flows to the platform coordinator and the platform supervisor by the internal reporting system, email, and face to face. Separately on-time performance and delays are communicated by an internal system. The platform coordinators are not hierarchically responsible for the platform employees, and do not take on a supervisory role. Their main task is to assign employees to arriving aircraft and coordinate in case of resource problems or delays. They work the same shifts as the platform employees. Other than that required for these responsibilities, they do not endeavor to control the execution of the turn-around process. The platform supervisor on the other hand is considered to be the hierarchical next in line for the platform employees. However, the supervisor has other responsibilities unrelated to the platform and is off-site for several days each week. The supervisor platform generally communicates to the platform coordinators and the platform employees through emails, and irregularly through stand-up meetings, and sometimes face to face. The supervisor reports to the General Manager of the ground handling division, and receives his management targets from him.

3) Control Actions

We verified that the six (management) control actions are required to effectively and safely execute the aircraft turn-around process. Goals are set for: on-time performance, maximum number of short-shipped / mishandled bags, maximum number of medium / heavy incidents, first bag and last bag target, kpi's, always safety first, and cost levels. Work processes and standards are set for: pre-flight, upon arrival, flight handling and departure. Work instruction for each action are available and accessible via the management system. Staff is divided into three categories. Scheduling of these is according to the demand of the three categories and the flight schedule. Facility and equipment is available to execute the process, as well as a back-up for all the equipment except the potable water service truck. Monitoring and Control is executed for on-time performance, short-shipped / mishandled bags, first-bag and last-bag times, and audits. Investigation are conducted when an irregularity has occurred. Little information was available about the management of financial resources.

4) Allocation of safety requirements to components

The initial safety constraints derived from the top level hazard (i.e. compliance with the platform regulations and rule base) has been allocated to the components of the control loop, as shown in Table 1.

Table 1: Allocation of requirements to components

Component	Allocated safety constraint
Controlled Process	Compliant execution of process
Sensor loop 1	Receival, transmission and presentation of compliancy of process to Platfom coordinator
Process Model loop 1	Platform coordinator can identify gap between current and target compliancy based on information
Control Algorithm loop 1	Platform coordinator can generate required control actions as a function of gap
Actuator loop 1	Receival, transmission and presentation of control signal at controlled process
Sensor loop 2	Receival, transmission and presentation of current state of platform coordinator to supervisor
Process Model loop 2	Supervisor can identify gap between current and target state of platform coordinator based on information
Control Algorithm loop 2	Platform supervisor can generate required control actions as a function of gap
Actuator loop 2	Receival, transmission and presentation of control signal at platform coordinator
Set Point	Implicit or explicit target state(s) for platform coordinator process and process compliancy available

5) Control loop effectiveness

The control actions have been analyzed for unsafe performance, using the flaw lettering indicated in section II. The results are detailed in Appendix 1: Control loop 1 effectiveness . In the analysis it quickly became clear that the Platform coordinator was not executing the safety management tasks as he did not see platform safety as his responsibility and therefore did not initiate interventions. The control loop is therefore not effectuated. (Loop 2 has also been analyzed but is not included in this paper as it is inconsequential for the conclusions of the study).

6) Safety performance

In 2010 the ground service provider experienced a number of incidents, which included two damages to customer aircraft requiring major repairs, a separation loss for Schengen (i.e. Euro-domestic passengers) and non-Schengen passengers, and a number of significant safety audit findings from a client airline.

B. Analysis of the current situation

The second analysis is a study of the current situation at the Ground Service Provider. As a result of the serious safety infringements in 2010, a quality and safety department was established, reporting directly to the Operations Director of the company.

1) Hazards and safety requirements

In comparison to the situation up to 2011, there are no changes regarding the hazards under consideration nor the safety requirements (constraints) to be specified.

2) Functional control structure

The current control structure for the ground services provider is shown in Figure 2Figure 1.

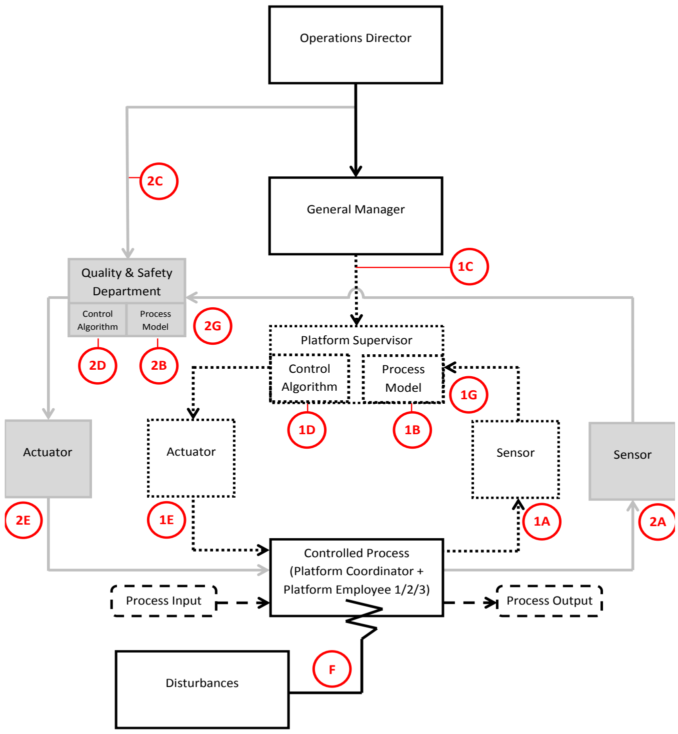

Figure 2: Current Functional Control Structure for the Ground Services Provider

The figure includes the newly created quality and safety department. For clarity the numbering of the flaws has been included in the figure. In comparison to the initial control loop, a new loop has been added in parallel to the original loops (shown in grey). The original, ineffective loops are shown with dotted lines. Loops 1 and 2 of the initial control structure have been combined to reflect the now non-hierarchical role of the platform coordinator. The Quality & Safety department consists of a manager and a number of officers, of which one has been assigned to the platform. Because of the small size of the department, the very direct reporting lines and the close relation between the manager and the officer, it has been assumed not to add value for the analysis to expand the department into a separate control loop. The Quality & Safety Manager has been promoted internally in this role after having gained line experience within the warehousing division of the company. The Quality & Safety officer for the platform has recently graduated from a local college but also has hands-on experience at the platform as a student worker. The platform employees report hierarchically to the platform supervisor as before. His availability is still limited. Information about the performance and execution of this process still flows through the internal reporting system as before. The Quality and Safety officer for the platform is also a recipient of this information.

3) *Control Actions*

For the current case this analysis did not differ from the retrospective case: the six (management) control actions are again required to effectively and safely execute the aircraft turn-around process.

4) *Allocation of safety requirements to components*

The initial safety constraints derived from the top level hazard (i.e. compliance with the platform regulation and rule base) have been allocated to the components of the control loop, similarly to what has been shown in Table 1 but not included in this paper for brevity.

5) *Control loop effectiveness*

The results for the identification of unsafe control actions are detailed in Appendix 2: Control loop 2 effectiveness – Current Situation. (Loop 1 is not included in this appendix as it is unchanged versus the initial situation). From the analysis it is apparent that control over safety management is vastly improved compared to the initial situation. Responsibilities for safety management have been assigned, and control actions are effectuated. However, because the Quality & Safety Department has been allocated a staff role, it does not hold all the executive rights it may require to achieve the safety standards.

6) *Safety performance*

Current safety performance is commendable, with high reporting rates of both risks and occurrences, and zero incidents with damage or injury. Audit reports are without significant findings.

C. *Comparison of results*

It follows from the analysis of the case study that in the retrospective case there were quite fundamental flaws in the control loop: the control loop for safety management was ineffective because the Platform coordinator was not executing any safety management tasks. At the same time safety performance was quite poor, as follows from the significant damages, audit findings and the passenger incident. Currently safety performance seems to be quite adequate., and the control loop is only marginally flawed. Therefore a qualitative relation between control loop effectiveness and safety performance has been identified for the current case study.

V. DISCUSSION & CONCLUSION

A. *Case study: Safety at the Griound Service Provider*

The case study of the Ground Service Provider demonstrates a qualitative relation between control loop effectiveness and safety performance, therefore lending credibility to the proposed causal relationship [13]. Furthermore, the results shown in appendix 1 indicate poor safety management across all six control actions. It was unfortunate for the company under investigation that it was only after several serious incidents that actions were taken to improve the situation. For the current situation the analysis has identified that safety management is predominantly assigned to the Quality & Safety Department. However, the Quality and Safety Manager and Officer have been allocated a staff role, and do not hold all the executive rights that may be required to achieve the safety standards. This risk has been acknowledged by the company and it is now planned to move the responsibility for safety management back into the hierarchical line.

B. *The STAMP framework*

The framework as applied in this research proved to be effective in determining control loop effectiveness. Although the original literature on the STAMP framework is specific about the identification of hazards [13], [14], the definition applied in this study proved sufficient for our purposes. We defined the safety constraints as compliance to the currently valid platform regulations. Any violation of the regulations is considered to create an aviation safety hazard and/or an occupational health hazard. This is justified by the effort that has been spent in defining the regulatory baseline [4]. The framework allows for the maintenance of the rule base under the (management) control actions of establishing work processes and standards, and monitoring and evaluating performance. An acceptable means to update the rule base is described by Hale and Borys [10], and can be assessed using the current methodology. Use of the functional control structures as depicted in Figure 1 and Figure 2 proved to be effective in identifying the components of the control loop and the information flows between them during the data collection stage. The tight definitions applied in the current study supported the identification and partitioning of the components of the control loop.

The application of the six (management) control actions that are required to manage safety proved useful. This study focused on normal system behavior rather than unwanted or hazardous behavior, congruent with the emergent characteristics of safety [11]. The six activities proved to form the repertoire with which the safety constraints can be enforced and were helpful in realizing a complete assessment.

The differentiation between the actions highlighted that the Quality & Safety Department at the Ground Services Provider in the current situation managed many, but not all of the safety management tasks. Of all the tasks, that of managing financial resources seemed the least relevant for the current case. Further research will whether this task is consistently superfluous for safety management, although at present this would seem surprising.

The allocation of the safety requirements and control actions to the components is necessary to define the blank Control loop effectiveness. Without such an allocation, the contribution of each components to control loop effectiveness is unclear. The use of the generic control loop flaws [13], [14], [19] was generally beneficial in identifying possible flaws. Further work is required to identify the value of the out-of-range disturbances and cognitive resistance. By definition out-of-range disturbances have not been taken into account by the designers and operators of the control loop, either because they were not recognized or because they were considered sufficiently improbable to be ignored. An evaluation of this control loop flaw requires somehow challenging the system design, and more guidance seems necessary. The cognitive resistance control flaw similarly requires the researcher to identify a failure in perception that is invisible to those participating in the control loop [23], and requires further work. Its value in the framework is that it allows for a functioning sensor and a satisfactory process model, yet a blockage in the control loop may still occur when there is a hesitation to switch from automaticity to effortful thinking [24], [25].

C. Methodology

The methodology to apply the STAMP framework has been described slightly differently in consecutive publications. Initially Leveson e.a. describe a seven step methodology in which the risks and vulnerabilities are identified of the new organizational structure for the NASA Independent Technical Authority, including the metrics and measures of effectiveness [19]. In the book "Engineering a Safer World" [13] the approach has been somewhat concentrated to a two step methodology, but many readers required additional assistance in the application of the methodology. This inspired the publication of a guide [14] in which the methodology has been further refined, and which formed the basis for the current undertaking. The modifications that we made to the methodology are in part due to the specific application to management, and in part a result of the effort to clarify the approach sufficiently for use by undergraduate students and practitioners. This will help to close the gap between research and practice [30]. Leveson suggests that the last step in the methodology (identifying causes of the unsafe control actions) "requires the most thought and prior experience by the analyst and there is, so far, much less help provided (…) It is also where information is generated to assist the designers in eliminating or mitigating the potential causes of the hazards". The methodology as applied in this research proved to be suitable to identify control loop effectiveness and may mitigate some of the difficulties associated with the original approach. The final product is the completed control loop effectiveness table. Besides its analytical value, this makes the results of the study comprehendible for company management, illustrating the diagnostic value of the methodology.

The longitudinal single case study approach [29] was effective in this study due to the significant change in circumstances between the two observations. Applications to a broader range of applications is required to corroborate the results of the current study.

D. A systemic approach to safety management

In this study we have taken a system approach to improving platform safety. In comparison with a more reductionist approach the emphasis in the current research was not on rule violations or those at the 'sharp end'[12]. Rather, the approach highlighted the interaction of system components at different hierarchical levels which results in safety performance as an emergent property of the system. The method is much more transparent than safety culture surveys, that may identify areas of weakness but have limited diagnostic capability and whose correlation with safety performance "still awaits a fundamental scientific underpinning" [6]–[8]. As such, the current study has shown the viability of a systemic approach. It is only to be hoped that the decomposition of the control loop into components inherent in the STAMP framework is not interpreted as a new form of reductionism.

References

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

[2] M. Verschoor and A. Young, "Willingness to report occurences in civil aviation in the Netherlands," the Hague, the Netherlands, 2011.

[3] A. D. Balk and J. W. Bossenbroek, "AIRCRAFT GROUND HANDLING AND HUMAN FACTORS (NLR-CR-2010-125)," Amsterdam, the Netherlands, 2010.

[4] R. J. de Boer, B. Koncak, R. Habekotté, and G.-J. van Hilten, "Introduction of ramp-LOSA at KLM Ground Services," in *Human Factors of Systems and Technology*, 2011.

[5] J. Ma, M. Pedigo, S. Louis, L. Blackwell, K. Gildea, K. Holcomb, and C. Hackworth, "The Line Operations Safety Audit Program : Transitioning From Flight Operations to Maintenance and Ramp Operations DOT/FAA/AM-11/15," Washington, DC, 2011.

[6] F. W. Guldenmund, "(Mis)understanding Safety Culture and Its Relationship to Safety Management.," *Risk Anal.*, vol. 30, no. 10, pp. 1466–80, Oct. 2010.

[7] A. R. Hale, F. W. Guldenmund, P. L. C. H. van Loenhout, and J. I. H. Oh, "Evaluating safety management and culture interventions to improve safety: Effective intervention strategies," *Saf. Sci.*, vol. 48, no. 8, pp. 1026–1035, Oct. 2010.

[8] F. W. Guldenmund, "Understanding and Exploring Safety Culture," Delft University of Technology, 2010.

[9] A. Hale and D. Borys, "Working to rule, or working safely? Part 1: A state of the art review," *Saf. Sci.*, vol. 55, pp. 207–221, Jun. 2013.

[10] A. Hale and D. Borys, “Working to rule or working safely? Part 2: The management of safety rules and procedures,” *Saf. Sci.*, vol. 55, pp. 222–231, Jun. 2013.

[11] N. G. Leveson, “Applying systems thinking to analyze and learn from events,” *Saf. Sci.*, vol. 49, no. 1, pp. 55–64, Jan. 2011.

[12] P. M. Salmon, R. McClure, and N. a. Stanton, “Road transport in drift? Applying contemporary systems thinking to road safety,” *Saf. Sci.*, vol. 50, no. 9, pp. 1829–1838, Nov. 2012.

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

[14] N. G. Leveson, “An STPA Primer,” Cambridge, MA, 2013.

[15] L. Pelegrín, “Evaluating Project Safety (System Engineering and Safety Management) in an Organization,” Heriot-Watt University, 2012.

[16] I. M. Dokas, J. Feehan, and S. Imran, “EWaSAP: An early warning sign identification approach based on a systemic hazard analysis,” *Saf. Sci.*, vol. 58, pp. 11–26, Oct. 2013.

[17] C. Harrison, M. Spencer, J. Thomas, N. Leveson, and C. Wilkinson, “Safety assurance in NextGen and complex transportation systems q,” *Saf. Sci.*, vol. 55, pp. 173–187, 2013.

[18] K. Kazaras, K. Kirytopoulos, and A. Rentizelas, “Introducing the STAMP method in road tunnel safety assessment,” *Saf. Sci.*, vol. 50, no. 9, pp. 1806–1817, Nov. 2012.

[19] N. G. Leveson, N. Dulac, B. Barrett, P. J. Carroll, and P. J. Cutcher-Gershenfeld, “Risk Analysis of NASA Independent Technical Authority,” Cambridge, MA, 2005.

[20] M. C. Davis, R. Challenger, D. N. W. Jayewardene, and C. W. Clegg, “Advancing socio-technical systems thinking: a call for bravery.,” *Appl. Ergon.*, vol. 45, no. 2, pp. 171–80, Mar. 2014.

[21] K. J. Astrom and R. M. Murray, *Feedback systems: An Introduction for Scientists and Engineers*. Princeton: Princeton University Press, 2012.

[22] S. Dekker and S. Pruchnicki, “Drifting into failure: theorising the dynamics of disaster incubation,” *Theor. Issues Ergon. Sci.*, vol. 0, no. 0, pp. 1–11, Nov. 2013.

[23] R. J. de Boer, “Seneca’s Error: An Affective Model of Cognitive Resistance ,” Delft University of Technology, Delft, 2012.

[24] D. Kahneman, *Thinking, fast and slow*, 1st ed. New York: Farrar Straus & Giroux, 2011.

[25] P. N. Johnson-Laird, *How we reason*. Oxford: Oxford University Press, USA, 2006.

[26] “Management,” *Wikipedia, the free encyclopedia*. [Online]. Available: http://en.wikipedia.org/wiki/Management.

[27] J. Helferich, “Radiation Oncology Safety An Application of ‘Managerial’ STPA,” in *STAMP Conference*, 2013.

[28] H. Fayol, *General and Industrial Management*. New York, NY: Pitman Publishing Corporation, 1949.

[29] J. Dul and T. Hak, *Case study methodology in business research*. Oxford: Butterworth-Heinemann, 2008.

[30] P. Underwood and P. Waterson, “Systemic accident analysis: examining the gap between research and practice.,” *Accid. Anal. Prev.*, vol. 55, pp. 154–64, Jun. 2013.

APPENDIX 1: CONTROL LOOP 1 EFFECTIVENESS – RETROSPECTIVE SITUATION (2010)

	Management task 1 Set goals and direction	**Management task 2 Establish work processes and standards**	**Management task 3 Staff, schedule and train**	**Management task 4 Manage facility and equipment**	**Management task 5 Allocate financial resources**	**Management task 6 Monitor and evaluate performance**
Error 1A Sensor	Positive: Aim to report as many risks and incidents as possible is well understood. Negative: --	Positive: All employees know how to report risks and incidents Negative: Reporting sometimes forgotten or ignored	Positive: All employees know how to report incidents Negative: There is not always sufficient time between flights to report, so that the incident is forgotten	Positive: Reporting system and email always available Negative: --	N/A	Positive: supervisor platform actually monitors reports of incidents. Negative: ..but he does not see the proactive (risk) reports
Error 1B Process Model	Positive: -- Negative: The platform coordinator does not see platform safety as his responsibility and does not react to signals of decaying safety margins	Positive: -- Negative: The platform coordinator does not see the creation of safety procedures as his responsibility	Positive: The platform coordinator understands the effects of resource mismatches Negative: The platform coordinator does not see the training of safety procedures as his responsibility	Positive: -- Negative: The platform coordinator does not see the management of facility and equipment as his task	Positive: -- Negative: The platform coordinator does not have budget responsibility	Positive: -- Negative: The platform coordinator does not see monitoring platform safety as his responsibility
Error 1D Control Algorithm	Positive: -- Negative: The platform coordinator does not see platform safety as his responsibility and does not initiate interventions.	Positive: -- Negative: The platform coordinator does not see the an intervention to improve compliance to safety procedures as his responsibility	Positive: The platform coordinator understands how to intervene in case of resource mismatches Negative: The platform coordinator does not initiate training of safety procedures	Positive: -- Negative: The platform coordinator does not initiate the management of facility and equipment as his task	Positive: -- Negative: The platform coordinator does not have budget responsibility	Positive: -- Negative: The platform coordinator does not take initiatives to monitor platform safety
Error 1E Actuator	N/A	N/A	Positive: The platform coordinator intervenes in case of resource mismatches Negative: --	N/A	N/A	N/A
Error F Out of Range process	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances	Positive: -- Negative: The platform coordinator does not prepare for out of range disturbances
Error 1G Cognitive Resistance	Positive: -- Negative: The platform coordinator does not see platform safety as his responsibility and does not react to signals of decaying safety margins	Positive: -- Negative: The platform coordinator does not see the creation of safety procedures as his responsibility	Positive:-- Negative: The platform coordinator does not see the training of safety procedures as his responsibility	Positive: -- Negative: The platform coordinator does not see the management of facility and equipment as his task	Positive: -- Negative: The platform coordinator does not have budget responsibility	Positive: -- Negative: The platform coordinator does not see monitoring platform safety as his responsibility

APPENDIX 2: CONTROL LOOP 2 EFFECTIVENESS – CURRENT SITUATION

	Management task 1 Set goals and direction	**Management task 2 Establish work processes and standards**	**Management task 3 Staff, schedule and train**	**Management task 4 Manage facility and equipment**	**Management task 5 Allocate financial resources**	**Management task 6 Monitor and evaluate performance**
Error 2A Sensor	Positive: Aim to report as many risks and incidents as possible is well understood. Negative: --	Positive: All employees know how to report incidents Negative: Reporting sometimes forgotten or ignored	Positive: All employees know how to report incidents Negative: There is not always sufficient time between flights to report, so that the incident is forgotten	Positive: Reporting system and email always available Negative: --	N/A	Positive: The Q&S department monitors reports of risks and incidents. Negative: --
Error 2B Process Model	Positive: The Q&S department acknowledges its responsibility in achieving safety targets Negative: --	Positive: The Q&S department acknowledges its responsibility in generating safety standards and procedures. Negative: --	Positive: The Q&S department acknowledges its responsibility in training for safety Negative: The Q&S department is not concerned with the effects of resource mismatches	Positive: The Q&S department will signal shortages in facility and equipment if this jeopardizes safety. Negative: The Q&S department does not see the management of facility and equipment as its task	N/A	Positive: The Q&S department actively ensures that safety is monitored by managers and by its own officers. Negative: --
Error 2D Control Algorithm	Positive: The Q&S department acknowledges its responsibility in achieving safety targets and knows how to initiate interventions. Negative: --	Positive: The Q&S department acknowledges its responsibility in establishing work processes and standards in the interest of safety and knows how to initiate interventions. Negative: --	Positive: The Q&S department acknowledges its responsibility in training staff in safety, and knows how to initiate interventions. Negative: The Q&S department does not acknowledge responsibility in managing capacity, and does not intervene	Positive: The Q&S department acknowledges its responsibility in the management of facility and equipment for safety, and knows how to initiate interventions. Negative: The Q&S department does not have formal rights to manage facility and equipment on behalf of the platform division.	Positive: -- Negative: The Q&S department does not have budget responsibility	Positive: The Q&S department acknowledges its responsibility in monitoring platform safety and knows how to initiate interventions Negative: The Q&S department does not have formal rights to reprimand employees in case of a lack of safety performance.
Error 2E Actuator	Positive: The Q&S department effectively intervenes when targets are threatened. Negative: The Q&S department does not have formal rights to intervene.	Positive: The Q&S department effectively intervenes when processes and standards are compromised. Negative: The Q&S department does not have formal rights to intervene.	Positive: The Q&S department effectively intervenes to enable safety training. Negative: The Q&S department does not acknowledge responsibility in managing capacity, and does not intervene.	Positive: The Q&S department effectively intervenes regarding the management of facility and equipment. Negative: The Q&S department does not have formal rights to intervene.	N/A	Positive: The Q&S department effectively on the monitoring of platform safety. Negative: The Q&S department does not have formal rights to intervene.
Error F Out of Range process	Positive: The Q&S department is prepared for out of range disturbances Negative: There is a belief that all out-of-range disturbances are accounted for.	Positive: The Q&S department has taken out of range disturbances in account in work processes. Negative:	N/A	Positive: -- Negative: There is a belief that all out-of-range disturbances in equipment and facilities are accounted for.	N/A	N/A
Error 2G Cognitive	Positive: No evidence of CR. Negative: There is a belief that all out-of-range disturbances are accounted for.	Positive: No evidence of CR. Negative: --	Positive: No evidence of CR. Negative: --	Positive: No evidence of CR. Negative: --	Positive: No evidence of CR. Negative: --	Positive: No evidence of CR. Negative: --