A System-Theoretic Model of Threat and Error Management in Flight Instruction

Ioana Koglbauer[a]*

* Corresponding author: Ioana Koglbauer, koglbauer@tugraz.at

[a]*Graz University of Technology, Kopernikusgasse 24/ IV, 8010 Graz, Austria, E-mail: koglbauer@tugraz.at*

Abstract

This study proposes a new model of threat and error management (TEM) in flight instruction. Currently TEM is taught using a linear model. However, linear models have limitations in describing complex processes involving multiple controllers, non-linear relationships or feedback. Thus, new methods are necessary for addressing the current complexity of TEM in the cockpit. The method presented here is based on system-theoretic process analysis (STPA). STPA is more suitable for describing control processes in complex systems with multiple and dynamic interactions among hardware, software, environment and people. The system-theoretic model of TEM proposed here addresses threats and errors in a more specific manner including the requirements for controlling a process (e.g. information and feedback, process model, control actions), communication and coordination among controllers and the hierarchical control structure. The new model is used to determine potential causes of hazards in each part of the control loop and in the hierarchical control structure. Potential causes of hazards are inadequate information or feedback, distraction, inadequate process models, communication problems between instructor and trainee, inadequate interface or automation, over-reliance on automation, over-reliance on the trainee, confusion by unexpected actions of the trainee, or of the automation, inadequate control actions. Thus, the system-theoretic model of TEM is a feasible and more comprehensive method for anticipating, preventing and managing threats and errors in flight instruction. The system-theoretic TEM model can be used for training flight instructors, for developing instruction scenarios and for analysing and preventing hazards and instructional incidents or accidents.

Keywords: Threat and Error Management; TEM; STAMP; STPA; Flight Instruction; Pilot.

1. Introduction

An investigation of the TEM process at 10 airlines found 7,257 errors during 2,612 observation flights (Klinect, 2005). The crew could not detect and manage on time 27% of these errors, having as a consequence a hazardous flight status in 1,347 of cases. Although flight crews successfully manage most of the errors and threats, TEM is a major part of the initial and recurrent training program.

Since threats and errors can be expected during flight, TEM is considered an essential capability of the pilots, especially in the challenging role of a flight instructor. Currently TEM is taught using a linear model developed by Helmreich, Klinect, & Wilhelm (1999) that is illustrated in Figure 1. According to this model the flight crew is responsible to manage expected or unexpected external threats, errors of other people they interact with, as well as errors of the crew members themselves. According to Helmreich et al. (1999) pilots' TEM task consists of anticipation and detection of external and internal threats, error avoidance and management of behaviours that may lead to a safe outcome or to an incident or accident. Outcomes of the crew's TEM process can be a safe flight or an incident or accident.
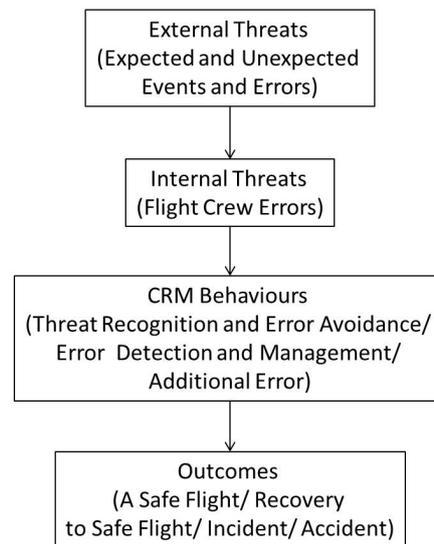

Fig. 1. Linear model of Threat and Error Management (adopted from Helmreich et al., 1999).

The current aviation system is complex and dynamic. This linear model has difficulties in explaining a complex process including non-linear relationships and feedback. Training should be adequate for the system in which pilots and instructors will operate (Martinussen, & Hunter, 2010). Thus, research is necessary to develop appropriate models for threat and error management in complex and dynamic systems.

2. Purpose of the study

This study proposes a new TEM model for flight instruction based on the System-Theoretic Process Analysis (STPA; Leveson, 2011a). The system-theoretic approach addresses control requirements of

individual controllers (e.g. trainee, instructor, automation), as well as multiple controller hazards, communication and coordination among controllers, and the enforcement of safety constraints at various levels of a socio-technical control structure. Thus, flight instructors and trainees can use a more comprehensive model for anticipating and managing threats and errors in their daily activity.

3. Method

STPA is a tool based on the System-Theoretic Accident Model and Process (STAMP; Leveson, 2004; 2011a and b). STPA begins with the specification of hazard and safety constraints which are necessary to control a hazard. At the core of STPA is the control loop. A controller can be human (e.g. pilot, trainee, instructor, examiner, inspector, manager) or automated (e.g. autopilot). The requirements for controlling a process are clear defined goals, the capacity of the controller to observe the controlled process, a model of rules and procedures on how to influence the process, and the ability to act and exert influence on the process in a given time and space (Leveson, 2011a). Feedback about the effect of control actions on the process is necessary for adjusting the control actions.

Thus, the controllers involved in the process are specified according to their control requirements and organized in a socio-technical control hierarchy. When a process involves multiple controllers, a specification of communication and coordination issues is necessary. In a subsequent step causal scenarios for inadequate control actions of each controller and means to prevent them are specified.

4. Towards a system-theoretic model of TEM in flight instruction

The process goal is to perform safe and efficient flight training. The hazard is an incident or accident. Safety constraints are identified and enforced to avoid the occurrence of an incident or accident. Figure 2 illustrates the system-theoretic model of flight instruction including the controllers involved in flight training (e.g. instructor, trainee and automation, and the higher-level controller) and their interaction in controlling the flight operation. Being higher in hierarchy the instructor controls both the trainee and the automatic controller. Since control processes related to flight are intrinsically related to space and time, these are part of the model. External disturbances can be external threats and errors such as weather, airport conditions and others that also influence the process and must be considered. Each controller receives information and feedback about the process directly or from another controller.

As Figure 2 shows, the work of an instructor is controlled by a higher level of the hierarchy. Thus, instructors do not decide themselves how they work. The higher level controller includes the head of training organization, company management, authorities, regulators, associations and unions. The flight instruction work is monitored and shaped by externally given requirements such as training objectives, exercises, procedures, equipment, schedule, colleagues and others.

Because of the dynamic nature of flight anticipation plays a central role in controlling the process. Thus, trainees must anticipate the future state of multiple parameters (e.g. own flight path, the

trajectory of other aircraft, effects of automation). In addition, the instructor has to anticipate the reactions of the trainee. According to the framework of anticipatory behavioural control (Hoffmann, 2003) internal model of actions are learned by comparison between predicted and actual sensory input. The anticipation-action-comparison unit is a tool developed by Kallus, Barbarino & van Damme (1997) that can be used for analysing threat and error management actions. Based on a mental model of the threat a pilot can predict future states of the system, possible errors and can take adequate recovery actions, based on his internal model of action. The match between real action and anticipated effects reinforces the mental model of threat detection and management. When threats and errors cannot be managed using the procedures contained in pilot's mental model corrective actions are necessary. Thus, both instructor and trainee need practice for learning and building their mental models of action in the process of flight instruction.

The feedback loop is a core element in STAMP and STPA. Feedback is necessary to check if the control actions have the expected result, and to adapt the control actions in order to obtain the necessary result. Each controller executes actions to influence the process, either directly or by giving an instruction or command to another controller.
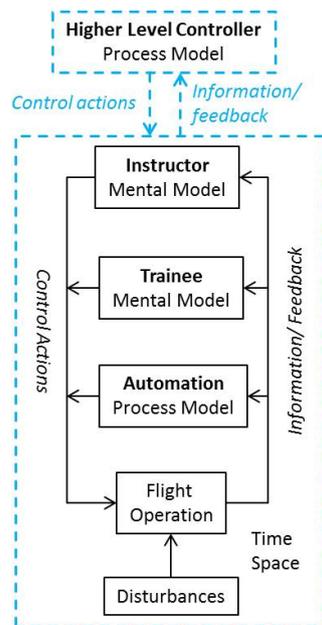

Fig. 2. System-theoretic model of the flight instruction process.

According to STPA the responsibilities of each controller are analysed. Thus, the trainee searches for information and feedback about the flight process using his or her senses, aircrafts' instruments and displays, warnings and alarms. The trainee processes this information according to a mental model that specifies unacceptable deviances from the goals, procedures on how to influence the flight process and reduce the deviation. The trainee exerts direct control or uses automation to control the flight process. The control actions of the trainee are controlled by the instructor. The trainee needs supervised practice and feedback from the instructor for completing and correcting his or her mental model of flight operation. Threat and error management is also learned during flight instruction. For being safe the

trainee needs to control the aircraft within the safe envelope, and to anticipate, prevent or manage threats and errors.

The flight instructor searches for information and feedback about the flight process from different sources: direct perception, instruments, displays and communication with the trainee. The instructor can use different control actions to influence the flight: giving verbal instructions to the trainee, giving control inputs concomitantly with the trainee, taking over control from the trainee, and using automation. Because of the multitasking nature of the flight, often the instructor performs a number of part tasks until the capacity of the trainee gradually increases to perform the whole task. In some cases the instructor requests the complete control of the flight, saying "my controls" and the trainee is expected to restrict from any inputs on flight process. This would be the case in a hazardous situation or when the instructor wants to prevent trainee's practice of a wrong procedure. However, in most of the cases the instructor will give verbal instructions helping the trainee to focus on information cues, necessary control actions and feedback. Whenever possible, the instructor allows the trainee to practice threat and error management under supervision. Rating of trainee's performance is also an instructor task. Usually ratings consider the type and amount of instructor inputs during the flight task. A higher rating is associated with less instructor inputs and reflects the trainee's ability to independently perform tasks.

Table 1. TEM-related Control Actions of the Instructors and Trainees.

Control Action	CA causes hazard	Lack of CA causes hazard	CA too early/ too late/ wrong sequence causes hazard	CA too long or too short causes hazard
Flight Instructor				
Monitoring the flight operation	Distraction, focusing too much on irrelevant aspects	Does not seek information and feedback	Monitors too infrequently, or too late	Does not monitor all the required sources of information; monitors too short;
Communication with the trainee	Commands an inadequate control action	Does not provide required verbal instructions	Provides instructions too late	Provides too short verbal instructions; Talks too much and distracts the trainee
Direct control inputs	Provides conflicting or uncoordinated control inputs	Does not take over the control	Provides control inputs too late; Takes over the control too late	Provides too short or too long control inputs
Trainee				
Monitoring the flight operation	Distraction, focusing too much on some aspects	Does not seek information and feedback	Monitors too infrequently or too late; Uses an inadequate scanning sequence	Does not monitor all the required sources of information; Too short fixations
Communication with the instructor	Provides incorrect information	Does not provide information when required	Provides information too early, too late or out of sequence	Provides too little or too much information
Control Actions	Provides inadequate control actions	A required control action is not provided; Does not follow the instructor's command	Provides control actions too early, too late or in the wrong sequence; Follows an instruction too early, too late or out of sequence	Provides too short or too long control inputs; Follows an instruction too long or stops too early

Using the system-theoretic process analysis (Leveson, 2011a) a hazard analysis can be performed to determine safe and unsafe control actions of the instructor and trainee pilot. Theoretically the hazard analysis includes for categories for each control action: the control action causes a hazard, the lack of control action causes a hazard, the control action is applied too late, too early or out of sequence, or it is applied too short or too long. In Table 1 adequate and hazardous control actions of the trainee and of the instructor are described.

Based on STPA (Ishimatsu, Leveson, Fleming, Katahira, Miyamoto, & Nakao, 2011) the following categories of multiple controller hazards can be identified for the process of flight instruction: both the instructor and trainee perform the required control action; none of the pilots performs a required action (e.g. monitoring the airspeed); one pilot (e.g. trainee) does not perform a required action, and the other pilot (e.g. instructor) performs the required action (e.g. the trainee does not monitor the glide path and the instructor tells him that they are too low); both pilots perform unsafe actions (e.g. initiate the go-around too late). Some of the potential causes of multiple controller hazards are communication problems between instructor and trainee, inadequate interface or automation, over-reliance on automation, over-reliance on the trainee, confusion by unexpected actions of the trainee, or of the automation.

Figure 3 illustrates a system-theoretic TEM model used for creating causal scenarios of threats and errors which are related to all segments of the control loop. The specification of causal scenarios described in STPA Step 2 can be used to determine how inadequate control actions of the higher level controllers, instructors and trainees could occur, as well as means to prevent them. It is not the purpose of this paper to describe all possible scenarios, but to provide a framework which shows how the system-theoretic model of TEM can be used for hazard analysis and prevention. Thus, two exemplary scenarios are presented here.
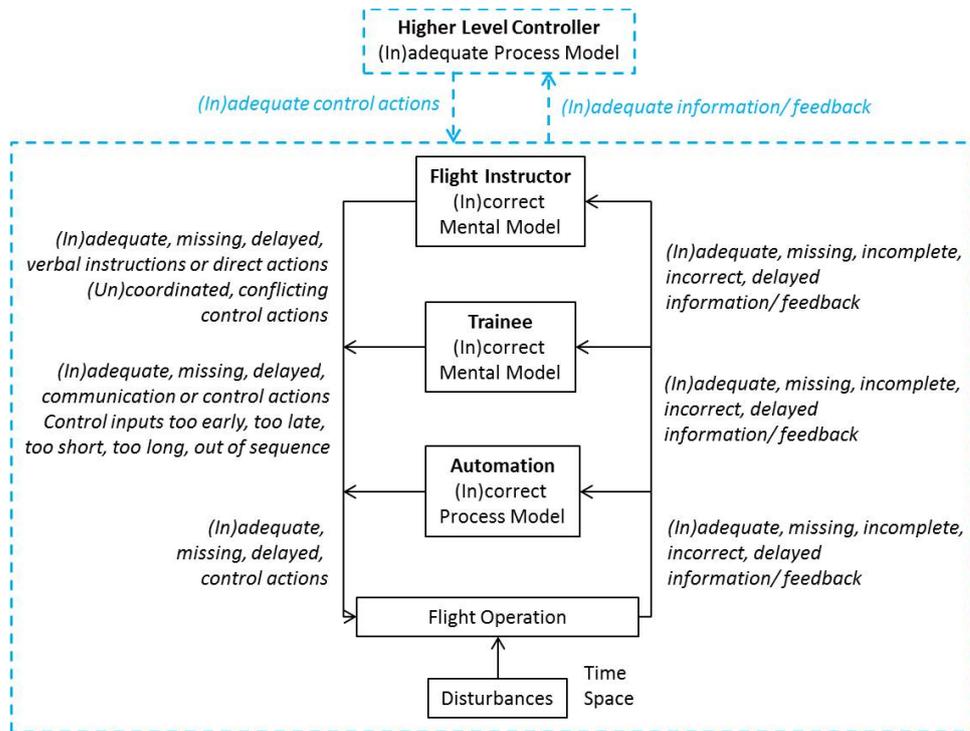

Fig. 3. System-theoretic model of Threat and Error Management (TEM)

Scenario 1: The trainee provides too short control actions and brings the aircraft in a hazardous state. For example the trainee stops too soon to increase the descend rate and reduce thrust, resulting in an unstable approach. This scenario could occur in following situations:

- The trainee does not monitor the altitude, airspeed, and vertical speed indications for feedback because she or he uses an inadequate scanning pattern, or is distracted, or

- The trainee has an inadequate mental model for anticipating the effects of her/ his control inputs, or

- The trainee has an inadequate mental model of the required parameters for the approach, or

- The trainee has an inadequate model of automation and believes that the automation will handle some parameters when it does not, or

- The trainee has an inadequate mental model on how to apply the control inputs.

Various measures can be taken for avoiding such a scenario during real flight instruction. The preventive measures are rooted in theoretical and practical simulator training, and briefing of the trainee before flight.

TEM controls suggested for avoiding the scenario 1:

- The instructor provides information about the adequate scanning pattern and checks the pattern of the trainee before the real flight using a cockpit mock-up or a simulator and gives feedback for correcting an inadequate pattern;

- The instructor provides information and checks the trainee's mental model for anticipating effects of her/ his control inputs and gives feedback to correct the trainee's mental model;

- The instructor provides information and checks the trainee's knowledge of the flight parameters used in approach and gives feedback when the knowledge of the trainee is not accurate;

- The instructor provides information and checks the trainee's mental model of the automation used in the particular type of aircraft, giving feedback to correct the mental model if necessary;

- The instructor provides information and checks the trainee's mental model of the control effects and flight dynamics of the particular type of aircraft, giving feedback to correct the mental model if necessary.

Scenario 2: The instructor pilot takes over the control from the trainee too late. For example the trainee flies an unstable approach below 500ft and the instructor takes over the control and goes-around too late. This scenario could occur in following situations:

- The instructor detects too late the cues indicating that a go-around is necessary because she or he is distracted, or

- The instructor relies too much on inadequate feedback received from the trainee and detects too late that trainee's control actions do not have the expected effect, or

- The instructor has an inadequate feedback from automation, believes that the automation will handle some parameters and detects too late that it does not, or

- The instructor has an inadequate mental model for anticipating the trainee's errors, or

- The instructor has an inadequate mental model of the parameters which require her/ his intervention during a mismanaged unstable approach;
- The instructor does not take into account the time and space necessary to intervene and correct the flight parameters;
- The instructor is confused by unexpected control actions of the trainee or of the automation.

TEM controls suggested for avoiding scenario 2:

- The instructor monitors the flight situation, instruments, automation and the trainee and avoids distraction;
- The instructor double-checks the information and feedback provided by the trainee and automation;
- The instructor is trained to anticipate trainees' errors;
- The instructor specifies or receives from her/ his organization procedures that specify parameters for taking over the control or making corrective actions.

These examples show how STPA can be used to model potential causes of hazards for each controller, in each part of the control loop. As compared to the linear model, the system-theoretic TEM model can be used to specify more comprehensive TEM control actions for the entire socio-technical system involved in flight instruction.

5. Conclusion

In this study a new and more comprehensive model of threat and error management was developed based on the system-theoretic process analysis (Leveson, 2004; 2011a). The new TEM model can be used for training flight instructors, for developing instruction scenarios and for analysing and preventing hazards and instructional incidents or accidents.

References

Helmreich, R. L., Klinect, J. R., & Wilhelm, J. A. (1999). Models of threat, error, and CRM in flight operations. In R. Jensen (Ed.) *Proceedings of the 10th International Symposium on Aviation Psychology*. Columbus, OH: The Ohio State University, 677-682.

Hoffmann, J. (2003). Anticipatory behavioral control. In Butz, M. V., Sigaud, O., Gerard, P. (Eds.) *Anticipatory behaviour in adaptive learning systems*. Springer, Berlin.

Ishimatsu, T., Leveson, N., Fleming, C., Katahira, M., Miyamoto, Y. & Nakao, H. (2011). Multiple controller contributions to hazards. *Conference of the International Association for the Advancement of Space Safety*, Versailles, France.

Kallus, K.W., Barbarino, M., van Damme, V. (1997). *Model of the cognitive aspects of air traffic control*. HUM.ET1.ST01.1000-DEL02. Eurocontrol.

Klinect, J.R. (2005). *Line Operations Safety Audit: A cockpit observation methodology for monitoring commercial airline safety performance*. Dissertation Thesis, University of Texas, Austin.

Leveson, N.G. (2004). A new accident model for engineering safer systems. *Safety Science, 42*, 237-270.

Leveson, N. (2011a). *Engineering a safer world*. Cambridge, MIT Press.

Leveson, N.G. (2011b). Applying systems thinking to analyze and learn from events. *Safety Science*, 49, 55-64.

Martinussen, M., & Hunter, D. R. (2010). *Aviation psychology and human factors*. CRC Press, Taylor & Francis Group, Boca Raton, FL.