A System-Theoretic Accident Model and Process with Human Factors Analysis and Classification System taxonomy

Michał Lower\textsuperscript{a}, Jan Magott\textsuperscript{a}, Jacek Skorupski\textsuperscript{b,⁎}

\textsuperscript{a} Warsaw University of Technology, Faculty of Transport, Koszykowa 75, 00-662 Warsaw, Poland
\textsuperscript{b} Warsaw University of Technology, Faculty of Electronics, Wybrzeże Wyspianskiego 27, 50-370 Wrocław, Poland

A R T I C L E  I N F O

Keywords: System-Theoretic Accident Model and Process (STAMP) Human Factors Analysis and Classification System (HFACS) Causal Analysis using STAMP (CAST)

A B S T R A C T

Formal methods are necessary for effective analysis of the causes of complex accidents. One of possibilities is the System-Theoretic Accident Model and Processes (STAMP) using a hierarchical safety control structure for finding control flaws leading to hazards. The aim of this paper is to enhance STAMP error taxonomy by Human Factors Analysis and Classification System (HFACS). The method proposed in this paper is STAMP-HFACS framework for accident analysis. This framework is STAMP structure-driven, i.e. levels of the HFACS structure are incorporated into components of the STAMP safety control structure. A result of the proposed procedure is the STAMP-HFACS diagram. To illustrate the applicability of the method one thread of the Überlingen midair accident was analyzed. The STAMP-HFACS methodology can express interactions between people, technical equipment, and the environment. It is not bound to an incident/accident events chain. It allows for an analysis of a safety-related occurrence focused on finding some adverse relationships between the components, especially at higher levels of the HFACS methodology. Proper recognition of these relationships, and especially their interpretation in system-theoretic terms related to specific components, can be of great importance for increasing the level of air traffic safety.

1. Introduction

Accident models can be classified into three categories: sequential (e.g., Heinrich, 1931), epidemiologic (e.g., Reason, 1990, Shappell et al., 2007) and systemic (e.g., Rasmussen and Svedung, 2000, Hollnagel, 2004, Leveson, 2012). Systematic methods are required in order to find the causes of air traffic events. According to (Leveson, 2012), accidents involve a complex, dynamic process. This process arises in interactions among humans, machines and the environment. CAST (Causal Analysis using STAMP), where STAMP stands for System-Theoretic Accident Model and Processes (Leveson, 2012, CAST, 2013), can be used for incident/accident analysis (to generate plausible scenarios). According to STAMP, system safety is mainly a control problem, not a reliability one, i.e. the system should satisfy safety constraints. A strong feature of STAMP is its safety control structure, e.g. it allows to take into account inter-component interactions by control and feedback. Hence system errors can be identified. STAMP error taxonomy (Stringfellow, 2010, Leveson, 2012) is hierarchical. However, according to (Harris and Li, 2011), the human factors of STAMP are under-specified.

When searching for errors in a concrete system, STAMP error taxonomy can be supported by additional error taxonomy. Taxonomies as contained in Anticipatory Failure Determination (AFD) (Visnepolschi et al., 1999) and Hierarchical Holographic Modeling (Kaplan et al., 2001) may be useful here.

This paper is on air traffic safety. In air transport, human errors occur in more than \(\frac{2}{3}\) of accidents and incidents. Hence it is reasonable to consider the following question: Can STAMP Error Taxonomy be enhanced by Human Factors Analysis and Classification System (HFACS)? HFACS (Shappell et al., 2007) is one of the most widely used human factors accident analysis frameworks in air, rail, and maritime transport and also in civil engineering. It is based on Reason’s “Swiss Cheese” model of human behavior (Reason, 1990) and Rasmussen’s human error taxonomy (Rasmussen, 1982). HFACS studies human error at four levels: Unsafe acts, Preconditions for unsafe acts, Unsafe supervision and Organizational influences. Each higher level affects the next downward level. This influence represents not only chains of events; it has recognized statistical dependencies between the levels (Li et al., 2008).

In (Harris and Li, 2011), the authors proposed an extension of the HFACS approach, called HFACS-STAMP, with constraint and control action concepts taken from STAMP. This approach is HFACS structure-
driven. Applying Rasmussen’s human mental model to STAMP/STPA is provided in (Hoshino, 2014).

Our approach, as proposed in this paper, is contrary to that of Harris and Li. It is called STAMP-HFACS (Lower et al., 2015). This framework is STAMP structure-driven, i.e. levels of the HFACS structure are incorporated into components of the STAMP safety control structure. The main difference between our STAMP-HFACS and the HFACS-STAMP as created by Harris and Li is that in HFACS-STAMP the levels of HFACS of an organization are not distributed into different components. Hence, in HFACS-STAMP the structure of the system is only partially represented.

In (Luxhoj and Coit, 2006), the authors presented the Aviation Safety Risk Model (ASRM) for risk modeling and analysis. An early version of the ASRM is based on Bayesian Belief Networks (BBN), a BBN extension called influence diagrams, and HFACS. The HFACS is primarily focused on human performance including errors as well as organization failures or deficiencies. For later version of the ASRM (Luxhoj and Oztekin, 2009), authors developed Hazard Classification and Analysis System (HCAS) to address some of the limitations of the HFACS. In (Luxhoj and Oztekin, 2009), the HCAS is Unmanned Aircraft System oriented. The HCAS is based on the Federal Aviation Administration (FAA) regulatory perspective: Aircraft, Airmen, Certification/Airworthiness, Flight Operations. The ASRM is appropriate for modeling risk in the absence of hard statistical data, e.g. for novel systems. In this case, expert judgements are incorporated into BBN. In (Luxhoj et al., 2017), the ASRM has been used in risk estimation for UAS (Unmanned Aerial System) operations in precision agriculture for targeted aerial application. In STAMP, an emphasis is put on control and feedback between the components, while they are in analysis focus neither in HFACS nor HCAS.

In (Lower et al., 2015), only the outline of STAMP-HFACS methodology is proposed. As an example, a serious air traffic incident of the Runway Incursion Type is analyzed. In this paper, a detailed description of the STAMP-HFACS method is presented. The direct aim of the paper is to present a methodology rather than a comprehensive accident analysis. To show the usefulness of the method, it was applied to an analysis of the Überlingen air traffic accident. Because of its complexity, we propose to split the analysis into threads. The analysis is focused on Tu-154 pilots. Many of the interesting relationships that illustrate our approach to the combined use of STAMP and HFACS can be shown on their example. At the same time, the existing dependencies at all levels of HFACS related to the work of the Tu-154 crew are not so well documented in the literature, where more attention is paid to issues related to the organization of air traffic control. Taking into account the necessity of limiting the size of the paper, only the thread of the incident related to the Tu-154 pilots is presented in more details. The application of the STAMP-HFACS method for multithreading analysis will be the subject of another work.

A suitable software tool is required in order to analyze a complex incident/accident process and to record it. We will show how to represent STAMP-HFACS analysis results in an A-CAST tool (Abdulkhaled, 2015) which will be a plug-in for XSTAMP. XSTAMP is An-extensible-STAMP-Platform tool support for safety engineering. Representation of the results in A-CAST was not considered in (Lower et al., 2015).

The rest of the paper is organized as follows. In Section 2 an introduction to STAMP is presented. Section 3 contains a description of HFACS. In Section 4 a description of the proposed STAMP-HFACS framework is given. In Section 5 we describe some aspects of the Überlingen accident in a way that is suitable for STAMP-HFACS application, which is then presented in Section 6. In the next section a representation of the STAMP-HFACS analysis results in the A-CAST tool is described. The last section contains final conclusions and further work plans.
2. Causal analysis using STAMP (CAST) in accident/incident analysis

The fundamental idea behind the System-Theoretic Accident Model and Processes (STAMP) (Leveson, 2012) is a hierarchical safety control structure. This structure is based on a classification of control flaws leading to hazards (Leveson, 2012), which is given in Fig. 1.

A component is a part of the system. It can be a person, a technical device, or an organization. It can be atomic or combined from other components. Causal Analysis using STAMP (CAST, 2013, Hickey, 2012, Leveson, 2012) schema is as follows:

1. Identify the system(s) and hazard(s) involved in the loss.
2. Identify the system safety design constraints and system requirements associated with that hazard.
3. Construct the safety control structure as it was designed to control the hazard and enforce the safety constraints.
   (a) Component responsibilities.
   (b) Control actions and feedback loops.
4. Determine the proximate events leading to the loss.
5. Analyze the event at the physical system level. Identify the contribution of the physical and operational controls, physical failures, dysfunctional interactions, communication and coordination flaws, and unhandled disturbances to the events. Determine why the physical control was ineffective in preventing the event. For each component, determine if it fulfilled its responsibilities or provided inadequate control.
6. Moving up the levels of the safety control structure, determine how and why each successive higher level contributed to inadequate control at the lower level.
   (a) For each system safety constraint, determine whether the responsibility for enforcing it was assigned to a component in the safety control structure or if (a) component(s) did not exercise adequate control to ensure their assigned safety constraints were enforced in the components below them.
   (b) Develop an understanding of all human decisions or flawed control actions in terms of: the information available to the decision maker, required information that was not available, behavior-shaping mechanisms (e.g., the context and influences on the decision-making process), the value structures underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.
7. Examine the coordination and communication contributors to the accident.
8. Determine the dynamics and changes in the system and the safety control structure that over time migrated the system to a higher risk.
9. Determine the changes that could eliminate inadequate control (lack of enforcing the system safety constraints) in the future and generate recommendations.

CAST has been used for many types of incidents (CAST, 2013):

- Aviation.
- Trains.
- Chemical plants.
- Off-shore oil drilling.
- Road tunnels.
- Medical devices.

Often, CAST analysis has allowed to identify causal factors that were omitted in official reports. The main advantage of CAST analysis is a structural approach which puts emphasis on control structure and inter-component interactions, i.e. controls and feedback. In this paper, we propose to apply HFACS in point 6, sub-point b of the above CAST schema in order to understand human decisions and flawed control actions.

3. Human Factors Analysis and Classification System (HFACS)

3.1. Outline of the HFACS

In the HFACS (Shappell et al., 2007) there are four levels and seventeen categories of factors. The levels are as follows:

- Level 1 – “Unsafe acts of operators”,
- Level 2 – “Preconditions for unsafe acts”,
- Level 3 – “Unsafe supervision” (lower management layer in Reason’s model),
- Level 4 – “Organizational influences” (higher management layer in Reason’s model).

The DOD HFACS Version 7.0 taxonomy is given in (DOD HFACS, 2016, p. 22) and repeated in Fig. 5 in Appendix A of this paper. The levels are:

- Level 1 – “Acts”,
- Level 2 – “Preconditions”,
- Level 3 – “Supervision”,
- Level 4 – “Organizational influences”.

In the taxonomy there are seventeen categories of errors, e.g. for preconditions there are the following categories:

- Physical Environment,
- Technological Environment,
- Physical Problem,
- Mental Awareness,
- State of Mind,
- Sensory Misperception,
- Teamwork.

The US Department of Defense has extended the HFACS by associating sets of factors with a category (DOD HFACS, 2016). There are 18, 17, 61, and 13, respectively, factors in Levels 4, 3, 2, and 1, e.g. for the category Judgement and Decision Making Errors, the following factors are associated with:

- AE201 Inadequate Real-Time Risk Assessment,
- AE202 Failure to Prioritize Tasks Adequately,
- AE205 Ignored a Caution/Warning,
- AE206 Wrong Choice of Action During an Operation.

The HFACS has been applied in analyses of events in air traffic (Li et al., 2008), remotely piloted aircraft operations (Tvarnyas et al., 2006), shipping (Celik and Cebi, 2009), rail transport (Baysari et al., 2008), civil engineering (Garrett and Teizer, 2009).

3.2. HFACS in aviation safety analysis

Aviation fulfills all of the conditions that allow us to include it into a class of complex systems with a very strong influence of the human factor. In such systems, the HFACS method of analysis is applicable in analyses of causes of incidents and accidents. In this method we examine not only the active errors and omissions directly leading to the event but we also extend the analysis to higher levels of the system design. Accidents and incidents in aviation must be considered in the context of a system in which they occur. It consists of three elements: air traffic, the air traffic control (ATC) system and the physical and organizational environment. Air traffic consists of the aircraft that move according to pre-established routes which are agreed upon and coordinated by Air Traffic Control services. Depending on the phase of the flight, these are: ACC (Area Control Center) – for aircraft in the cruise phase of the flight, APP (Approach control) – for aircraft
approaching landing and climbing after take-off, and TWR (Tower control) for taking off and landing aircraft. Every ATC service supervises a specific part of airspace which is divided into elementary sectors. These can be combined dynamically into larger structures in the case of low traffic. The most important element of these services are the air traffic controllers (ATCos) who ensure safe and suitably arranged traffic flow in control sectors under their supervision. In their control decisions, ATCos have to take into account the state of the environment, and in particular meteorological conditions, but also of the non-physical environment, e.g. procedures and regulations that to a large degree govern the organization of air traffic. The non-physical environment is defined by international organizations, particularly the ICAO (International Civil Aviation Organization), the national civil aviation authorities, as well as the management system of the ATC structure.

According to the structure presented in Fig. 5 in Appendix A, the HFACS applied to an analysis of the causes of incidents includes four levels:

1. Acts. This is a group of active errors committed (e.g. bad decisions or incorrect assessment of input information) and negligence resulting, for example, from routine. It may include even deliberate violation of adopted rules (e.g. the suicide of the Germanwing’s pilot in the French Alps).

2. Preconditions. Making mistakes at the first level is usually reinforced by a combination of factors which have a direct impact on the operators involved in the traffic (pilots, ATC controllers). This group of errors includes, in particular, issues in interpersonal communication, the physical and mental state of important participants of the events, as well as the state of the environment, both physical and technological.

3. Supervision. Because of the possible negative effects, the air transport system has numerous supervision mechanisms. Irregularities and especially neglect in this area may contribute to premises to make mistakes.

4. Organizational influences. The management of the organization, and in particular high level managers’ approach to safety issues, can play a key role in the development of the whole causal chain, which can finally produce an air accident.

4. STAMP-HFACS framework

4.1. The reason for incorporating the HFACS into STAMP analysis

First, some limitations of the HFACS will be presented. In order to point to these limitations, the results of the CAST analysis of an accident of a U.S. Coast Guard 6505 helicopter (Hickey, 2012) will be presented. Second, because STAMP taxonomy of human errors is somewhat underspecified, a proposal of extending STAMP Individual and Organizational Error Taxonomy (Stringfellow, 2010) using HFACS taxonomy will be given.

A short description of the CG-6505 helicopter accident (Hickey, 2012) is as follows: on September 4, 2008, a Coast Guard HH-65 helicopter (CG-6505) and a 47-foot Coast Guard small boat (CG-47317), both stationed near Honolulu, Hawaii, were conducting hoisting training at approximately 8 p.m. local time when the helicopter’s hoist became snagged on the small boat’s engine room dewatering standpipe. The helicopter eventually crashed and all four people on board (pilot, co-pilot, flight mechanic, and crewperson) were killed.

Per standard procedures and policy, the Coast Guard performed a detailed investigation (Mishap Analysis Board (MAB) in accordance with DOD HFACS 6.2) of the CG-6505 mishap which detailed the accident’s causes, contributing factors, and the recommendations to address these issues (Hickey, 2012).

Table 1 (which is a part of Table 2 included in Appendix B) illustrates the expressive power of HFACS 7.0 when compared to CAST analysis. The first column contains the CAST findings given in (Hickey, 2012). The second column illustrates how the MAB findings cover the CAST findings. The third column contains an interpretation of the CAST findings that has been obtained by the authors of this paper using HFACS 7.0.

To conclude, the CAST findings are relatively well covered by the DOD HFACS 7.0 categories (factors). This confirms the high expressive power of the DOD HFACS 7.0 taxonomy. However, the HFACS is insufficient for identifying system errors.

Technical equipment can be taken into account according to the HFACS category of Technological environment. However, the technical components are not represented separately. The structure is not modeled. Therefore, there is no requirement to model the responsibilities of the components. Hence there is no obligation to model inter-component interactions. In consequence, the modeling power of control and feedback between the components is insufficient.

In the literature, there have been trials to incorporate individual and organizational error categories into STAMP error taxonomy; for instance, according to Individual Error Taxonomy (Stringfellow, 2010), at the controller level inadequate control actions occur due to:

1. Inadequate control goal,
2. Design of the control algorithm does not enforce constraints,
3. Model of the controlled process is inconsistent, incomplete, or incorrect,
4. Model of the organizational structure (other controllers in the control hierarchy) is inconsistent, incomplete, or incorrect,
5. Inadequate coordination between decision makers,
6. Inadequate execution of the control loop.

A more detailed taxonomy with even three levels of nesting is presented in (Stringfellow, 2010).

For a human being, e.g. an aircraft pilot or air traffic controller, a control algorithm and model of the controlled process are insufficient to define the control actions. Hence we propose to add a new group called Inadequate individual preconditions to this taxonomy. Individual preconditions describe the context in which a decision is made. This group is based on the Physical and Mental State part which contains four categories and a Teamwork category of Level 2 of the HFACS structure (Fig. 5 in Appendix A), and is given as follows:

7. Inadequate individual preconditions:
   7.1. Inadequate physical properties,
   7.2. Inadequate state of mind,
   7.3. Inadequate sensory misperception,
   7.4. Inadequate communication channels provided in the organization,
   7.5. Inadequate safety management and learning processes,
   7.6. Inadequate interactions with external bodies.

According to the Organizational Error Taxonomy (Stringfellow, 2010), inadequate control actions occur due to:

1. Inadequate assignment of goals, control authority and responsibilities to controllers,
2. Inadequate allocation of resources to controllers throughout the organization,
3. Inadequate assignment of controller hierarchy,
4. Inadequate communication channels provided in the organization,
5. Inadequate communication of system-level goals and constraints,
6. Inadequate safety management and learning processes,
7. Inadequate interactions with external bodies.

The authors of this paper suggest to specify point 6 of the above list in the following manner:

6. Inadequate safety management and learning processes:
   6.1. Inadequate organizational influences (Categories of Organizational Influences, i.e. HFACS Level 4):
The STAMP safety control structure in point 6.b of the CAST schema in the analysis of a Coast Guard HH-65 helicopter mishap (one row only) +, +/−, −/+ −, − respectively, means that the MAB Findings have covered the CAST findings good, partially, poorly partially, not covered.

<table>
<thead>
<tr>
<th>Frequent occurrence of overcontrol/overtorque in nighttime hoisting operations</th>
<th>How MAB Findings have covered the CAST Findings (partially based on (Hickey, 2012, pages 114–116))</th>
<th>Interpretation of the CAST Findings Using DOD HFACS 7.0 Category (Factor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The physical system does not provide adequate feedback and controls to the pilot to assist the pilot in safely executing nighttime hoisting operations</td>
<td>MAB did not address systemic factors</td>
<td>Performance-Based Errors (AE104 Over-Controlled/Under-Controlled Aircraft/Vehicle/ System)</td>
</tr>
<tr>
<td>The pilot relies heavily on limited visuals and the altimeter to ensure the approach/hover is conducted at a safe distance</td>
<td>Generally accepts risk</td>
<td>Physical Environment (PE101 Environmental Conditions Affecting Vision)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Technological Environment (PE202 Instrumentation &amp; Warning System Issues)</td>
</tr>
</tbody>
</table>

6.1. Resource Problems,
6.1.2. Inadequate personnel selection and staffing,
6.1.3. Inadequate policy and process issues,
6.1.4. Inadequate climate/culture influences.
6.2. Inadequate supervision (Categories of Supervision, i.e. HFACS Level 3):
6.2.1. Supervisory violations,
6.2.2. Planned inappropriate operations,
6.2.3. Inadequate supervision.

Except for the above extension, the HFACS taxonomy can support the STAMP Error Taxonomy in error scenario structuring when detailed semantics is required.

4.2. Construction of a STAMP-HFACS diagram

In the STAMP-HFACS approach, the HFACS categories that are associated with the analyzed event are incorporated into components of the STAMP safety control structure in point 6.b of the CAST schema in the following manner:

A component of the STAMP safety control structure is characterized by the following properties:

- Safety-Related Responsibilities,
- Context in which a Decision is Made,
- Unsafe Decisions and Control Actions,
- Process Model Flaws.

In order to illustrate a human factor impact on an incident, HFACS elements are incorporated into the safety control structure as follows:

1. Select all such components of the safety control structure that contain a human factor,
2. For each component selected in point 1, choose such levels of the HFACS structure that will be included in this component,
3. For each level chosen in point 2, select its categories and factors included in these categories that should be considered in the event analysis, and add human factors that are not included in HFACS but are associated with analyzed event.
4. Add how the factors of HFACS categories, and human factors that are not included in HFACS but associated with the event influence the other factors for:
   - interactions between components,
   - influence inside the component,
   - and assign the semantics of errors and the influence between them for the analyzed event to the component’s properties.

Because of variety of causes of events, it is possible that HFACS factors list is insufficient. HFACS has been changed during its history. If there exists a human factor which has not yet been included in HFACS taxonomy in a time, then the taxonomy need to be extended. It is clear that future changes in civil air transportation, e.g. unmanned aerial vehicles, should be taken into account in future HFACS taxonomy. Therefore, in points 3 and 4, human factors that are not included in HFACS but are associated with the event are taken into account. A result of the above procedure is the STAMP-HFACS diagram, see Fig. 3.

The analysis of causes of an air traffic occurrence concerns an accident over Überlingen that took place on July 1, 2002 (BFU, 2004). In airspace controlled by Area Control Centre (ACC) Zurich a collision of two aircraft took place (Tu-154 Bashkirian Airlines and Boeing 757-23-AF DHL) on the German-Swiss border near Lake Constance. The sequence of events was as follows (chronologically):

1. Boeing 757, operating for DHL (B757), was the first to contact ATCo from ACC Zurich. It was at flight level FL 260 (approximately 7900 m). ATCo allowed to climb to FL 320 (approximately 9700 m) directing it straight to the important navigational waypoint Tango VOR. The crew asked for permission to climb to FL 360 (approximately 11,000 m). After six minutes such permission was issued.
2. At the time when communication between the same ATCo and the Tu-154 aircraft was established the aircraft occupied light level FL 260 (approximately 7900 m). After six minutes such permission was issued.
3. In both aircraft a TA (Traffic Advisory) warning from TCAS took place. In response, ATCo instructed the Tu-154 aircraft to descend to FL 350.
4. The TCAS system generated an RA (Resolution Advisory) for the B757 aircraft consisting of a command to descend. An analogous RA command to Tu-154 was to climb, which was contrary to the earlier instruction of ATCo.
5. Since the previous command to descend to FL 350 was not confirmed by the Tu-154 crew, ATCo repeated the instruction for them about collision traffic at FL 360.
6. The B757 crew continued the descent, increasing vertical speed, and informed the controller about this maneuver.
7. The TCAS system required an increase in vertical climb speed for the Tu-154, then a collision in the air took place.
5.2. Circumstances of the event

The above description of the event focuses on elements directly related to aircraft control. At the same time, some circumstances that could be considered favorable to the accident occurred.

1. ACC Zurich (the air traffic control service responsible for aircraft in the cruise phase of flight) had recently introduced new vertical separation minima in the upper airspace. These required service work on the radar. Technical teams performed this work precisely on the day of the event. Its essential element was to switch the radar into fallback mode in which some system functions would not work. We can therefore speak about a situation of reduced effectiveness of the air traffic control system. One of the manifestations of this decrease was a reduced refresh rate of the traffic information on the controller’s display. This reduction also affected another important element (from the safety point of view) – the system of short-term collision alert (STCA). In basic mode, the STCA gives visual and audible messages about an expected conflict with detailed information about the aircraft concerned. However, in fallback mode only audio messages can be heard. Furthermore, it is not possible to determine the aircraft remaining in a conflict situation. It should be emphasized that this situation was anticipated by the safety management system in ACC Zurich because, in accordance with the operations manual, switching the radar into fallback mode is associated with increased radar separation from 5 to 7 NM. Regardless of this remedy, the ATCo was not informed (he was not aware of this) that the STCA system was not operating normally.

2. Maintenance works also included a telephone communications network. As a result, the ACC Zurich control center was cut off from the possibility of telephone contact with neighboring air traffic control centers.

3. In ACC Zurich, the air traffic control center that was directly responsible for the airspace in which the collision occurred, due to low air traffic, only one controller remained on duty. He was combining the functions of Executive Controller (EC) and Planning Controller (PC). The second controller was in the rest lounge. This was standard and routine, and the second controller had to appear in the control room in the morning when the traffic was higher. Because of the distance between the rest lounge and the operating room, his appearance could not be immediate.

4. In ACC Zurich’s area of responsibility an “exceptional occurrence” took place involving the need to handle a delayed Airbus A320 (A320) that had to land in Friedrichshafen. This was not a very complicated task but it was necessary to agree on the transfer of responsibility among different workstations. On each of them there were different controllers, including the executive controller (EC) and planning controller (PC). The second controller was in the rest lounge. This was standard and routine, and the second controller had to appear in the control room in the morning when the traffic was higher. Because of the distance between the rest lounge and the operating room, his appearance could not be immediate.

5. The necessity to handle the A320 aircraft caused a change in the conventional method of the controller’s work. He used two monitors simultaneously that were displaying the traffic situation differently. One of them presented the standard view of the whole area of responsibility while the other presented only its part (zoom), which was aimed at better monitoring of the landing A320 aircraft movements. On both screens aircraft involved in the collision were visible, but due to the zoom function being applied the scale was different. The lack of communication with TWR Friedrichshafen forced the controller to use two different workstations. On each of them he used a different communication frequency and another monitor. On one of them he communicated with the B757 and Tu-154 aircraft, on the other with the A320 aircraft.

6. The neighboring control center UAC (Upper Area Control) Karlsruhe noticed the possibility of aircraft collision but, because of inoperative phones at ACC Zurich, they failed to pass on the information about the threat.

5.3. Analysis of errors/contributing factors from the Tu-154 crew

1. The crew of the Tu-154 aircraft had noticed conflicting traffic on their own flight level before the TCAS system generated a TA warning. They discussed this fact among themselves but took no action, in particular they did not inform the controller about the fact.

2. Tu-154 crew decided to treat the ATCo instruction to descend as mandatory, thereby rejecting the RA command to climb coming from the TCAS. The crew held a brief discussion about this discrepancy and made a decision which was further exacerbated by the subsequent instruction to descend from the controller. The repetition of the ATCo’s decision was the result of the lack of confirmation of earlier instructions. It can therefore be assumed that if the crew had not considered the conflicting commands and instead immediately notified the controller of the TCAS command, he would have become aware of the danger. A recommendation to notify the flight controller about a TCAS command is included in the TCAS operational manual.

3. The activities of the Tu-154 flight crew were determined to some extent by their anticipation of the future. The crew expected to descend, since that was provided by their flight plan. Therefore, the received instruction to descend was obvious to them, and this explains why they treated it as more important than the TCAS advisory, especially since the earlier radio correspondence between the Tu-154 crew and the ATCo left no doubt that the controller was aware of B757 aircraft presence on the same flight level.

4. Tu-154 crew operated in a multi-person environment. There were five crew members. The pilot flying (PF), who was seated in the left seat, was subjected to the procedure of control (supervision) during the flight, which was performed by the instructor (pilot not flying (PNF)), who also served as a pilot in command (PIC) of the aircraft and was seated in the right seat. The navigator was seated behind them. In the third row were the co-pilot (CP) and the flight engineer. In fact, the PIC made decisions, including the decision to descend, against the TCAS instruction. This was against the rules, as the PF should have made the decisions. At the same time this confirms the lack of adequate cooperation among the crew members because only one of the crew members (the CP who should be a commander but had no particular function in the flight) attempted to challenge this decision.

5. It was an obvious logical error to adopt that the ATCo instruction was superior to the TCAS resolution advisory. This error was supported by the lack of proper training. It goes without saying that the TCAS command to climb in one of the aircraft is coupled with the command to descend in the other. The Tu-154 crew heard the ATCo command contrary to their TCAS instruction but did not hear the analogous command directed to B757. If such a command for B757 had been issued it would have been heard by both crews on the radio. Thus it was obvious that the B757 crew would proceed as was suggested by the TCAS. Following the ATCo’s command by the Tu-154 flight crew could not effectively lead to a solution of the conflict.

6. The (BFU, 2004) report contains an air carrier’s declaration that the Tu-154 crew has completed all required training sessions in a timely manner. So the causes of improper demeanour should be sought mainly in training methods. Flight simulators used in Bashkirian Airlines were not equipped with TCAS. It was not possible to train crew members to make practical use of this system. Furthermore, according to Bashkirian Airlines, in the last 6 months prior to the accident the pilots had not been faced with TCAS occurrences. The pilots knowledge in this regard came only from training based on the literature. Therefore, assuming good theoretical training of pilots, we can conclude that they had knowledge but they lacked skills.
5.4. Analysis of errors/contributing factors from the ATCo

1. The air traffic controllers violated the principle set out by the rules that the position should be operated by two controllers. This rule was violated many times in a repetitive manner. It can be determined that on the day of the accident this error was committed by both controllers, as the situation that one of them went to the restroom was agreed upon and accepted by both of them.

2. The controllers did not use the full capabilities of a supplementary air traffic management support system in the form of flight progress strips. Their analysis would have allowed to easily find that the aircraft were on collision trajectories. This analysis did not take place because there was no record of collision on the strips.

3. The ATCo on duty devoted most of his attention to A320’s landing in Friedrichshafen. This was not a mistake because the operations manual dictated such a course and it was necessary because the approach to Friedrichshafen airport with radar control is complicated and any disruption in communicating instructions concerning necessary maneuvers to the landing aircraft can result in the situation when continuation of the approach is not possible. The report (BFU, 2004) explicitly states that: “The radar control to the final approach requires the unrestricted attention of the air traffic control officer. Even the shortest delay in the assignment of headings may result in an airplane position from which an approach is no longer possible”. Additionally, to service the A320, the controller had to divide his attention between two monitors at two workstations. Such kind of engagement may be described as “very busy”. In such cases, the controllers may lose situational awareness of other events. Distracting the controller’s attention by other aircraft in the sector was a factor contributing to his not noticing the collision situation. A similar example can be found in (Lower et al., 2016) concerning the air incident at Chopin Airport in Warsaw. In this aviation event, the controller was busy with a landing helicopter and did not notice the possible collision of two aircraft taking off simultaneously. The role of this factor was significantly increased by the lack of a second controller who could have handled the A320 aircraft as well as by the already discussed communication problems.

4. The controller did not hear the warning sound emitted by the STCA system. He was busy mainly with observation of the radar display and activities related to voice communications, thus he was not concentrated on the reception of sound stimuli. A fully functional STCA system, generating also visual warnings, would probably have allowed the controller to figure out that a conflict situation was taking place.

5. The ATCo did not properly assess the actual distance between the Tu-154 and B757 aircraft. Both aircraft occupied the same strips. Their analysis would have allowed to easily find that a conflict situation was taking place. If so, he should have been aware that his instructions could be in conflict with the TCAS resolution advisory.

5.5. Analysis of errors/contributing factors from the TCAS

1. The TCAS systems installed in both aircraft fulfilled the standards of second generation version 7.0 and worked exactly as designed. Thus it is difficult to talk about an error, however, an imperfection of the algorithm was clearly revealed. It concerned the case when one of the aircraft responded correctly to the RA message and the other did not. This situation may have been a result of a message perception problem or the failure of the control system which prevented proper operation. In this case the aircraft whose crew was able to react properly should have received reversed TCAS indications which could have prevented the accident. Such a change in the TCAS algorithm was implemented in its 7.1 version.

2. Activation of the TCAS had a degrading effect on the functioning of the ATC system. Both the TCAS and the ATC systems, acting independently, were able to prevent an accident. However, their combined action did not, because the recommendations they generated were contradictory. In this situation, the Tu-154 crew had no other choice - they had to act against the recommendation of one of these systems. If only one of them worked, such an action should be considered very unlikely. The essence of the problem lies in the fact that information about the RA generated in the aircraft is not automatically transmitted to the controller. He/she can only learn about this when informed by the pilot. Although it is recommended by the TCAS operations manual, such communication can be difficult, as was in the present case. Information about performing the maneuver as ordered by the TCAS was transferred to the controller by the B757 crew, but with a long delay due to the short-term absence of the co-pilot in the cockpit and the usage of a radio frequency dedicated for communication between the controller and the Tu-154 pilot. Efforts to eliminate this gap were made a few years later, however, there is still no complete agreement as to the reasonableness of such a procedure. There are also counter-arguments; the most important of these is the loss of independence of both systems.

6. STAMP-HFACS analysis of the Überlingen accident

This section presents application of the method to an analysis of the Überlingen air traffic accident. The thread of the incident related to the Tu-154 pilots is presented in more details. The assessment of causes and factors leading to the accident was developed using the adjudications of the (BFU, 2004) report. We also used complementary opinions from independent experts. We are referring to persons who were responsible for investigating aviation occurrences conducted by the Air Navigation Services Provider and Airport Operator at the request of the State Commission on Aircraft Accident Investigation. At the same time, they were the persons responsible for implementing Safety Management Systems (SMS) in these institutions. When coding factors using the HFACS method, the inter-rater reliability is very important (Ergai et al., 2016). The procedure of agreeing and accepting the coding is presented below. In the initial phase, the work was carried out in a three-person team (authors of the article). The procedure was as follows:

(a) A have created a list of potential factors and corresponding coding was generated.
(b) Each of the three team members assessed individually the presence of each factor (coding).
(c) Since the assessment involved a dichotomous response: yes (the given dependence/influence exists) and no (the given dependence/influence does not exist), only factors where two or more coders agreed moved to the next stage (at least 67% agreement).
(d) When all coders agreed, factor was accepted (100% agreement).
(e) When agreement was 67% (two out of three coders agreed), the three coders discussed each factor in an attempt to reach consensus.
(f) If consensus was achieved (100% agreement), the factor was accepted. If agreement remained at 67%, a fourth person (expert) was consulted. Factor was accepted if agreement reached 75%, otherwise it was rejected.

Analysis of this procedure indicates that the level of compliance necessary to accept the coding was not less than 75%. If two out of the three team members agreed, the expert’s opinion prevailed.

6.1. Identify the systems and hazards involved in the loss

The analyzed accident did not only have fatal consequences but it was also very complex in terms of the systems involved. The most significant of them was the air traffic control service ACC Zurich, in which we can distinguish important subsystems: air traffic controllers,
technical equipment, technical maintenance service and procedures used, and the management and supervision system, in this case performed by Skyguide. The second major system involved in the event is the Tu-154 aircraft of Bashkirian Airlines, for which we can distinguish the following subsystems: the crew, onboard anti-collision TCAS system and organizational system used by this air carrier together with the applicable procedures, training and selection of staff. The third system is the B757 DHL aircraft with a similar structure as the Tu-154 aircraft system. The indirect impact on the course of events was: the upper area control center UAC Karlsruhe and the international civil aviation legal and organizational system. The main hazard is a mid-air collision due to two aircraft operating at the same flight level.

6.2. Identify the system safety design constraints and system requirements associated with that hazard

The overall structure of the system ensuring the safety of air traffic is based on the following principles. Based on information about the
location of aircraft in the airspace coming from many different sources, the ATC support system creates a visualization that is displayed on the controller’s display. Along with the available flight plans, it is the basis for issuing clearances for aircraft to move in accordance with established parameters (speed, altitude, direction). The principles used in air traffic control are described in detail in document (ICAO, 2007). The most important of them, which were applicable in the present case, are as follows:

1. The air traffic controller (ATCo) provides so-called vertical separation between aircraft, which means that they move on fixed, different flight levels. The standard vertical distance between the flight levels is 1000 feet.
2. If it is necessary (preferred) that the aircraft fly on the same flight level, the controller maintains a horizontal separation expressed in units of distance or time of flight.
3. The airspace is divided into ATC sectors where responsibility is imposed on one person (executive controller). No other persons, in particular controllers of neighboring sectors, are entitled to give instructions to aircraft crews.
4. The primary means of communication between pilots and controllers is radio communication. All correspondence takes place in the same frequency band. This means that the controller responsible for the sector and also all aircraft under his/her control hear each other over the radio. At the same time they do not listen to other frequencies.
5. The transfer of control between the sectors is coordinated by the planning controller who is a member of the sector’s controller team. He/she uses fixed telephone lines for this purpose. Agreement usually comes down to determining the point (described in three dimensions) where the control is transferred. For operational reasons, sometimes bringing the aircraft to this point requires complex maneuvers.
6. The ATCo’s actions can be aided by collision detection and resolution (CD&R) systems. The most commonly used are two systems that differ in the time horizon of action – MTCD (Medium Term Conflict Detection) and STCA (Short Term Conflict Alert). When these systems detect a collision threat, they signal this by audible and visual signals.
7. In the event of a failure of the basic controller support system, as well as an auxiliary tool, flight progress strips (in paper or electronic form) are used. They allow for traffic situation awareness in case of loss of radar imaging.
8. The last element of the safety structure is the onboard TCAS system whose job is to detect a conflict and to recommend emergency maneuvers to pilots. TCAS systems operate completely independently of the other elements of the air traffic safety structure.

6.3. Construct the safety control structure as it was designed to control the hazard and enforce the safety constraints

The basis for determining the safety control structure is mutual communication between the above-mentioned systems and the rules and procedures for cooperation and supervision. The overall safety structure is shown in Fig. 2.

6.4. Determine the proximate events leading to the loss

The factors directly leading to the accident are arranged in the following sequence (BFU, 2004):

1. The controller allows two aircraft to occupy the same flight level with collision courses without providing vertical separation.
2. The Tu-154 pilot acts contrary to the collision resolution advisory of the TCAS by performing a descent instead of a climb maneuver.

6.5. Determine why physical control was ineffective in preventing the event

With regard to the first of the major causes of the accident, it can be determined that it resulted from the controller’s lack of situational awareness. This situation was caused, on the one hand, by a lack of concentration due to small traffic followed by a rapid increase in the workload associated with the need to service the A320. On the other hand, the lack of situational awareness resulted from only partial functionality of the controller support system (STCA). With regard to the second main cause, it can be stated that the ineffectiveness of the related safety barrier (TCAS system) resulted from deficiencies in the training of the Tu-154 crew, and also from a lack of clarity in the system of regulations and international standards. In point 6.6 it will be shown how STAMP-HFACS diagram is created. In this paper, the second cause only has been selected to be analyzed.

6.6. Moving up the levels of the safety control structure, determine how and why each successive level contributed to inadequate control in the lower level

(a) For each system safety constraint, determine whether the responsibility for enforcing it was assigned to a component in the safety control structure or if (a) component(s) obtained adequate control to ensure their assigned safety constraints were enforced in the components below them.

Generally speaking, incorrect operation (control) occurred in the control system of ACC Zurich (in all subsystems mentioned before) and in the Tu-154 aircraft (also in all subsystems, including the TCAS, which was working correctly technically but was not sufficiently protected from having the crew override its commands). Additionally, poor communication and coordination favored the occurrence of the accident.

The crews of both the Tu-154 and B757 aircraft were responsible for proper use of the safety barrier provided by the TCAS. They were the executive components implementing safety procedures within the whole safety structure. With respect to flight crew B757, it can be concluded that their performance was correct, while the Tu-154 crew’s performance was incorrect.

In Fig. 3 the light-red rectangles correspond to STAMP control or feedback errors.

(b) Develop an understanding of all human decisions or flawed control actions in terms of: information available to the decision maker, required information not available, behavior-shaping mechanisms (e.g., the context and influences on the decision-making process), the value structures underlying the decision, and any flaws in the process models of those making the decisions and why those flaws existed.

Incorrect operation of the “Tu-154 crew” component had several causes and contributing factors. These have been discussed in detail in Section 5.3. Summing up, it can be stated that there was excessive information in the form of two conflicting commands (TCAS and ATCo). The context in which the wrong decision was made can be described as problems in crew cooperation and lack of training. These problems have been included into the category of violation of supervision
Fig. 3. STAMP-HFACS diagram for errors and contributing factors of Tu-154 Crew and TCAS.
procedures. The crew was poorly selected, which violated the decision-making structure (wrong professional relations) and increased the probability of making a wrong decision (deficiencies in training).

‘b’ is decomposed into four steps b) 1. - b) 4.

b) 1. Select all such components of the safety control structure that contain a human factor,

In Fig. 2 the components: Tu-154 crew, B757 crew, ATCo 1, ATCo 2, Management of the ATC in Zurich, Bashkirian AirLines, and International provisions contain human factors.

b) 2. For each component selected in point b) 1, choose such levels of the HFACS structure that will be included in this component,

Each of the Aircraft Crew and Air Traffic Control models is composed of HFACS Levels 1 and 2 as the Tu-154 Crew model in Fig. 3. The environmental factors (physical and technological) of Level 2 are located outside of these models. Levels 3 and 4 can be located in one component or distributed over different components of a system, see International provisions: Training systems and Guidance for pilots, Bashkirian Airlines in Fig. 3. The DOD HFACS Version 7.0 taxonomy is given in (DOD HFACS, 2016, p. 22) and repeated in Fig. 5 in Appendix A of this paper.

b) 3. For each level chosen in point b) 2, select its categories and the factors associated with these categories that should be considered in the incident analysis, and add human factors that are not included in the HFACS but are associated with analyzed event,

In Fig. 3 the green rectangles correspond to error categories in the HFACS framework that are associated with this accident.

b) 4. Add how the factors of the HFACS categories, and human factors that are not included in the HFACS but associated with the event influence the other factors for:
– interactions between components,
– influence inside the component,
– and assign the semantics of errors for the analyzed event to the components’ properties.

The dependencies between factors analyzed below are represented as token arcs with numbers 1–8 in Fig. 3. In order to represent these dependencies in A-CAST software tool notation (Abdulkhaleq, 2015), the following notation will be introduced. The HFACS factors are interpreted as properties of the STAMP safety control structure with identifier of the form $C_{P,i}$ where (see Fig. 4):

- $C$ - component, $C \in \{IPTSGPM,BAL,Tu-154C,...\}$, the meaning of abbreviations is given in next two paragraphs,
- $P$ - property type $P$ of the component $C$, $P \in \{SRR,CDM,UDCA,PMF\}$,
- $i$ - index of the property type $P$ of the component $C$.

Abbreviations will be introduced in the notation for the dependencies between factors. For selected components in Fig. 3, the following abbreviations are used:
– International provisions: Training systems and Guidance for pilots, ATC Management Systems - IPTSGPM,
– Bashkirian Airlines - BAL,
– Tu-154 Crew - Tu-154C.
For the property types of a component of the STAMP safety control structure, the following abbreviations are used:

- Safety-Related Responsibility - SRR,
- Context in which a Decision was Made - CDM,
- Unsafe Decision or Control Action - UDCA,
- Process Model Flaw - PMF.

The above abbreviations are used in the notation according to Fig. 4.

The HFACS factors in their context are characterized as follows:

identifier = \{semantics\},

e.g. IPTSGPM_UDCA_2 = \{SI004 Failed to Provide Appropriate Policy/Guidance, i.e. the lack of operation description when the TCAS RA and ATCo command are inconsistent\}

The HFACS factor identifiers are created in the following manner. According to the legend below the STAMP-HFACS diagram in Fig. 3, the small squares indicate the property type that a HFACS factor is assigned to, e.g. OP002 and SI004 of IPTSGPM are UDCA property type, while SI003 of BAL is PMF and SI008 of BAL is UDCA. Examples of the HFACS factor identifiers inside their contexts are (see Fig. 4): IPTSGPM_UDCA_3, IPTSGPM_UDCA_2, BAL_PMF_1, and BAL_UDCA_2, respectively. For the component C, there can be more than one property P of given type, e.g. SRR, CDM, UDCA, and PMF, so the P is indexed as P_i, e.g. UDCA_2.

Sometimes, the factors are aggregated by logical and operators. Hence, new properties are defined (see Fig. 3), e.g.

\[ \text{BAL_CDM}_1 = \{\text{IPTSGPM_UDCA}_2 \, \text{and} \, \text{IPTSGPM_UDCA}_4\}, \]

where BAL_CDM_1 is the context in which BAL decision made.

1. A few years earlier a similar accident took place in Japan. The circumstances were identical. The pilot acted as instructed by the controller instead of following the instructions of the TCAS. No conclusions were drawn that would have resulted in adequate changes in international air traffic.

The following HFACS factors inside their context are introduced:

\[ \text{IPTSGPM_UDCA}_1 = \{\text{OP003 Provided Inadequate Procedural Guidance or Publications}, \text{ i.e. the lack of procedural description that RA from TCAS has higher priority than the ATCo command}\}, \]
\[ \text{IPTSGPM_UDCA}_2 = \{\text{SI004 Failed to Provide Appropriate Policy/Guidance}, \text{ i.e. the lack of operation description when the TCAS RA and ATCo command are inconsistent}\} \]

Therefore, IPTSGPM_UDCA_1 influenced IPTSGPM_UDCA_2.

Additionally, let the following factors be used (see Fig. 3):

\[ \text{IPTSGPM_UDCA}_3 = \{\text{OP002 Organizational Program/Policy Risks not Adequately Assessed}, \text{ i.e. the policy of risk assessment was not sufficiently sensitive}\}, \]
\[ \text{IPTSGPM_UDCA}_4 = \{\text{SI007 Failed to Identify/Correct Risky or Unsafe Practices}, \text{ i.e. lack of awareness and response to the threat posed by the lack of operation description when the TCAS RA and ATCo commands are inconsistent}\} \]

Therefore, IPTSGPM_UDCA_3 influenced IPTSGPM_UDCA_4.

In Fig. 3, the two influences as mentioned above are represented by the dashed arc from the rectangle with the label (14) Policy & Process Issues ... to rectangle (13) Inadequate Supervision ... of the component International provisions ... . Symbol \( i \), where \( i \in \{1,2,3,4\} \), denotes HFACS level \( i \).

2. No precise and clearly defined superiority of TCAS commands over the controller's instructions resulted in the fact that in some countries pilots were not properly trained.

\[ \text{BAL_CDM}_1 = \{\text{IPTSGPM_UDCA}_2 \, \text{and} \, \text{IPTSGPM_UDCA}_4\} = \{\text{SI004 Failed to Provide Appropriate Policy/Guidance, i.e. the lack of operation description when the TCAS RA and ATCo command are inconsistent}\} \, \text{and} \, \{\text{SI007 Failed to Identify/Correct Risky or Unsafe Practices i.e. lack of awareness and response to the threat posed by the lack of operation description when the TCAS RA and ATCo commands are inconsistent}\} \]
\[ \text{BAL_PMF}_1 = \{\text{SI003 Failed to Provide Proper Training, i.e. the lack of training issues when the inconsistency between the TCAS RA and ATCo commands occurs}\} \]
\[ \text{BAL_CDM}_1 \text{ influenced } \text{BAL_PMF}_1. \]

Despite the incident in Japan, training programs did not include the situation when the commands of the ATCo and TCAS RA were inconsistent. This was due to unidentified hazards of such situation. Therefore, in Fig. 3 the solid arc from the component International provisions ... to the component Bashkirian Airlines is labeled by Unidentified hazards.

3. BAL_UDCA_1 = \{SP002 Inappropriate Team Composition\} is explained as follows. As a result of organizational decisions, professional relationships (which should guarantee adequate internal supervision) were violated in Tu-154. The first pilot (PF), due to his position in the airline management, was in fact a superior of the second (PFN, PIC) and third (CP) pilot. At the same time the second pilot (PFN, PIC) served as an instructor, and supervised and evaluated the work of the first pilot (PF). Finally, the third pilot (CP) was the first officer and should be a commander of the aircraft, however, during this flight he had no particular task.

\[ \text{Tu-154C_PMF}_1 = \{\text{PP101 Failure of Crew/Team Leadership and PP104 Rank/Position Intimidation}, \text{ i.e. it was not exactly clear who was in command, and who had to make decisions and plan tasks for the crew members; formal differences in the position (rank) of the crew members in the organization (Bashkirian Airlines) reduced their ability to efficiently perform ongoing tasks}\} \]
\[ \text{BAL_UDCA}_1 \text{ influenced } \text{Tu-154C_PMF}_1. \]

The STAMP analysis shows inadequate control actions. The management of Bashkirian Airlines did not notice a danger in the control actions (unidentified hazards) which resulted from this state. Therefore, the solid arc from component Bashkirian Airlines to component Tu-154 Crew is labeled as Unidentified hazards.

4. On the basis of the pilots' conversations and lack of adequate cooperation among the crew members, it can be noticed that there was mental discomfort resulting from unclear professional relationships. The resulting situation can be classified at Level 2 as State of Mind, specifically PC205 Personality Style.

\[ \text{Tu-154C_CDM}_1 = \{\text{PC205 Personality Style}, \text{ i.e. mental discomfort resulting from unclear crew relationships among pilots}\} \]
\[ \text{Tu-154C_PMF}_1 \text{ influenced } \text{Tu-154C_CDM}_1. \]
5. Tu-154C_{CDM\_3} = (PC109 Technical or Procedural Knowledge Not Retained after Training reinforced by PC105 Negative Habit Transfer, i.e. the situation that occurred was a new phenomenon which went beyond skills that had been practiced)

\textit{BAL\_PMF\_1} resulted in Tu-154C_{CDM\_2}.

The STAMP analysis shows inadequate control action. The relationship shown in Fig. 3 concerns the third and second levels of HFACS. As such, it describes the negligence not so much in the training process itself. The inadequate control action resulted from an inappropriate training model (\textit{Process models that are inconsistent or incorrect}, see the solid arc from \textit{BAL} to Tu-154C) and more specifically in the scope of the training that had been adopted by Bashkirian Airlines management system.

Tu-154C_{CDM\_3} = (PC110 Inaccurate Expectation caused by the following reasons. A rational analysis of reality was hindered by mental discomfort resulting from unclear relationships among pilots. The logical dependencies leading to the correct decision were unnoticed by the crew of Tu-154. It should be noted here that the Tu-154 crew had information which could have logically led them to the right choice. They should have known that the TCAS in B757 issued a command to descend and there was no other command changing it. The actions of the Tu-154 crew were, to a certain extent, the result of predicting the future based on routine activities. They expected to receive an instruction to descend, as so provided their flight plan)

The STAMP analysis shows inadequate control actions; more precisely, it could be defined as \textit{Unidentified hazards}, see the solid arc from \textit{BAL} to Tu-154C in Fig. 3.

\textit{BAL\_UDCA\_2} = (SI008 Selected Individual with Lack of Proficiency, i.e. the crew was not sufficiently prepared when the TCAS RA and ATCo commands are inconsistent) Tu-154C_{CDM\_1} and \textit{BAL\_UDCA\_2} influenced Tu-154C_{CDM\_3}.

6. Tu-154C_{UDCA\_1} = (AE107 Rushed or Delayed a Necessary Action – more precisely, a fairly long analysis of the situation was conducted by the pilots. It can be expected that their response should have been much faster. The responses and actions of pilots can be much faster and even automatic thanks to their experience. Regarding the proper response to TCAS alarms, it is difficult to gain experience only through many years of practice. This is due to the fact that many years of professional work not necessarily means that the pilots respond to TCAS alarms frequently. In addition, the TCAS system was then a relatively new system. Therefore, the only possibility to acquire necessary skills in this field was practical training on simulators. In this case the Tu-154 pilots did not attend such training. Thus, according to the HFACS methodology we assumed that poor training of the pilots led to their lack of necessary reflexes. It is also possible that pilots reacted slowly because they did not know how TCAS works. However, the report (BFU, 2004) shows that TCAS training had a theoretical character in Bashkirian Airlines and all of the pilots knowledge about the TCAS system came from training based on the literature. As a result, it appears that the problem with the improper operation of the pilots was related to lack of skills rather than lack of knowledge)

Tu-154C_{CDM\_2} and Tu-154C_{CDM\_3} influenced Tu-154C_{UDCA\_1}.

7. Tu-154C_{UDCA\_2} = (AE202 Failure to Prioritize Tasks Adequately with the following semantics. It can be assumed that the new circumstance during the flight was not standard for the pilots. The reactions of the pilots were not instinctive and immediate. They began a relatively long analysis of the situation. According to the cited taxonomy, in the given circumstances the pilots made decisions based on the knowledge they possessed. In accordance with this knowledge the pilots should have informed the ATCo about the TCAS command when such a message appeared. This recommendation is contained in the operations manual of the TCAS system. The controller was not notified about the command of the TCAS system.) Tu-154C_{CDM\_2} and Tu-154C_{CDM\_3} influenced Tu-154C_{UDCA\_2}. Tu-154C_{UDCA\_3} = (AE201 Inadequate Real-Time Risk Assessment) Tu-154C_{CDM\_2} influenced Tu-154C_{UDCA\_3} Tu-154C_{UDCA\_4} = (AE206 Wrong Choice of Action During an Operation, which was manifested by decreasing flight level according to the ATCo instruction) Tu-154C_{CDM\_3} and Tu-154C_{UDCA\_3} influenced Tu-154C_{UDCA\_4} Tu-154C_{UDCA\_5} = (AE205 Ignored a Caution/Warning expressed as follows. The third pilot (CP), who had no particular function in the flight, attempted to challenge the wrong decision but the warning was ignored. In fact, he quickly withdrew from making any further attempts to defend his point of view because of his personality. It is possible that the “authority gradient” problem caused no reaction to the warning but the fact is that the existing warning was ignored.) Tu-154C_{PMF\_1} and Tu-154C_{CDM\_1} and Tu-154C_{CDM\_2} and Tu-154C_{CDM\_3} influenced Tu-154C_{UDCA\_5}.

8. Tu-154C_{UDCA\_6} = (AV002 Commits Widespread/Routine Violation with the following meaning. Three experienced pilots were present in the aircraft and were very well trained in the opinion of Bashkirian Airlines (one of them was an instructor) and none of the pilots tried to take appropriate action. Professional training of Tu-154 crew can be considered from two reference points. On the one hand, pilots took all the training required by the airline and, according to the air carrier's declaration, were well trained. On the other hand, the objective analysis of the scope of this training shows that, in comparison with other air carriers, the scope of the training offered and required should in this case be considered insufficient. Especially with regard to the TCAS system. Thus, with a global outlook on the problem, there are deficiencies in pilot training. The presented situation has even deeper consequences. The crew, who follows the rules learned in the training, is convinced that is doing the right thing. So if the same situation is repeated, it can be expected that the decision of the pilots will be the same every time - wrong. In the HFACS method, such a repetitive error is classified as routine)

Tu-154C_{CDM\_2} and Tu-154C_{PMF\_1} influenced Tu-154C_{UDCA\_6}

STAMP-HFACS approach is a multi-criteria decision making approach with categories and factors arranged in hierarchical structure. Hence, Analytic Hierarchy Process (Saaty, 1990) can be used when estimating the relative weights of factors.

\textit{Discussion of the STAMP-HFACS analysis results}

To show the advantages of using the concept of the STAMP-HFACS analysis, we will compare the results to those shown in Johnson’s (2004) report. It points to two immediate causes of the accident: the command to descend given to Tu-154 was too late and the maneuver was contrary to the generated TCAS RA. Johnson’s report also
deteriorating simultaneously with a lowering of the level of system
shown that the corresponding indicator, called RiskSOAP, had been
of the event is shown in (Chatzimichailidou and Dokas, 2015). It was
154 aircraft and Bashkirian Airlines. The lack of a clear de-

determines three systemic causes, but none of them is related to the Tu-
154 aircraft and Bashkirian Airlines. The lack of a clear definition of
superiority in TCAS commands in relation to the controller’s commands
was identified as having a significant impact on the course of the ac-
cident (recommendations 18/2002 and 16/2004). This is equivalent to
relation 1 in our STAMP-HFACS analysis. Recommendation 06/2004,
related to the pilots’ responses to TCAS resolution advisories, is
equivalent to relation 2. Recommendation 07/2004 concerns pilot
education and training to increase confidence in the ACAS and is si-

tural to our relation 5. However, there is some difference here, as re-
commendation 07/2004 is directed at ICAO, and our analysis identifies
the whole sequence of influences, i.e. starting at ICAO but also with the
strong role of Bashkirian Airlines. There are also two recommendations
directed at the Civil Aviation Authority of the Russian Federation. One
of them (14/2004) identifies the need to include ACAS scenarios in
training. This is included in our analysis in relation 6. The other re-

6.7. Examine coordination and communication contributors to the accident

Many of the erroneous control actions shown in Fig. 3, in the con-
text of the human factor, are related to processes of communication and
coordination. In a few cases we are dealing with irregularities, and in
others with a total lack of communication and coordination. In the
analyzed aspect of the accident there was a lack of communication in
the relation: Tu-154 crew – ATCo. It should be conducted in order to
inform the controller about the conflicting TCAS command. At the same
time, communication errors (internal interaction) occurred in the “Tu-
154 crew” component. Indeed, there was an exchange of comments
about the situation which did not lead to appropriate action.

6.8. Determine the dynamics and changes in the system and the safety
control structure over time that migrated the system to a higher risk

With regard to the two main causes of the accident (see Section 6.4),
a deterioration in the safety control structure in time can clearly be
observed. An increasingly deeper lack of the controller’s situational
awareness is observed, mainly due to a high workload and poor per-
ception of important signals. The Tu-154 crew’s decision-making
structure also degraded in the course of the event. In the first stage of
the accident the crew was aware of existing nearby traffic and correctly
considered the possible decisions. At a later stage, after the pilot had
made a wrong decision, no mechanisms that can restore the proper
functioning of the decision-making system were functioning. A detailed
analysis of the deterioration of situational awareness of the participants
of the event is shown in (Chatzimichailidou and Dokas, 2015). It was
shown that the corresponding indicator, called RiskSOAP, had been
deteriorating simultaneously with a lowering of the level of system
safety.

The above content concerns accident’s timeline. The deterioration
in the safety control structure in time should be analyzed in longer time
scale. Let us recall some conclusions from Section 6.6. The policy of risk
assessment in International provisions: Training systems and Guidance
for pilots, ATC Management Systems was not sufficiently sensitive. No
precise and clearly defined superiority of TCAS commands over the
controller’s instructions resulted in the fact that in some countries pilots
were not properly trained.

6.9. Determine the changes that could eliminate inadequate control in the
future and generate recommendations

With regard to the “Tu-154 crew” component, after analyzing the
errors in the process control, two recommendations can be formulated.

1. It is necessary to identify clearly whose commands are superior, i.e.
those of the controller or of the TCAS. Due to the global nature of
this problem it is necessary to solve it at the highest possible level
and in the framework of international regulations. As a result of this
accident this was done by the ICAO. This recommendation, how-
ever, can be extended. Other examples of possible discrepancies
between onboard and external commands or possible conflicting
commands from onboard systems, such as the TCAS or EGPRW
(Enhanced Ground Proximity Warning System) should be sought. To
eliminate the dependence marked as “1” in Fig. 3, it is necessary to
review air incident reports. To eliminate the dependence marked as
“2”, it is necessary to conduct a theoretical analysis based on the
specification of onboard equipment algorithms.

2. Situations when a person higher in the hierarchy of the institution
organizing the work of the component (in this case Bashkirian
Airlines) is a less important member of the crew (in terms of deci-
sion making) should be avoided. Such a situation cannot be com-
pletely eliminated. Examples are cases of training, for example, a
less experienced pilot as the aircraft commander. For such situa-
tions, however, clearly defined procedures are necessary, especially
in emergency or unusual situations.

7. Representation of the results of the analysis using the A-CAST
tool

A suitable software tool is required due to the complexity of the
analysis. A-CAST (Abdulkaleq, 2015) is an open tool which supports
the application of CAST and automates the activities of CAST accident
analysis. The A-CAST tool as a plug-in will be integrated with XSTAMPP
to assist safety analysis in performing CAST. In A-CAST there is a view
with the parties: Safety-Related Responsibilities, Context in which a
Decision is Made, Unsafe Decisions or Control Actions, and Process
Model Flaws of a component. The results of the STAMP-HFACS analysis
are stored in all of the above parts, except for the responsibilities.
First, let us consider the statement:

Tu-154C_CDM_4 influenced Tu-154C_UDCA_1.

The context Tu-154C_CDM_4 will be stored in the part Context in
which a Decision is Made of the Tu-154 Crew component, while Tu-
154C_UDCA_1 in the part Unsafe Decisions or Control Actions of the same
component. Additionally, the statement:

Tu-154C_CDM_4 influenced Tu-154C_UDCA_1

can be added to the part: Context in which a Decision is Made
or the statement:

Tu-154C_UDCA_1 was influenced by Tu-154C_CDM_4

can be stored in the part:

Unsafe Decisions or Control Actions.

Let us consider the result:

Tu-154C_CDM_1 and BAL_UDCA_3 influenced Tu-154C_CDM_3.
Tu-154C_CDM_1 and Tu-154C_CDM_3 will be put into the part Context in which a Decision is Made of the Tu-154 Crew component. BAL_UDCA_3 will be located in the part Unsafe Decisions or Control Actions of the Bashkirian Airlines component.

Additionally,

Tu-154C_CDM_1 and BAL_UDCA_3 influenced Tu-154C_CDM_3

or

Tu-154C_CDM_3 was influenced by Tu-154C_CDM_1 and BAL_UDCA_3

can be put into the Context in which a Decision is Made of the Tu-154 Crew component.

In order to build greater STAMP-HFACS diagrams, a plug-in for creating them is required.

8. Conclusions and future work

First, the limitations of STAMP and HFACS were discussed. The accident of a Coast Guard helicopter with four fatalities of its crew members was analyzed as a case study. In the accident a small Coast Guard boat strongly interacted with the helicopter. The main advantage of CAST (Causal Analysis using STAMP) was an emphasis on the system structure. This feature enables the analysis of inter-component interactions, i.e. control and feedback. The HFACS is not oriented at these interactions. Therefore, in the case study the analysis based on HFACS omitted many systemic aspects. However, when analyzing the expressive power of HFACS taxonomy, the taxonomy covered well the CAST findings for the above accident. HFACS contains a detailed classification of operator and management level errors with preconditions for operator errors. On the other hand, STAMP Individual and Organizational Error taxonomy contains positions oriented at human errors. However, this is a general taxonomy with a rather weak concentration on the classification of organizational errors and the physical and mental state of operators. Hence the goal of this paper was to combine the advantages of both approaches, i.e. to support STAMP Individual and Organizational Error taxonomies with the HFACS taxonomy.

Second, a new platform called the STAMP-HFACS was defined. The STAMP Individual and Organizational Error taxonomy was extended by the HFACS taxonomy. It was shown how the HFACS categories and factors should be incorporated into CAST schema. We showed how properties such as Unsafe Decision and Control Action, Process Model Flaw, and the Context in which a Decision is Made of the STAMP safety control structure can be partially expressed using HFACS categories and factors with detailed semantics. We showed how to represent mutual influence (the causal-consequence relation) among the above properties. Therefore, this is a contribution to the modeling of dynamics in STAMP.

The application value of the STAMP-HFACS approach was illustrated for one thread of the Überlingen mid-air accident. One of the main errors committed by the air traffic controller who supervised the airspace over Überlingen was approval to change the flight level of the DHL transport aircraft. This caused that this aircraft and Tu-154 were on collision courses. The influence of higher HFACS levels on lower levels was illustrated by the following components: International provisions: Training systems and Guidance for pilots, ATC Management System, Bashkirian Airlines, and the Tu-154 Crew. The example indicates how to incorporate four levels of the HFACS structure into the STAMP safety control structure. The analysis performed here showed a migration of the consequences of negligence at a higher system level to higher risk states and a decision error at a lower level. Additionally, errors on intermediate levels were shown. Our analysis allows to present whole sequences of influences that are not visible in other methods. In addition, many aspects of the analysis can be represented with much greater detail. However, the authors understand that testing of the new taxonomy with a thread of one accident is not sufficient for practical applications. More research is necessary to confirm STAMP-HFACS applicability in real accident investigation.

When compared with the STAMP approach alone, the STAMP methodology enriched by stratified HFACS improves the specification of human errors. The STAMP-HFACS methodology can express interactions between people, technical equipment, and the environment. It is not bound to an incident/accident events chain. The STAMP-HFACS also enables analysis of hidden factors, e.g. management errors.

From a practical point of view it is very important to conduct safety analyses proactively. The STAMP-HFACS approach as presented in this paper is one of the possibilities for carrying out the idea of proactivity. It allows for an analysis of a safety-related occurrence focused on finding some adverse relationships between the components, especially at higher levels of the HFACS methodology. Even if in a particular case they did not have a major impact on the event, they may have had a significant impact in another case. Proper recognition of these relationships, and especially their interpretation in system-theoretic terms related to specific components, can be of great importance for increasing the level of air traffic safety.

We outlined how to represent the STAMP-HFACS analysis results, i.e. the properties of STAMP components and the influences between them, in A-CAST tool which will be a plug-in for XSTAMPP. XSTAMPP is the software tool for STAMP. In order to build greater STAMP-HFACS diagrams, this work needs to be automatized and a software tool, e.g. another plug-in, for creating diagrams is required.

In the next stage of our work we will analyze other threads. These will include problems with the organization of maintenance work at ACC Zurich, the absence of one of the controllers, an improper algorithm of TCAS operation. It seems very important to analyze the impact of individual threads on one another, and the reinforcement or weakening of their effects.
Appendix A

See Fig. 5.

Fig. 5. DOD HFACS 7.0 taxonomy.

Source: DOD HFACS, 2016, p. 22.
Appendix B

See Table 2.

Table 2

<table>
<thead>
<tr>
<th>CAST Findings (Hickey, 2012, pages 107, 108)</th>
<th>How MAB Findings have cover the CAST Findings (partially based on (Hickey, 2012), pp. 114–116)) Comments</th>
<th>Interpretation of the CAST findings Using the DOD HFACS 7.0 Category (Factor)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequent occurrence of overcontrol/overtorque in nighttime hoisting operations</td>
<td>+ / − MAB did not address systemic factors It generally accepts risk</td>
<td>Performance-Based Errors (AEI04 Over-Controlled/Under-Controlled Aircraft/Vehicle/System)</td>
</tr>
<tr>
<td>The physical system does not provide adequate feedback and controls to the pilot to assist the pilot in safely executing nighttime hoisting operations</td>
<td>+</td>
<td>Physical Environment (PE101 Environmental Conditions Affecting Vision)</td>
</tr>
<tr>
<td>The pilot relies heavily on limited visuals and the altimeter to ensure that the approach/hover is conducted at a safe distance</td>
<td>+ / − MAB did not address more systemic factors</td>
<td>Technological Environment (PE202 Instrumentation &amp; Warning System Issues)</td>
</tr>
<tr>
<td>Due to:</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− inadequacies in the hoist system (e.g. the lack of a dynamic slip clutch),</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− lack of sensors on the hoist system resulted in inadequate feedback to the air crew regarding entangled status,</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− and communications (e.g. the inability of the boat crew to communicate directly with the air crew, resulting in sub-optimal control/feedback), CG-6505 and its crew were not able to adequately control the hoist system to prevent entanglement.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of capabilities (e.g. lighting) for ditching</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of standardized training of ditching procedures</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Lack of emphasis on Ditching &amp; Paramount Importance of Life Safety</td>
<td></td>
<td></td>
</tr>
<tr>
<td>The only required signature on the Standardization Visit Procedures Checklist is that of the Aviation Training Center Instructor Pilot. Additionally, the only required signature on the Search and Rescue Procedures Checklist is the unit’s instructor pilot. Failure to require the pilot under instruction and his/her chain of command (operations officer and commanding officer) to sign these forms results in inadequate accountability and transparency (e.g. control and feedback) with respect to pilot/aircrew proficiency and potential hazards/operational risks</td>
<td>−</td>
<td>Mental Awareness (PC109 Technical or Procedural Knowledge Not Retained After Training)</td>
</tr>
<tr>
<td>General lack of control and feedback in the management of existing capabilities (e.g. HH-65):</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Lack of formal periodic capability gap assessment (e.g. Operational Analysis) required/performed. Lack of review of minor mishaps to identify safety-related capability gaps.</td>
<td>+ / − MAB did not examine systemic issues resulting in failure to identify capability gap</td>
<td>Planned Inappropriate Operations (SP006 Performed Inadequate Risk Assessment - Formal)</td>
</tr>
<tr>
<td>− Lack of formal integration/standardization of helicopter operational capabilities across platforms.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Sponsor capability and requirements cataloging; Lack of systematic process for documenting existing system and sub-system capabilities and operational capability gaps.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>− Lack of Safety Advocacy to Address Known Risks: Rather than advocating correction/mitigation, the Aviation Safety Division generally accepted known aviation operational risks (e.g. nighttime hoisting operations).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insufficient sponsor (e.g. Office of Aviation Forces) and user group (e.g. aviation operators) involvement, including like platforms and interfacing capabilities during acquisition and modernization efforts</td>
<td>+</td>
<td>Policy &amp; Process Issues (OP007 Purchasing or Providing Poorly Designed or Unsuitable Equipment)</td>
</tr>
<tr>
<td>Insufficient involvement with industry regarding state of the market capabilities and procedures</td>
<td>−</td>
<td>Policy &amp; Process Issues (OP007 Purchasing or Providing Poorly Designed or Unsuitable Equipment)</td>
</tr>
<tr>
<td>Lack of standardized training (observation and reporting) of Crew Resource Management and Operational Risk Management programs through use of multiple training delivery sources, collateral duty program, and limited programmatic guidance. Lack of identification/cataloguing of operational risks and mitigating actions specific to operational procedures/conditions</td>
<td>− / +</td>
<td>Policy &amp; Process Issues (OP002 Organizational Program/Policy Risks not Adequately Assessed, OP004 Organizational (formal) Training is Inadequate or Unavailable, OP006 Inadequate Program Management)</td>
</tr>
</tbody>
</table>