

CZECH TECHNICAL UNIVERSITY IN PRAGUE
FACULTY OF TRANSPORTATION SCIENCES

Martin Dillinger

**Visualization of STAMP-based Safety
Analysis Outputs in the Aviation**

Diploma Thesis

2021

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta dopravní

děkan

Konviktská 20, 110 00 Praha 1



K621 **Ústav letecké dopravy**

ZADÁNÍ DIPLOMOVÉ PRÁCE (PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení studenta (včetně titulů):

Bc. Martin Dillinger

Kód studijního programu a studijní obor studenta:

N 3710 – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Vizualizace výsledků bezpečnostních analýz
v letectví dle modelu STAMP**

Název tématu (anglicky): **Visualization of STAMP-based Safety Analysis Outputs in
the Aviation**

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cíl práce: Navrhnout vizualizace výsledků bezpečnostních analýz dat získaných z provozu leteckých organizací pomocí modelu STAMP využitelných v systémech řízení provozní bezpečnosti v letecké dopravě.
- Analyzujte model bezpečnosti STAMP a metodiky, které z něho vychází
- Analyzujte současná řešení pro vizualizaci dat (tzv. safety dashboards) v letectví
- Vytvořte databázi vybraných událostí z leteckého provozu kompatibilní s modelem bezpečnosti STAMP
- Proveďte analýzu vytvořené databáze pro identifikaci klíčových ukazatelů bezpečnosti a navrhnete jejich vizualizaci
- Vytvořené řešení ověřte a vyhodnoťte



Rozsah grafických prací: dle pokynů vedoucího diplomové práce

Rozsah průvodní zprávy: minimálně 55 stran textu (včetně obrázků, grafů a tabulek, které jsou součástí průvodní zprávy)

Seznam odborné literatury: Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N., Thomas, J. STPA Handbook, 2018.
Leveson, N. CAST Handbook, 2019.

Vedoucí diplomové práce:

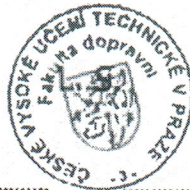
Ing. Andrej Lališ, Ph.D.
Ing. Slobodan Stojić, Ph.D.

Datum zadání diplomové práce: **17. července 2020**
(datum prvního zadání této práce, které musí být nejpozději 10 měsíců před datem prvního předpokládaného odevzdání této práce vyplývajícího ze standardní doby studia)

Datum odevzdání diplomové práce: **17. května 2021**

- a) datum prvního předpokládaného odevzdání práce vyplývající ze standardní doby studia a z doporučeného časového plánu studia
b) v případě odkladu odevzdání práce následující datum odevzdání práce vyplývající z doporučeného časového plánu studia

doc. Ing. Jakub Kraus, Ph.D.
vedoucí
Ústavu letecké dopravy



doc. Ing. Pavel Hrubeš, Ph.D.
děkan fakulty

Potvrzuji převzetí zadání diplomové práce.

Bc. Martin Dillinger
jméno a podpis studenta

V Praze dne.....17. července 2020



K621 **Department of Air Transport**

MASTER'S THESIS ASSIGNMENT

(PROJECT, WORK OF ART)

Student's name and surname (including degrees):

Bc. Martin Dillinger

Code of study programme code and study field of the student:

N 3710 – PL – Air Traffic Control and Management

Theme title (in Czech): **Vizualizace výsledků bezpečnostních analýz
v letectví dle modelu STAMP**

Theme title (in English): **Visualization of STAMP-based Safety Analysis Outputs in
the Aviation**

Guides for elaboration

During the elaboration of the master's thesis follow the outline below:

- Thesis goal: Propose visualization of the results of safety analyses from aviation operations data by means of STAMP model, usable within the aviation safety management systems.
- Analyze STAMP safety model and methods that are based on it
- Analyze the current solutions for data visualizations (safety dashboards) in the aviation
- Establish a database of selected aviation safety occurrences compatible with STAMP safety model
- Perform analysis of the established database for identification of key safety performance indicators and propose their visualization
- Validate and evaluate the proposed solution



Graphical work range: according to the supervisor's instructions

Accompanying report length: minimum of 55 pages of text (including figures, graphs and tables, which are part of the report)

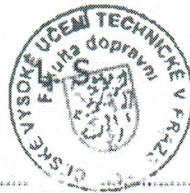
Bibliography: Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.
Leveson, N., Thomas, J. STPA Handbook, 2018.
Leveson, N. CAST Handbook, 2019.

Master's thesis supervisor: **Ing. Andrej Lališ, Ph.D.**
Ing. Slobodan Stojić, Ph.D.

Date of master's thesis assignment: **June 17, 2020**
(date of the first assignment of this work, that has be minimum of 10 months before the deadline of the theses submission based on the standard duration of the study)

Date of master's thesis submission: **May 17, 2021**
a) date of first anticipated submission of the thesis based on the standard study duration and the recommended study time schedule
b) in case of postponing the submission of the thesis, next submission date results from the recommended time schedule

doc. Ing. Jakub Kraus, Ph.D.
head of the Department
of Air Transport



doc. Ing. Pavel Hrubeš, Ph.D.
dean of the faculty

I confirm assumption of master's thesis assignment.

Bc. Martin Dillinger
Student's name and signature

Prague June 17, 2020

Poděkování (Acknowledgement)

Mé poděkování za odevzdání této diplomové práce patří zejména mým dvěma vedoucím práce, doc. Ing. Andreji Lališovi, PhD. a Ing. Slobodanu Stojícovi, PhD., kteří mi věnovali svůj čas při pravidelných konzultacích a vždy se mě snažili navést na správnou cestu k vyřešení nelehkých úloh praktické části. Děkuji taktéž své rodině za podporu, péči a umožnění studia na vysoké škole a mým přátelům za motivaci a naplnění studentských let zábavou.

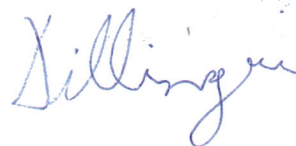
Prohlášení (Declaration)

Prohlašuji, že jsem předloženou práci vypracoval samostatně a že jsem uvedl veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Nemám závažný důvod proti užívání tohoto školního díla ve smyslu § 60 Zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon).

V Praze dne 9. srpna 2021

Bc. Martin Dillinger



Abstrakt

Cílem této diplomové práce je vizualizování dat získaných z analýz nebezpečí založených na systémovém kauzálním modelu STAMP. STAMP považuje provozní bezpečnost za dynamický problém řízení. Nehody se stávají v důsledku nedostatečného řízení nebezpečí. Řídící struktura by měla aplikovat omezení na procesy v systému, aby se předešlo nebezpečím. Práce vytváří databázi leteckých nehod a incidentů kompatibilní s modelem STAMP, za účelem analyzování provozních dat a návržení vizualizace. Výstupy z analýz nebezpečí jsou kvalitativní data, která je možné využít v leteckých organizacích. Práce navrhuje jejich grafické znázornění tím, že se zaměřuje na řídicí zpětnovazební smyčku a zkoumá její funkčnost. Výsledkem je „safety dashboard“, který zobrazuje nedostatky a vlastnosti řídicí smyčky a umožňuje jejich průběžné monitorování a sledování trendu. Zpracovaná data jsou vizualizována a interpretována, aby byl ověřen přínos pro systémy řízení bezpečnosti v letectví.

Klíčová slova

Bezpečnost, Safety dashboard, System-Theoretic Accident Model and Processes, Systém řízení bezpečnosti, Vizualizace kvalitativních dat

Abstract

The aim of this diploma thesis is to visualise the results of hazard analyses based on System-Theoretic Accident Model and Processes (STAMP). STAMP considers safety as a dynamic control problem. Accidents are caused by inadequate control over hazards. Control structure shall enforce constraints on system processes to prevent hazards. The thesis creates a database of air accidents and incidents compatible with model STAMP to analyse operational data and propose visualization. The outputs of STAMP-based hazard analyses are qualitative data, usable within aviation organisations. The thesis proposes their graphical representation by focusing on a control feedback loop and examining its functionality. The result is a safety dashboard that displays deficiencies and properties of the control loop and enables their continuous monitoring and providing trends. Processed data are visualised and interpreted to verify their contribution to aviation Safety Management Systems.

Key Words

Safety, Safety Dashboard, Safety Management System, System-Theoretic Accident Model and Processes, Visualization of Qualitative Data

Table of Contents

1	Introduction	11
2	Current Approach to Managing Safety.....	13
2.1	Historical Development of Safety Models.....	13
2.1.1	Era of Technical Factors.....	14
2.1.2	Era of Human Factors.....	14
2.1.3	Era of Organisational Factors	15
2.1.4	Era of Systemic Factors	16
2.2	Legislation	17
2.3	Safety Management in Aviation	19
2.3.1	Safety Management System (SMS).....	19
2.3.2	Safety Data Collection and Processing System (SDCPS).....	22
2.3.3	Safety Performance Indicators (SPI)	24
2.3.4	Safety Dashboard.....	27
3	Systems Theory	32
3.1	Systemic Approach.....	32
3.1.1	Reasons for New Paradigm	32
3.1.2	Properties of Complex Systems.....	34
3.2	Model STAMP.....	35
3.3	STAMP-based Analysis.....	38
3.3.1	STPA	39
3.3.2	CAST	42
3.3.3	Active STPA.....	43
3.3.4	STAMP-based Software	45
4	Assignment: STAMP-based Database	46
4.1	SBIT.....	46
4.2	Source of Data	48

4.3	Model of Processes	49
4.4	Data Processing.....	51
4.5	SBIT Dashboard	52
4.6	Results Interpretation	53
5	Assignment: Visualization of STAMP-based Outputs.....	57
5.1	Safety Outcomes from STAMP-based Hazard Analyses	57
5.2	Difficulties of STAMP-based Qualitative Data Visualization	58
5.3	Control Loop.....	59
5.4	Introduction to Proposed Solution	61
5.5	Source of Data	62
5.6	Data Transformation	63
5.7	Evaluation of Control Loop Elements	64
5.8	Evaluation of Control Loop Characteristics	66
5.9	Results of Control Loop Characteristics	71
5.10	Continuous Monitoring.....	73
5.11	Use of Proposed Method Based on SBIT Database	75
5.12	Practical Examples of STAMP-based Visualization and Interpretation.....	76
5.12.1	First Example – Controller Pilot.....	76
5.12.2	Second Example – Controller ATC.....	82
6	Discussion.....	84
6.1	Requirements for Performing Visualization	84
6.2	Limitations of the Proposed Method	85
6.3	Advantages of Visualization.....	87
7	Conclusion.....	89

Abbreviations

Abbreviation	Meaning
ADREP	The Accident/ Incident Data Reporting System
ASRS	Aviation Safety Reporting System
ATC	Air Traffic Control
BPMN	Business Process Model and Notation
CAST	Causal Analysis based on Systems Theory
ECCAIRS	European Co-ordination Centre for Accident and Incident Reporting Systems
FMEA	Failure Mode and Effect Analysis
FTA	Fault Tree Analysis
HAZOP	Hazard and Operability Study
ICAO	International Civil Aviation Organization
MIT	Massachusetts Institute of Technology
SBIT	STAMP-based Investigation Tool
SDCPS	Safety Data Collection and Processing System
SMS	Safety Management System
SPI	Safety Performance Indicator
STAMP	System-Theoretic Accident Model and Processes
STPA	System-Theoretic Process Analysis
TCAS	Traffic Collision Avoidance System

1 Introduction

Civil aviation belongs to high-risk industries. Aircraft move with high energy in environment with limited capacity. Despite challenges coming in hand with development of aviation industry, number of accidents steadily decreases on a long-term basis. Thanks to significant endeavour to improve safety, air transport is safer than road transport¹. Statistics prove that following motto “Safety First” is worth.

Requiring high level of safety in all fields of civil aviation persists and the motivation shall not decline because the system changes and develops quickly. Aviation is a sociotechnical complex system with wide hierarchical structure. As aviation experiences fast pace of development by using modern technologies, implementing software, and changing requirements, new hazards are occurring. Safety management must cope with all new difficulties.

Complex systems are hard to manage because they contain undesired interactions among their components. These interactions are characterised by emergent properties that are not satisfactorily handled by traditional safety models and methods. It is necessary to apply systemic approach across aviation organisations. New safety model and hazard analysis technique is needed to manage hazardous state of a system with potential leading to accident.

Researchers at Massachusetts Institute of Technology (MIT) developed System-Theoretic Accident Model and Processes (STAMP) and methods based on it. STAMP defines all safety related mishaps as a control problem and a lack of safety constraints. STAMP is an accident causality model that focuses on control structure, system design, and safety requirements. All deficiencies can be treated by sophisticated control structure that is enforced and updated whenever system tends to migrate toward state of higher risk.

Mission of this diploma thesis is to promote implementation of STAMP-based hazard analyses into aviation organisations. Using STAMP-based methods in operations is at its beginning. The goal of the thesis is to propose visualization based on outputs from STAMP-based analyses. The outputs are qualitative data which are preferred as a compact text for decision-making rather than statistics. The STAMP-based outputs are more about searching for system design errors and control structure deficiencies than predicting probabilities how likely is accident to

¹Significantly less passengers die of air accidents globally per year (around 500 casualties) than due to road transport accidents (around 1.3 million casualties).

[<https://aviation-safety.net/statistics/period/stats.php>]

[<https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries>]

happen. If the data are visualised, they can provide more arranged safety information and quantification enables continuous monitoring including providing trend lines.

Current Safety Management Systems are based on safety dashboards that display trends of specific occurrences and monitored precursors. This approach could be supplemented by safety performance indicators related to model STAMP and their visualization. Graphical results are better understood and interpreted by analysts. Such application could help to provide system requirements and safety constraints more effectively.

In this diploma thesis, STAMP-based database of aviation incidents and accidents is established to get acquainted what are the outputs of hazard analyses and which data may be monitored. Current STAMP-based safety dashboard is described which is followed by proposal of new visualization. Proposed visualization is validated based on data from established STAMP-based database. Interpretation of visualised outputs validates the utility of proposed solution for aviation organisations. Limitations and contributions of proposed method are identified and concluded.

2 Current Approach to Managing Safety

Safety is a crucial property of civil aviation in modern world. Aviation is a high-risk field of engineering as aircraft fly almost at the speed of sound at higher level of troposphere with pressurised cabin. There is also enormous number of flights in airspace as well as movements at airports. The capacity is limited, and operations demand complex infrastructure which is expensive to build and maintain. Heavy traffic and production pressure bring a lot of hazards. This requires professional approach to controlling risks and well-developed regulations.

Passengers take for granted that their lives aren't significantly threatened by boarding an aircraft. Aviation authorities require high level of safety and constantly monitor evolution of the system. The struggle to come even closer to so called "Vision 0" is immense and the effort to have decreasing trend lines of accidents and incidents in fast changing world is essential. However, this is a result of decades of development of safety models and learning from failures. Those outdated safety approaches and pieces of knowledge are still important nowadays, but they are not sufficient for current complex systems and modern technology as is used in civil aviation.

2.1 Historical Development of Safety Models

A long time ago, safety was not too important for population as there were no embedded techniques to control hazards. Lack of managing safety results in harm or loss. Deaths and injuries were quite common occurrences at workplace. In times of industrial revolution, injuries of workers meant production to stop or slow down. Failure of technology that harmed personnel started to be unacceptable since it was a reason to be less productive than competitors. It was a predecessor of eras of various factors that influence safety (see Figure 1).

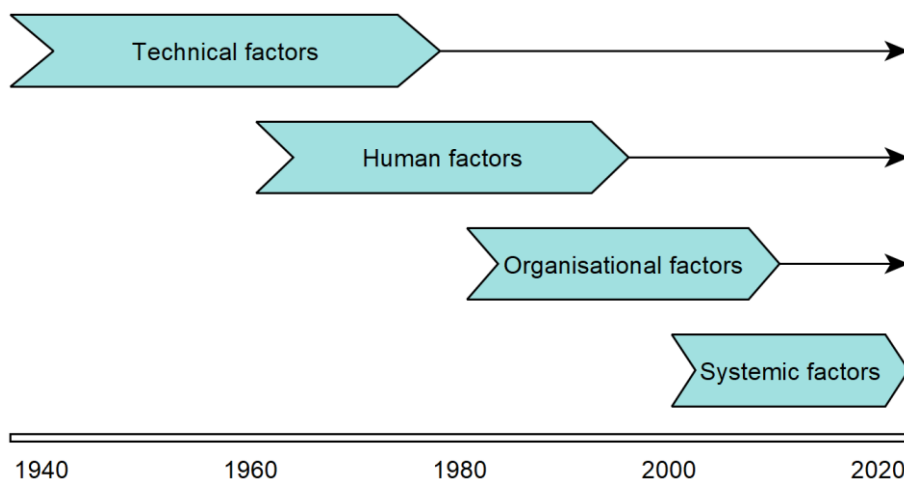


Figure 1 - Different approaches to managing safety throughout history

2.1.1 Era of Technical Factors

In the early stage of aviation, the goal was to make firm construction of an aircraft that is able to withstand various static and dynamic forces (aerodynamic, elastic, inertia). Together with moments that affect the aircraft's construction, steady structural design needed to be built at the time of limited technical solutions. Civil aviation required high reliability of the framework and control systems because aircraft contains a lot of mechanical elements that should not fail.

The Heinrich's Domino Theory states that accidents result from a chain of sequential events. One failure triggers following one and it leads directly to loss. If we remove a key factor (unsafe act), the sequence is stopped and failure is omitted. Heinrich also came up with a ratio between minor and major accidents that is usually valid. Heinrich's pyramid says that on 1 accident there is approximately 30 incidents and 300 near misses preceding the loss. It was an inspiration to focus on minor incidents in the future as well in order to diminish those mishaps. [1]

To evaluate risks and increase reliability of equipment, fundamental techniques originated. Risk is a potential leading to an accident. Risk is severity of the negative outcome combined with probability that negative outcome will happen. Failure Modes and Effects Analysis (FMEA) is a tool for assessing risk of a failing process. Severity, probability, and detectability are evaluated. The output is risk priority number that determines the importance of potential cause of mishap. Hazard and Operability Study (HAZOP) is another tool to identify and prioritise hazards in the system. The outputs from safety methods are arranged into hazard register and the risk is graphically represented in risk matrix. Category of the outcome is classified as acceptable or unacceptable.

Fault Tree Analysis (FTA) is a method specialised in component reliability. The analysis goes top-down through the tree and searches for predisposed weaknesses. The calculation shares a probability of each component to fail. Relative probability results show which component is most likely to not work as intended. FTA analyses the way from causes to failure, meanwhile Event Tree analyses the way from failure to consequences. The combination of both analyses is called Bow-tie method. Mentioned methods are still in use for evaluation of reliability of equipment or elements in a technical system.

2.1.2 Era of Human Factors

Research and more advanced technology made the technical system reliable. However, throughout the time it was found out that reliable system does not necessarily mean safe system.

There were several accidents where hardware and software worked as intended but the failure occurred due to human incorrect perception and mental model. Technique of Human Error Rate Prediction (THERP) thinks that it is possible to describe human behaviour in the same way as technology (similar to FTA). THERP calculates the reliability of human and likelihood of performing mistake.

It was observed that humans are not machines that are irreplaceable in monotonous activities, but human's quality is in making decisions. Human's performance is not perfect and so limitations of humans were depicted. Performance effectiveness is higher when human undergoes optimum stress. Human remains vigilant certain amount of time, after that monotonous work makes him tired. Regular practise training improves preparedness for emergencies. Human Cognitive Reliability (HCR) adds to mentioned findings that humans respond to unusual situations in time according to their knowledge, rules, and skills. The more practically-skilled is the person, the faster and appropriate is the response.

Conceptual model SHELL puts stress on misunderstanding between human and outer entities. The miscommunication usually arises from interface. Model SHELL describes flawed cooperation among human and software, hardware, environment, and liveware. Investigations of past accidents and researches in human factors revealed acceptable conditions in which workers should perform their tasks. This field is called ergonomics and it is about adjusting the system to human's performance and making working conditions more pleasant with understanding of human's physical and psychological aspects.

Swiss Cheese Model compares system defences to slices with holes which serve as protection against accident. Holes in the layers are drawbacks permitting "a trajectory of accident opportunity" to go through these defences. These latent conditions are hidden in the system and need to be covered by other safety barriers. The system shall be designed so to be able to stop active failure going through weakened barriers.

2.1.3 Era of Organisational Factors

Deeper research and analysis of findings led to the classification of the organisational factors which include the organisational culture and the operational context of a complex environment. Aviation industry started to understand that pilot is not the only one to blame. There is wide hierarchical structure above the actual processes that has the power to influence working

procedures and conditions and change system's routine. Management of a company and national or international regulators also share responsibility for safety. [2]

It happens that confusing rules and contradictory requirements come from diverse organisations due to not clearly stated interface between them. Overload of paperwork does not support dynamic air or ground processes involving strict time limitations. It is paramount not to have isolated point of view but to look at system extensively. AcciMap is a method for sociotechnical systems. Deficiencies arise at all levels of control hierarchy (organisation, authority) and actively contribute to accident.

2.1.4 Era of Systemic Factors

Systemic approach follows on from organisational factors. It is crucial to take system as a whole and not to decompose it into pieces by analytical reduction. This approach does not work in complex systems. System is comprised of many elements that interact among each other and older safety techniques are not able to detect these hardly predictable interactions. Processes in complex systems are dynamic non-linear and its properties coming from interactions are emergent. New models that cope with emergent properties are being developed. One of them is model STAMP (System-Theoretic Accident Model and Processes) used in safety engineering. This model characterises failures as control structure deficiencies and a lack of enforcement of safety constraints. Model STAMP is further described and used as a key safety model in this thesis.

Another novel approach is call Safety II. Safety II struggles to be more proactive and receives data not only from rare negative outcomes, but from day-to-day operations. By analysing much bigger amount of data, it is possible to achieve the target that as many processes go as well as possible. Safety II gives human into the foreground because it is the element that always solves the problem in some way by flexible and resilient behaviour.

Functional Resonance Analysis Method (FRAM) and Resilience Analysis Grid (RAG) try to strengthen the system by resilience to any deviation from stable position. Complex systems are filled with variable performances that interact and create resonance. Resonance is a phenomenon that could break the system. These methods endeavour to reduce mutual resonance and stabilise the system back to safety space. New system designed on the basis of Safety II shall comply with following capabilities: to react, monitor, learn, and anticipate.

The era of systemic factors comes up with complexity problems involving humans as well as technology. Especially Safety II has brought findings that shall not be underestimated. Human factors shall be considered as a symptom that needs to be investigated rather than a cause of failure. Human makes decisions most of the time and must balance between being effective (productive) and being thorough (safe). Personnel also cannot always follow stated rules and procedures thus deviates from theory and adjusts tasks (phenomenon called practical drift). Pilots should not lose situational awareness which is a key aid for them, and investigators shall avoid hindsight bias by putting themselves more in the pilot's shoes.

Findings mentioned above imply how extensive fields must be covered in safety, therefore Safety Management Systems (SMS) are being implemented in aviation organisations to cope with all the difficulties arising in complex high-risk sociotechnical systems. Importance of planning and updating system design sophisticatedly grows with the complexity of the system. Technology used nowadays much differs from times when systems were free from software and automation that increases complexity. More detailed reasoning about change in paradigm to managing safety of current systems and why systemic approach is crucial for safety engineering is described in Chapter 3 (Systems Theory).

2.2 Legislation

Aviation is highly regulated industry. The benefits of regulations are reflected in continuously decreasing rates of accidents. There is a guidance material Safety Management Manual (Document 9859) published by ICAO for creation of effective Safety Management System. Safety management seeks to proactively mitigate safety risks before they result in air accident or incident. Through the implementation of safety management, member states can manage their safety activities in a more disciplined, integrative, and focused manner. Possessing a clear understanding of its role and contribution to safe operations enables a member state, and its aviation industry, to prioritise actions to address safety risks and more effectively manage its resources for the optimal benefit of aviation safety. Safety Management Manual presents how aviation safety evolved and shares practical pieces of advice how to monitor the safety performance of the system and manage the risks. [3]

Implementation of Safety Management System (SMS) in the Czech Republic which is a member state of European Union is obeyed to European regulations, originated in European Union Aviation Safety Agency (EASA). European regulations gradually establish rules for aviation organisations to implement and develop SMS. The cornerstone for SMS establishment

is regulation 965/2012. Regulation 2018/1189 specifies common rules for safety management. Safety targets on a European level are stated by European Programme for Aviation Safety and European Plan for Aviation Safety more in detail.

In the Czech Republic, the regulation for aviation safety management is called L19. This regulation is based on Annexes to the Convention on International Civil Aviation Organization, specifically Annex 19. The regulation L19 is the latest Annex adopted from ICAO and it establishes the rules, obligations, and responsibilities to the Czech Republic and its aviation authorities and organisations. The regulation L19 emphasises the importance of managing safety in air operations and communicates the structure and function of Safety Management System and State Safety Programme. L19 was processed by Civil Aviation Authority of the Czech Republic and published by Ministry of Transport.

Experience has shown that accidents are often preceded by safety-related incidents and deficiencies revealing the existence of safety hazards. Safety information is therefore an important resource for the detection of potential safety hazards. In addition, whilst the ability to learn from an accident is crucial, purely reactive systems have been found to be of limited use in continuing to bring forward improvements. Reactive systems should therefore be complemented by proactive systems which use other types of safety information to make effective improvements in aviation safety [4].

Safety data should be categorised using taxonomies and supporting definitions to capture and store data in meaningful ways. Taxonomies and definitions establish a standard language and improve the quality of information and communication. They can also facilitate information sharing and exchange. Several types of taxonomies exist, such as the aircraft models, airports, and types of occurrences. [3]

The safety performance of the organisation should be demonstrable and should clearly indicate to all interested parties that safety is being managed effectively. One approach for demonstrating this is through a safety dashboard, which is a visual representation that enables senior executives, analysts, managers, and safety professionals a quick and easy way to view the organisation's safety performance. Member states of European Union should contribute to the improvement of aviation safety through the introduction of more proactive and evidence-

based safety systems which focus on accident prevention based on the analysis of all relevant safety information (see Figure 2). [4]

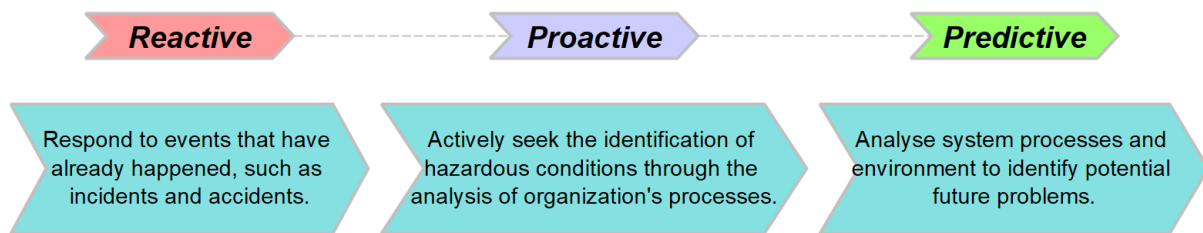


Figure 2 - Safety management strategies - the trend of assuring high level of safety is to discover new methods how to predict future negative outcomes [23]

2.3 Safety Management in Aviation

Safety management is an organisational function, which ensures that all safety risks have been identified, assessed, and satisfactorily mitigated. The objective of safety management in the aviation industry is to prevent human injury or loss of life, and to avoid damage to the environment and to property. Safety management is commonly understood as applying a set of principles, framework, processes, and measures to prevent accidents, injuries, and other adverse consequences that may be caused by using a service or a product. It is that function which exists to assist managers in better discharging their responsibilities for operational system design and implementation through either the prediction of system's deficiencies before errors occur or the identification and correction of system's deficiencies by professional analysis of safety occurrences. [5]

The strategy of reaching high level of safety sounds simple – to learn from previous failures in order to avoid repetition of similar failures in future. This approach works but predicting accidents is much more challenging because we must totally understand what is wrong. This is a reactive approach, the way how we usually investigate air accidents. Nevertheless, waiting for accident to happen is risky and ineffective way of compliance, therefore proactive activities like seeking for hazardous conditions and updating procedures are implemented. There are several regulating initiatives to implement safety management in aviation – Global Aviation Safety Plan at worldwide level, European Plan for Aviation Safety for countries of European Union, State Safety Programme at national level and Safety Management System at organisational level.

2.3.1 Safety Management System (SMS)

Safety means freedom from the risk of unacceptable harm. An integrated set of regulations and activities aimed at improving safety at national level is called State Safety Programme (SSP).

For ensuring safety in organisations there is a continuous process called Safety Management System (SMS). SMS is a systematic approach to managing safety, including the necessary organisational structures, accountabilities, policies, and procedures. SMS analyses impact of air operations on safety in various fields of aviation (aerodromes, maintenance, airlines, handling, air services). It records various data and sets acceptable level of safety. For SMS database, it is important to have reliable and objective inputs for processing data and receiving worthy safety information. [3]

Beside comprehensive safety oversight, SMS has following tasks on to-do list [6]:

- Continuously monitor and measure hazardous processes;
- Mitigate risks and set acceptable level of safety;
- Keep documentation of identified hazards;
- Establish a voluntary and compulsory safety reporting system²;
- Improve and support the entire safety culture.

Theoretically, 100% safe system would be static without any production (there would be infinite separation spacing to avoid potential conflict between aircraft). This system would not work because the goal of aviation is to be highly productive and to utilise all available capacity. The goal of earning money from endless productivity goes against safety intentions. This conflict is called 2P dilemma (protection against production).

² The key rule of being non-punitive in voluntary reports must be followed (to promote just culture).

Even though safety saves huge amount of money by preventing losses (active safety) and mitigating negative outcomes (passive safety), the costs for all the regulations, limitations, and other safety-related units are significant and diminish the competitiveness. High risk brings benefits as well as danger of major losses. For this reason, there are two levels, both defending different interest (see Figure 3). First level is Acceptable Level of Safety Performance stated by safety management and second level is Maximum Acceptable Cost per Operation stated by financial management. An organisation must maintain profitability to stay in business by balancing output with acceptable safety risks and the costs involved in implementing safety risk controls. Safety Management System creates acceptable level of safety. In the picture, we can also observe that level of safety is not dependent on production. There is a trend across Europe to provide the same level of safety (high and uniform) throughout all aviation activities not restricted by production volume. [3]

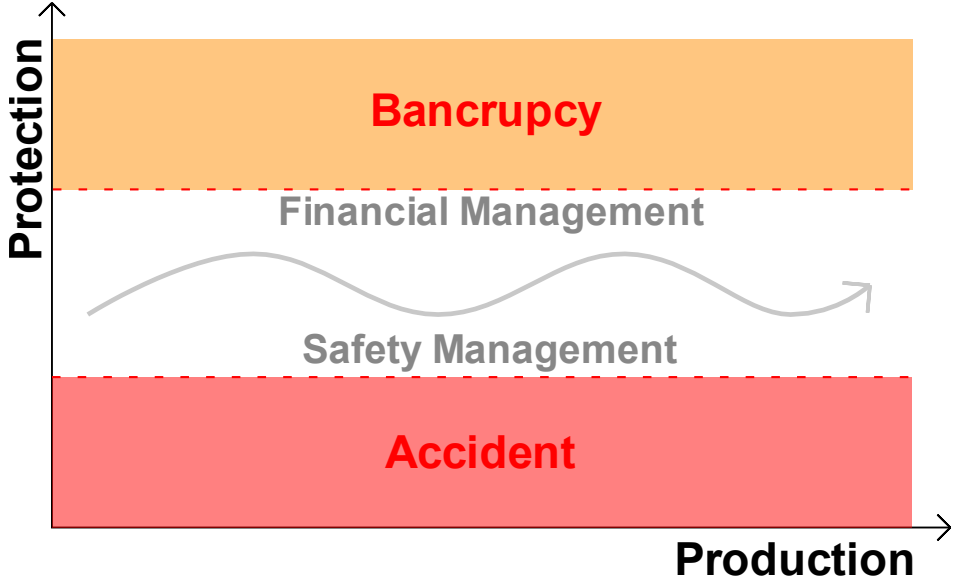


Figure 3 - Diagram of 2P dilemma shows safety space where the system operates; too low focus on safety means catastrophe and too high focus on safety means unacceptable costs

Safety Management System consists of four key elements:

- 1) Safety policy and objectives

It's the first important milestone of SMS implementation that defines the value of safety in the overall business and performance framework of the organisation. Ideally, the safety policy should confirm the organisation's commitment to safety and clearly indicate that safety is afforded highest priority in the service provision. This SMS element summarises obligatory legislative documents and shares responsibility for safety. Safety objectives are established as desired safety performance targets or triggers of non-compliance. [3]

2) Safety risk management

Risk management is an iterative process of identification, analysis, and elimination or of those hazards, as well as the subsequent risks, that threaten the viability of an organisation. The process of managing risks composes of describing the system, searching for hazards, assessing the risk, analysing the cause, and contributing factors and controlling the risk. The risk can be either eliminated or mitigated to an acceptable level (by reducing probability or severity). Safety measures need to be taken to comply with stated safety objectives. [3]

3) Safety assurance

Safety assurance comprises of all planned and systematic actions necessary to afford adequate confidence that a product, a service, an organisation, or a functional system achieves acceptable or tolerable safety. It demonstrates that organisational arrangements and processes for safety achievement are properly applied and continue to achieve their intended objectives. This SMS element assures safety oversight, collection of data, and management of change. [3]

4) Safety promotion

Safety promotion provides means, processes, and procedures ensuring that aviation personnel are trained and competent to perform their safety management duties. It plays the role in achieving effective control of safety risks and promoting positive safety culture across the system which educates personnel and consequently provides new source of safety-critical data from operations. [3]

2.3.2 Safety Data Collection and Processing System (SDCPS)

“You can’t manage what you can’t measure” said Lord Kelvin. Safety data collection and processing systems have allowed civil aviation to gain deeper understanding of operational errors. It makes it easier to answer the question why they happen and how to minimise them. Data and their correct interpretation are crucial for decision-making. It would be lost potential not to collect available data for management of organisation whether for safety, quality, or financial department.

Safety data is what is initially reported or recorded as the result of an observation, inspection, or measurement. It is transformed to safety information when it is processed, organised, integrated, or analysed in a given context to make it useful for management of safety. Safety information may continue to be processed in different ways to extract different meanings. The effective safety management is highly dependent on the effectiveness of safety data collection, analysis, and overall management capabilities. Having a solid foundation of safety data and safety information is fundamental for safety management since it is the basis for data-driven decision-making. Reliable safety data and safety information is needed to identify trends, make decisions, and evaluate safety performance in relation to safety targets and safety objectives, and to assess risk. It is required that service providers develop and maintain a formal process to collect, record, act on, and generate feedback on hazards in their activities, based on a combination of reactive and proactive methods of safety data collection. [3]

The importance of data is evident but current approach is focused mostly on negative occurrences in operations because deficiencies of the system are most visible and the evidence of lack of safety requirements is obvious. However, this predominantly reactive approach has disadvantage. At some point air transport can look so “safe“ (meaning that we are out of major accidents because we measure “unsafety”, not safety) that we do not have enough data to analyse real safety state and cannot reveal potential risks. This phenomenon is called safety paradox. To receive more data, we need to look into minor incidents and occurrences without safety effects. Organisations shall collect ordinary data from day-to-day operations as well, in order to be proactive and have information about its safety behaviour.

Reporting system shall be established to collect data from operational personnel that are directly in touch with processes. Obtained safety data shall be stored in safety database. Data should be ideally categorised using taxonomies and supporting definitions in order to better sort data to appropriate class in meaningful terms. Common taxonomies and definitions establish a standard language, improving the quality of information and communication. Captured information can be then shared, exchanged, and displayed in safety dashboard. An example of taxonomy in aviation is ICAO ADREP and ECCAIRS. SMS appreciates any kind of reports propagating different point of view on safety operations. SMS guarantees non-punitive approach and keeping the reporter anonymous in return. Those just culture fundamentals build better confidence in safety managers and promote safety culture.

Data quality shall be ensured by following criteria [7]:

- Validity – data collected are acceptable for its intended use;
- Completeness – no relevant data are missing;
- Consistency – The degree of consistency and error avoidance in the measurement of a given parameter can be reproduced;
- Accessibility – data are readily available for analysis;
- Timeliness – data are relevant for the period of interest and is available on a timely manner;
- Security – data are protected from inadvertent or deliberate modification;
- Accuracy – data contain no error.

Sources of safety data at level of organisation are [3]:

- Accidents and incidents final reports – conclusions about mishaps;
- Mandatory reports – reports of accidents and serious incidents;
- Voluntary reports – reports of inappropriate safety procedures;
- Inspections – observations of breaking the procedures;
- Audits – compliances with regulations;
- Sensors – automated measurement of data.

2.3.3 Safety Performance Indicators (SPI)

Safety performance is defined as a service provider's safety achievement that is specified by its safety performance targets and safety performance indicators. Safety performance management determines whether its activities and processes are working effectively to achieve its safety objectives by measuring and monitoring collected data. The measurement of performance is accomplished through the identification of safety performance indicators (SPIs). SPI is a data-based safety parameter used for monitoring and assessing performance. The SPIs approach to safety performance measurement aim is to increase the organisation's potential for an effective safety management which considers systemic and operational issues. Safety management struggles to push all operational risks under an acceptable level of safety performance. To reach desired safety performance, safety performance targets shall be established, and triggers shall be chosen. Safety triggers can help to reliably monitor real time safety status and control risks.

[3]

Data serving as SPIs can be qualitative or quantitative. Quantitative indicators relate to measuring by quantity and are preferred over qualitative indicators which are primarily descriptive because they are more easily counted. Quantitative indicators are ordinarily expressed absolutely as number of occurrences or relatively as a rate (occurrences per movements). Normalised measure of performance is better compared, and the information received is more accurate and valuable.

Quality data as an input for monitoring safety performance must be collected. In terms of safety management, the focus on clearly negative events should be considered with some caution, because [8]:

- In systems such as aviation with a low number of high consequence negative outcomes, the low frequency of such outcomes may give the wrong impression that the system is safe;
- The information is available too late to act on it;
- Counting final outcomes will not reveal any of the systemic factors, hazards, or latent conditions that have a potential to result in high consequence negative outcomes, under the same conditions;
- Where the resilience of a system has been undermined, such outcomes are more likely to occur by chance and therefore these outcomes may draw unwarranted attention and use scarce resources when they are not predictive of later events.

Indicators can be divided into two major groups according to time when the issue was observed (before, during, after mishap) – lagging and leading indicators (see Figure 4). Both types are worth to monitor although it is not simple to ensure their reliable collection. Those indicators measure either metrics that record safety events that have occurred or metrics that provide information on current situation affecting future performance. Lagging indicators are useful to

validate the effectiveness of specific safety actions and risk barriers or to support the analysis of information derived from existing leading indicators.

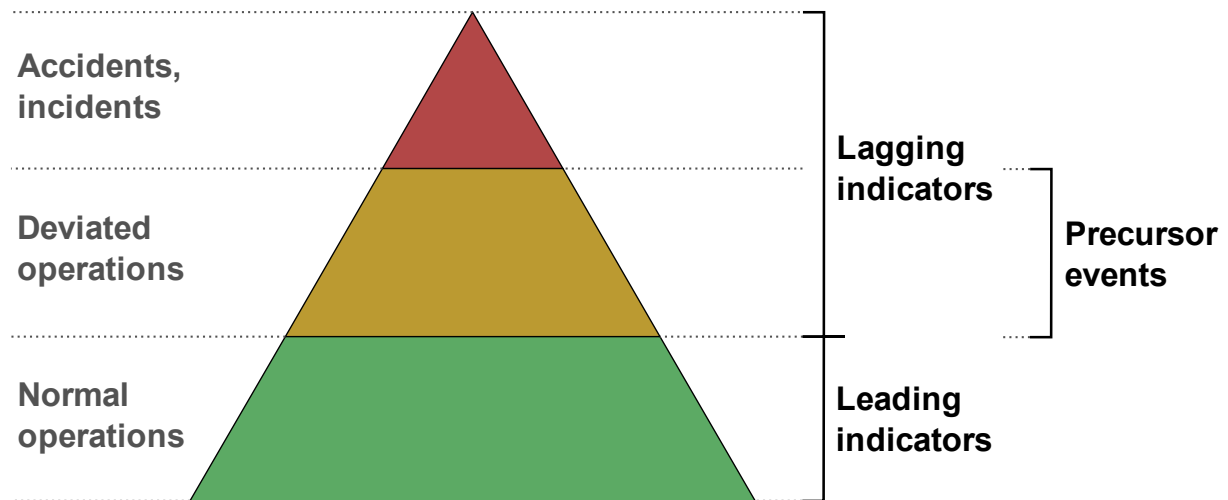


Figure 4 - Schematic pyramid of data that can be categorised as lagging or leading indicators [3]

Lagging indicators are reactive. They are easy to detect but hard to avert. Those occurrences are usually high severe and low probable. Precursor events indicate a potential for loss but are detected and controlled into safe state in time³. Precursors are considered as low-level system failures and are great means of caution for safety management. The advantages of lagging indicators are that their measurement is precise and the SPIs reflect actual safety performance in the past. By monitoring trends of safety occurrences, we may extrapolate future numbers and verify the existence of latent conditions. However, this assumption is valid only if there are no changes in procedures or no degradation of the system, which goes against the dynamics of aviation. The disadvantage is that we cannot predict potential hazards without experiencing accidents or serious incidents. As it is oriented on negative outputs, number of occurrences is limited.

Leading indicators are proactive. They are hard to detect and measure their impact on safety but easy to control. Leading indicators should measure both: things that have the potential to become or contribute to a negative outcome in the future (negative indicators), and things that contribute to safety (positive indicators). From a safety management perspective, it is important to provide sufficient focus on monitoring positive indicators to enable strengthening of those positive factors that make up company's safety management capability. They adjust safety priorities and the determination of actions for safety improvement.

³ For example: Number of unstabilized approaches

Examples of lagging safety performance indicators usually monitored at certified airports:

- Number of runway incursions;
- Number of runway excursions;
- Number of foreign object debris collisions;
- Number of wildlife strikes;
- Number of ground collisions;
- Number of ground handling service damages.

Examples of leading safety performance indicators:

- Percentage of pilots who underwent specific training;
- Frequency of safety meetings;
- Number of employees with more than five-year experience;
- Number of bird scaring activities;

2.3.4 Safety Dashboard

Safety performance monitoring is an essential component of aviation Safety Management System. Monitoring of safety can be compared to human immune system. In an SMS database, performance monitoring charts can pull data in real time to display the latest information to managers. [9]

SMS performance monitoring basically involves ongoing collection of safety data that indicates the health and progress of an aviation SMS implementation. It is also used to ensure that key safety goals are achieved. Aviation safety charts present SMS information to stakeholders. This enables stakeholders to make decisions about safety and business. The platform where relevant safety data are shared in well-arranged form is called safety dashboard. Safety dashboard is a visual representation that enables safety managers a quick and easy way to view the organisation's safety performance.

Sophisticated database and tool for safety dashboard should comply with following conditions [9]:

- User-friendly – crucial element to arrange the dashboard well in order to mitigate misinterpreting the information;
- Configurable – possible to change in time as the system evolves;

- Secure – resistant against unlawful threads coming from outside of the system;
- Full featured for a complete SMS – consisted of all elements that need to be measured and monitored;
- Easily accessed – using modern web-based technologies.

Safety dashboard presents statistical outputs visually. Essential characteristic is to be balanced and well-arranged. The dashboard must display all important data but it might not go too deep into detail otherwise safety manager, a person that will read the presented data and gain knowledge about current state of safety, will be overloaded. In order to offer a perspective of the system to the future, trend lines should be displayed. Linear trending is a statistical technique that calculates historical values and shows the trend (increasing or decreasing). Thanks to trend, safety manager can estimate following value in a specific time. The trend line should not count with for example number of incidents this month as the month is under way, the value is still rising and it has not been completed yet.

To visualise the data clearly and grippingly, charts (graphs) are used rather than long lists of values or large spreadsheets. International Civil Aviation Organization (ICAO) published a recommendation how to keep safety dashboard organised. According to the publication, a human looks at a graph for only 3 seconds and needs to grasp the information otherwise the focus is lost. It follows that the simpler the graph, the better. Providing too much information at one place can be as wrong as providing a lack of information. Human being cannot process all the received data in a short time unless the dashboard is intuitive and well-arranged. [10]

The following list presents the most important knowledge-based facts how to design a dashboard. Those tips should be followed to adjust the planned visualization for safety manager [10]:

- Always provide a description of the axes and a legend;
- Use only one unit per graph (avoid multiple vertical axes);
- Start the graph at 0 to avoid distortion (proportions between columns are not accurately represented);
- Do not use 3D visualization;
- Reduce number of pie charts and prefer single bar charts instead;
- If visualised data contain sequence, a line chart is a good option;

- If column labels are long, bar charts have better layout than column charts (horizontal rather than vertical);
- Stacking (a single category is represented in a single column one over the other) saves space of a dashboard, but the distribution could seem confusing;
- Moving averages and trend lines provide better understanding of the evolution of fluctuating data (data with significant volatility pattern);
- Data are better remembered if they are represented in a pleasant and attractive way.

A dashboard is a comprehensive collection and visualization of key statistics (performance indicators). A dashboard can be built using programming languages and specialised libraries, or by using off-the-shelf software products. A dashboard is composed of widgets that are placed into a grid. In a dashboard, following widgets can be used:

- Graphs;
- Meters;
- Numbers;
- Lists;
- Maps;
- Text;
- Clock.

A safety dashboard is fundamental tool for Safety Management System. Safety managers need to answer questions about the operations and a status of safety of the organisation. A safety dashboard shall reliably provide answer to them. The questions are [11]:

- 1) Are we safe?
- 2) Is there anything we should worry about?
- 3) Is there any action we should take?

Recommended practices during establishing a new dashboard are [11]:

- Think in terms of areas of interest rather than specific indicators;
- Keep a balance between reactive and proactive indicators;
- Do not be afraid of proposing changes to the dashboard content visualizations;
- Embrace a User-Centered Design⁴ approach and explore the needs of the end users.

⁴ User-Centered Design is an iterative process of adjusting a visualization to potential users.

There are four areas of interest that shall be a part of a safety dashboard oriented on aviation. These areas must be monitored preferably with leading and lagging safety performance indicators. General dashboard describes a state of safety in whole system. The four areas consist of specific points that should be taken into account during designing safety dashboard:

- 1) Operational safety (safety performance and following the targets)
 - Display 3 to 5 charts of leading/ lagging indicators that monitor safety occurrences;
 - Find contributing factors that drive those occurrences;
 - Show hotspots to see which units/ infrastructure is most affected;
 - Show highlights connected with temporary changes.
- 2) People and culture (reporting culture and attitude to safety)
 - Trend of reporting rate for safety occurrences;
 - Trend of reports on fatigue and overload situations;
 - Rate of participation on not mandatory training connected with safety and human factors;
 - Progress in enthusiasm on safety culture initiatives.
- 3) Technical system (health status of equipment)
 - Normalised trend of technical problems during operations;
 - Number of workarounds put in place by personnel to overcome technical issues;
 - Ratio between planned and unplanned maintenance interventions;
 - Trend of cumulated duration of technical issues.
- 4) Change management (how changes affect the safety)
 - Trend of corrective actions;
 - Status of ongoing change projects;
 - Important recommendations with implementation status;
 - Overview of forthcoming changes and their potential impact on safety.

Each chart can also include alert level area and target level area (see Figure 5). Alert and target criteria are stated in safety objectives (usually established by the organisation at the beginning of a season according to its safety policy). The former should be avoided, the latter should be achieved. An alert level is a value that is determined as a trigger of unacceptability. Alert can be set in more levels and shall inform the safety manager that stricter mitigating action must be provided. A target level shows the desired (or predicted) value as defined previously in safety

objectives. Alerts and triggers of safety performance indicators are a great tool how to control safety performance and how to adopt a mitigating action as soon as possible. [12]

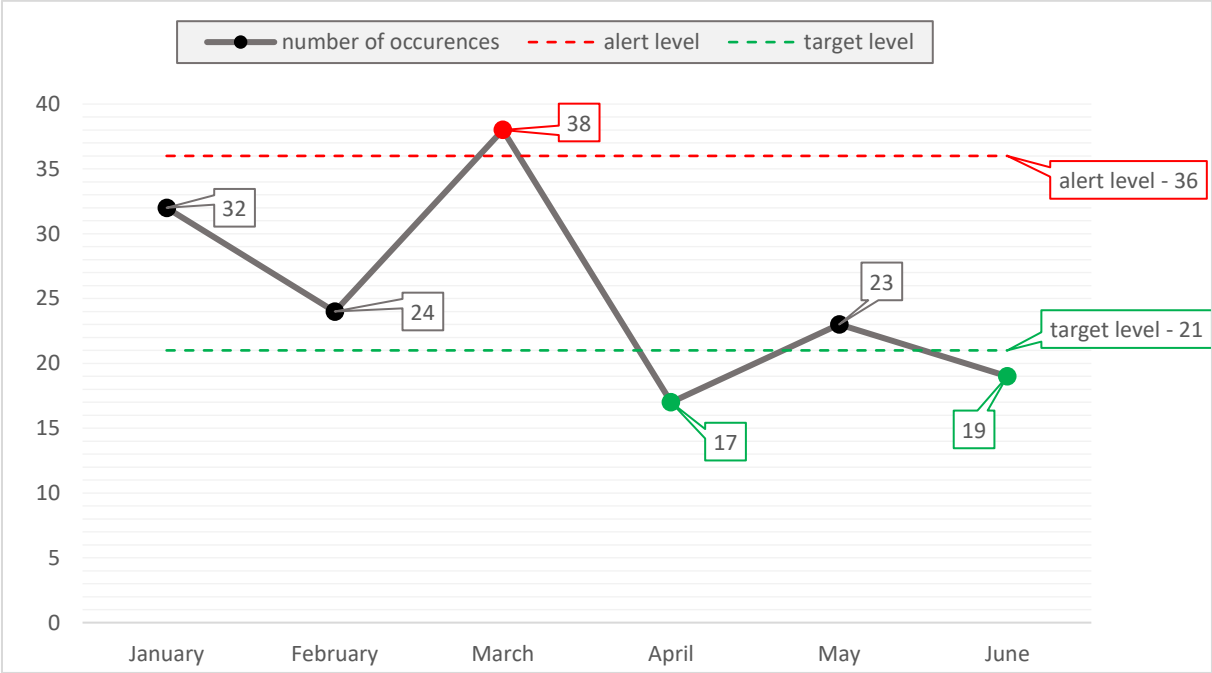


Figure 5 - Example how alert and target levels can be displayed in a chart

3 Systems Theory

Historical evolution of safety approaches is a proof of dynamics of aviation. The whole aviation system is getting more complex over time and pressure on reaching higher level of safety is increasing. Safety must be considered in the context of the overall system, not isolated individuals, parts, events, or outcomes. Traditional models are focused on single components only, which is insufficient for complex systems. There are accidents even though there are no component failures in the system. Mishaps can come from interactions which are not covered by frequently used safety models. Systemic approach copes with this phenomenon. Systems engineering focuses on design, integration, and managing complex systems over their life cycles. [13]

Systems theory is the interdisciplinary study of systems, which are cohesive groups of interrelated, interdependent parts that can be natural or human-made. Every system is bounded by space and time, influenced by its environment, defined by its structure and purpose, and expressed through its functioning. A system may be more than the sum of its parts if it exhibits synergy or emergent behaviour. Changing one part of a system may affect other parts or the whole system. The goals of systems theory are to model a system's dynamics, constraints, conditions and clarifying principles of the system. [14]

3.1 Systemic Approach

In the simpler world of the past, classic safety engineering techniques that focus on preventing failures and chains of failure events were adequate. They no longer suffice for the types of systems we want to build, which are stretching the limits of complexity human minds and our current tools can handle. Society is expecting more protection from responsible operators, managers, and regulators that are in charge of high-risky systems. [15]

Current systems especially those related to aviation are full of complexity. Above the level of execution of intended processes, there is always organisational level that co-ordinates work (company management) and supervisory level that regulates operations (aviation authority). This hierarchic structure is responsible for managing safe and fluent execution of processes.

3.1.1 Reasons for New Paradigm

Currently used safety models and tools for identifying hazards are quite outdated. Methods such as Failure Mode and Effect Analysis (FMEA) or Fault Tree Analysis (FTA) came into existence

after World War II. These models still work however present systems have changed a lot. FMEA and FTA reveals root cause of failure in an isolated component and it will always be important. But it can be successfully used only in limited scale for simple technical equipment. There shall be another analysis above complete system based on systems theory. Complex systems consist of big number of components and include humans that control automated processes. Even if every single component works as intended, when we put it all together, there are a lot of processes that fail due to wrong interactions among components. Traditional models are also based on probability which estimates how likely is one component to fail which again does not include interactions and so resulting probabilities could be distorted. For these reasons, we need new approach on system level that copes with complex sociotechnical systems.

Systems are much more complex these days. The increase in complexity is exponential. Current systems include new technologies, especially involvement of computers. Technology is changing faster than engineering techniques are responding to these changes. Software has revolutionised the engineering. We can make dozens of processes digitised and automatic, just by invisibly changing the code. Consequently, we can no longer understand and anticipate all undesired system behaviours. System needs elaborated requirements for software. The problem is usually system design error. That is the field that feels the lack of our attention. [16]

Human role in the system changed significantly. Human is not reliable for monotonous processes in comparison to automation. But human is good at controlling the function and making decisions. All in all, human operator is ordinarily blamed for accidents and incidents despite the fact that we do not know details about it. We shall first understand how the system is designed, if safety requirements are established, and whether all necessary information is available for human operator. System theory views human error as a product of the environment in which it occurs. To reduce operator error, environment where operator works must be changed. Human error is never a cause itself. Operators often work in imperfect system with insufficient procedures and not ergonomic interfaces. Human error is a symptom of a system that needs to be redesigned. Economics forces systems to be efficient and automation is one of the ways how to achieve it. Existence of goal conflicts and production pressures are frequent contributing factors. Decreasing tolerance for single accidents pushes all the safety endeavour forward. [16]

3.1.2 Properties of Complex Systems

Behaviour of a system cannot be easily inferred from its properties. In systems theory, complex systems are modelled as a hierarchy of levels of organisation, each more complex than the one below, where a level is characterised by having emergent or irreducible properties. Safety is an emergent property of systems that arises from the interaction of system components. Emergent properties are properties of complex systems that are not apparent from their components in isolation, but which result from the relationships and dependencies they form when placed together in a system. They are difficult or even impossible to predict since the ultimate results of couplings and mutual interactions are unknown. To avoid violation of safety constraints, we must bring emergent properties under control and enforce safety requirements, rules, and limitations. [17]

Complex systems often have nonlinear behaviour, meaning they may respond in different ways to the same input depending on their state or context. Systems tend to migrate toward states of higher risk. They are adaptive which means that they have the capacity to change and learn from experience. Complex systems are never static. Positive and negative feedback is always a part of complex systems. Open systems are viewed as interrelated components that are kept in a state of dynamic equilibrium by feedback loops of information and control.

Assumption that reliability equals safety is no longer valid in complex systems. Focus on failure events and the reliability engineering techniques to prevent them does not account for social and organisational factors in accidents, system accidents, software errors, human errors, and adaptation over time. Increasing the reliability of the individual components or protecting against their failure would not have prevented the loss. Prevention requires identifying and eliminating or mitigating unsafe interactions among the system components. [17]

There are two types of accidents. Component failure accidents are caused by single or multiple component failure. On the contrary, component interaction accidents arise in interactions among components and this phenomenon is more frequent in more complex systems. Undesired interactions are exaggerated by introduction of software into the system. Relationship between safety and reliability is shown on Figure 6 and it calls for a new model with systemic approach.

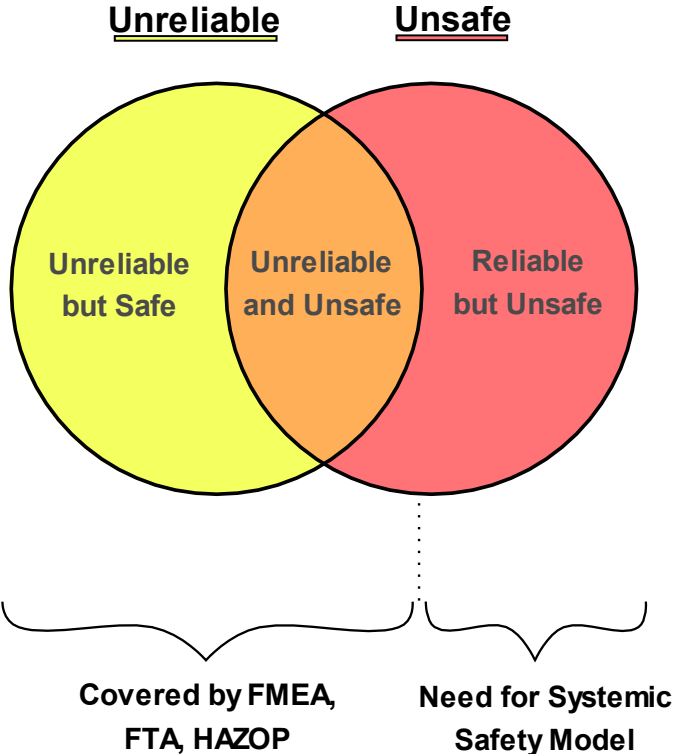


Figure 6 - Venn diagram presents a connection between unreliable scenarios and unsafe scenarios; the set of Reliable but Unsafe is not covered by traditional safety models

3.2 Model STAMP

Systems theory provides the foundation necessary to build the tools required to stretch our human limits on dealing with complexity. Excessive complexity is the key problem of current systems but cannot be reduced in the world rushing for automation and productivity. The goal is to deal with complexity using new model based on systems theory. Massachusetts Institute of Technology (MIT) has exhaustively studied new approach to safety. Main researcher in engineering of safe systems is Professor Nancy Leveson. Professor Leveson strived to replace traditional chain-of-events models by a new system-thinking model. The outcome is Systems-Theoretic Accident Model and Processes (STAMP). [15]

STAMP considers safety as a dynamic control problem rather than problem of reliability. Emergent properties that arise from processes must be controlled by controller (see Figure 7). Hazards result from lack of enforcement of safety constraints in system design. The goal is to control the behaviour of the components and systems as a whole, in order to ensure safety constraints are enforced in the operating system. STAMP is an accident causality model which integrates into engineering analysis causal factors such as software, human decision-making and human factors, new technology, social and organisational design. STAMP is relatively new (introduced in the beginning of 21st Century), yet it is already being used in space, aviation, health care, chemical, nuclear, defence, and other sectors.

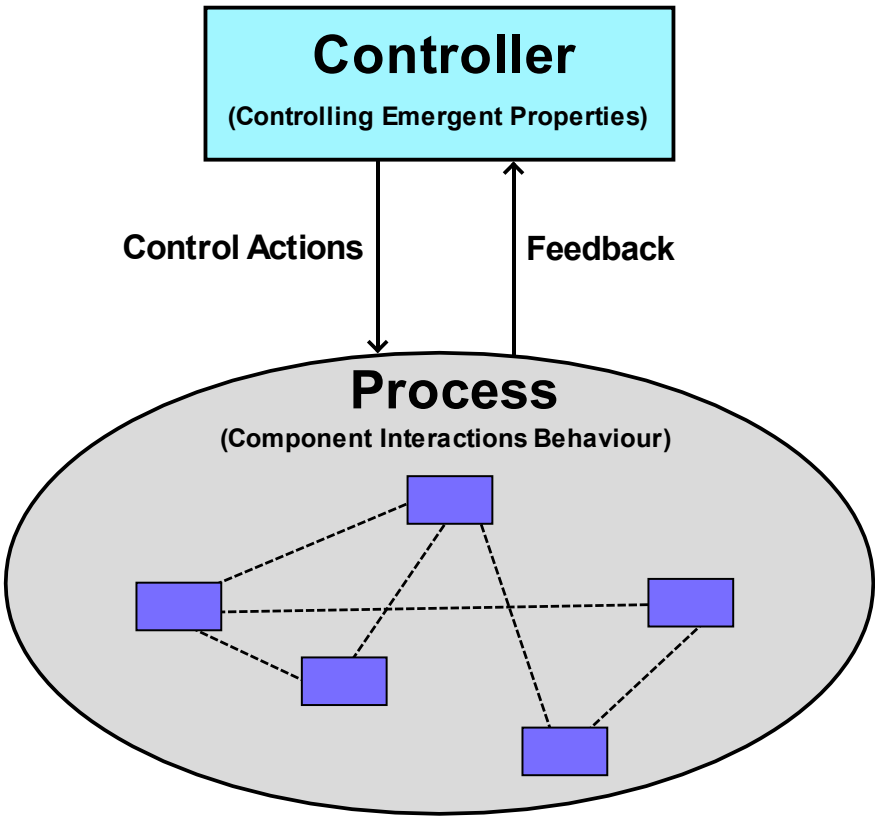


Figure 7 - The idea of STAMP is to focus on the way how processes are controlled [16]

STAMP enables us to design an effective control structure that eliminates or reduces adverse events. Safety is viewed as a control problem, and it is managed by a control structure embedded in an adaptive socio-technical system. The aim of the control structure is to enforce constraints on system development and on system operations that result in safe behaviour. In this framework, understanding why an accident occurred requires determining why the control structure was ineffective. That is how we can prevent future accidents.

Model STAMP is able to cover following mishaps:

- Scenarios from traditional hazard analysis methods (failure events);
- Component interaction accidents;
- Systemic factors (affecting all components and barriers);
- Software and software requirements errors;
- Human behaviour (in a non-superficial way);
- System design errors;
- Indirect or non-linear interactions and complexity issues;
- Migration of systems toward greater risk over time.

Control structure consists of control loops (see Figure 8). Each control loop is represented by controller (human or automated software) that acts on the foundation of control algorithm and process model. Controller issues control action (command) to the controlled process that is executed by actuator. A reaction of the process is measured by sensor that provides feedback to controller. Corrective feedback helps to achieve the desired performance. Mishap occurs when there is inadequate enforcement of safety constraints, inadequate execution of the control action, or inadequate or missing feedback.

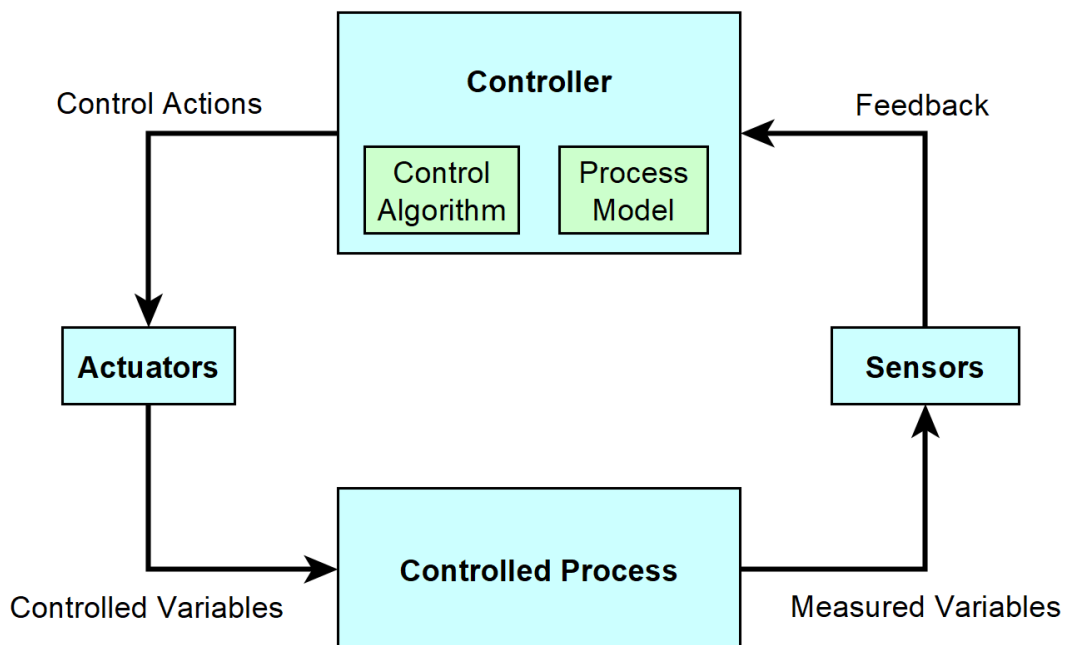


Figure 8 - Scheme of a generic control loop (adopted from [19])

3.3 STAMP-based Analysis

A set of tools and methods has been developed, tied to causality model STAMP. The goal is to identify potential causes of accidents, that is, scenarios that can lead to losses, so they can be eliminated or controlled in design or operations. The analysis can be performed during designing new system (at the time of concept) or evaluation can be made during operations or after damage occurs (for investigation). [19]

The earlier the change of a system is made, the cheaper and easier it is to implement the change. It happens these days that a system is designed, and a one-time evaluation of safety hazards is the very last step before launching the system. But this approach is ineffective. Safety assessment should be a continual process for designing systems and should actively create the system framework. Changes in system are simply and effectively embedded into system at early stage of development process (see Figure 10). Editing or adjusting procedures during operations is more demanding and operators need special training for changes of requirements. If safety constraints are still not enforced, there is a possibility for accident to happen. After experiencing huge losses associated with accident, the pressure on enhancing control structure is much stronger but costs for improvements are immense. Rework of safety requirements and constraints shall be done as early as possible which will reinforce overall system and increase level of safety. [19]

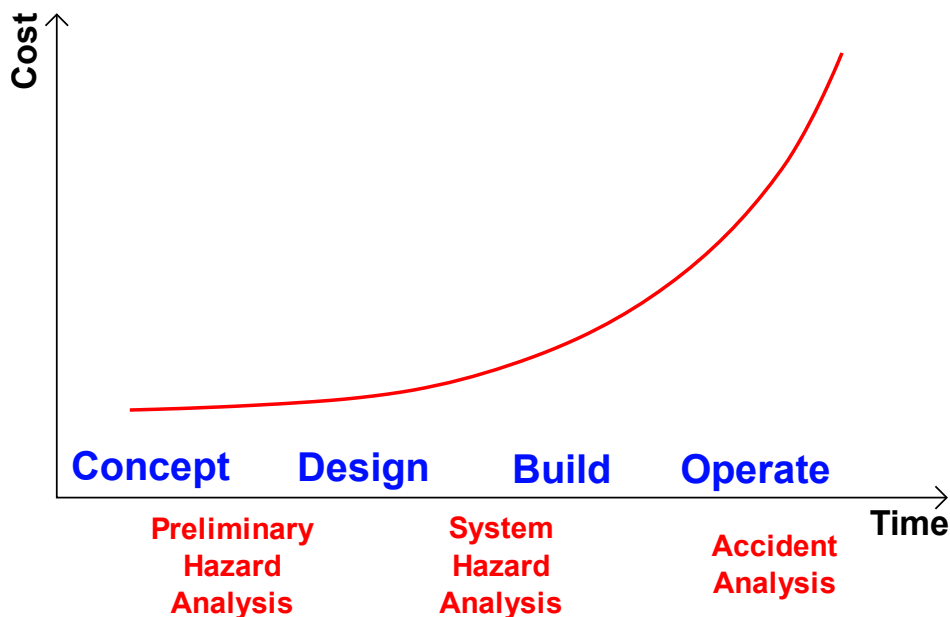


Figure 10 - Cost of design changes over system lifetime [19]

Many evaluations and comparisons of STAMP-based analyses to more traditional hazard analysis methods, such as FTA, FMEA, and HAZOP have been done⁵. In all of these evaluations, STAMP-based analysis found all the causal scenarios detected by the traditional analyses, but it also identified many more, often software-related and non-failure, scenarios that the traditional methods had not found. In addition, STAMP-based analysis turned out to be much less costly in terms of time and resources than the traditional methods. There are more STAMP-based analyses: relatively new techniques are applicable not only for safety, but also for security and other system-level properties. [19]

3.3.1 STPA

System-Theoretic Process Analysis (STPA) is a proactive analysis method that analyses the potential cause of accidents during development and operations so that hazards can be eliminated or controlled. STPA enables us to analyse very complex systems. “Unknown unknowns” that were previously only found in operations can be identified early in the development process and either eliminated or mitigated. Both intended and unintended functionality are handled. STPA includes software and human operators in the analysis, ensuring that the hazard analysis includes all potential causal factors in losses. STPA provides documentation of system functionality that is often missing or difficult to find in large, complex systems. [19]

STPA is a rigorous top-down system engineering technique that has the ability to identify potential design flaws. STPA consists of four stages of the analysis (see Figure 12) that need to be executed. The desired results after completing all stages are generated as a list of unsafe control actions with context and scenarios leading to hazards. Hazards must be prevented because they could lead to a loss in a worst-case scenario. STPA reveals low-level and high-level hazards of the system and potential losses, conducts a survey how the system works, identifies controllers and their control actions, and proposes system requirements and constraints. STPA uses a model of the system’s safety control structure for the identification of potential unsafe control actions. [19]

⁵ For example, running STPA on a flight test performed by U.S. Air Force. [25]

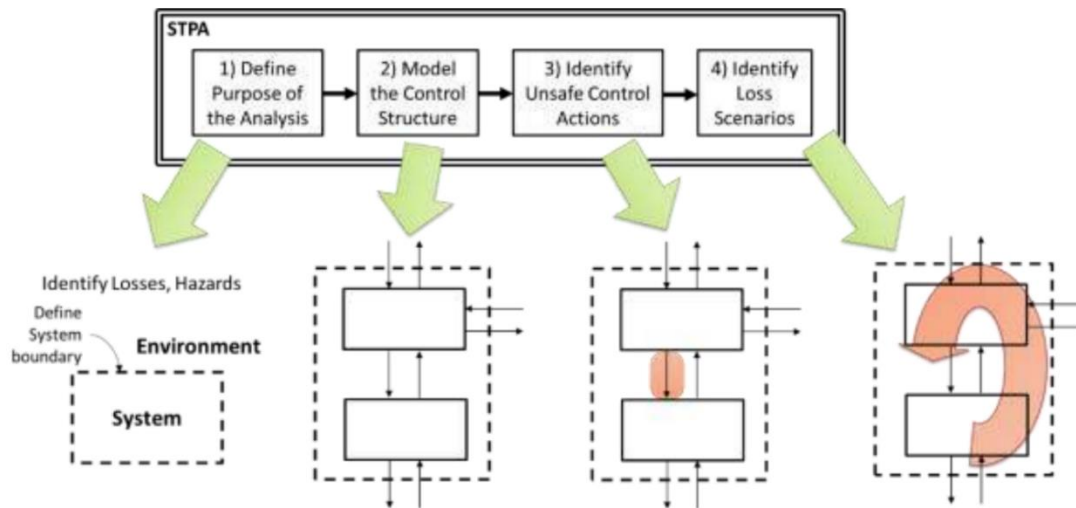


Figure 12 - Four stages of STPA that should be chronologically executed [19]

The four steps to execute STPA are following (see Figure 12):

1) Define Purpose of the Analysis

The goal of the hazard analysis is to prevent various losses (e.g. human injury, property damage, environmental pollution, loss of performance). First step of STPA identifies losses in the industry and system-level hazards. A hazard is defined as a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss. Boundary of the system is set (usually includes only processes which are under our control). Safety constraints shall be established for each system-level hazard. A system-level constraint specifies system conditions or behaviours that need to be satisfied to prevent hazards.

2) Model the Control Structure

The second step is a modelling of the hierarchical control structure. Control structure is a functional system model that is composed of feedback control loops. An effective control structure will enforce constraints on the behaviour of the overall system. A controller provides control actions to control some process and to enforce constraints on the controlled process. The control algorithm represents the controller's decision-making process which determines the control actions to provide. Controllers also have process models that represent the controller's internal beliefs used to make decisions. Process models (mental models) may be updated in part by feedback used to observe the controlled process. Systems typically have several overlapping and interacting control

loops. These loops are modelled which creates hierarchical control structure. In some cases, simply drawing a control structure diagram with all defined elements can make previously undiscovered flaws obvious. A control structure emphasises functional relationships and functional interactions, which is very useful for identifying problems like design flaws.

3) Identify Unsafe Control Actions

The next step after completing the model with control structure is finding unsafe control actions which, in specific context, lead to hazard. Control actions can be unsafe either when they are provided but within wrong context, or the control action is not provided at all. To ensure traceability, every unsafe control action shall be linked to a hazard. According to STPA, there are four types of unsafe control actions:

- Not providing the control action leads to a hazard;
- Providing the control action leads to a hazard;
- Providing the control action too early, too late, or in the wrong order;
- The control action is applied too long or stopped too soon.

4) Identify Loss Scenarios

The final step finds causal factors that lead to unsafe control actions. Loss scenario is a way how unsafe control action occurs. The initiation of loss scenario comes from deficiencies in a generic control loop. It can be inadequate process model, unsafe control input, inadequate control algorithm of a controller, problems on control path, not effective controlled process, inadequate feedback, or wrong sensor information received. Feedback radically influences controllers as it is crucial input for generating new control actions. Scenarios with control actions that are sent but improperly executed or not executed may be caused by delays in communication, transmission errors, lost communication, and other problems. [19]

STPA outputs are worthy source of information for refining and reinforcing current system, especially its control structure. The outputs are useful for driving the system's architecture, creating requirements, enforcing safety constraints, identifying design recommendations, establishing mitigations and safeguards, evaluation of existing design decisions, and designing more effective Safety Management Systems.

3.3.2 CAST

Causal Analysis based on Systems Theory (CAST) is a retrospective analysis method that examines an accident or incident that has occurred and identifies the causal factors that were involved. CAST is similar to STPA but applied at different time of system life and the steps used in STPA are adjusted and arranged into different order. CAST can be used to identify the questions that need to be answered to fully understand why the accident occurred. It provides the basis for maximising learning from the events. The goal of CAST is to get away from assigning blame and shift the focus strictly on how to prevent similar losses in the future. It is necessary to minimise hindsight bias and to determine why people behaved the way they did, given the information they had at the time. [15]

A loss results from the combination of a hazardous system state and environmental state. The engineers or system designers and the system operators only have under their control the system itself and not the environment. Because the purpose is to prevent hazards, that aim is achievable only if the occurrence of the hazard is under someone's control. Operators can manage safety only through the design or operation of the system by controlling the hazard or system state.

CAST is a structured technique to analyse accident causality from a system perspective. CAST is an analysis method, not an investigation technique. But performing the CAST analysis will assist in identifying what questions need to be answered and what information needs to be gathered during the investigation. The purpose is creating a comprehensive explanation as to why the loss occurred and to help formulate recommendations to prevent related accidents in the future. Because a cause of an accident is defined in STAMP to be a safety control structure that did not prevent the loss, then the goal of the accident investigation is to identify why the safety control structure was unable to enforce the safety constraint that was violated and to determine what changes are required to prevent a related loss in the future. [15]

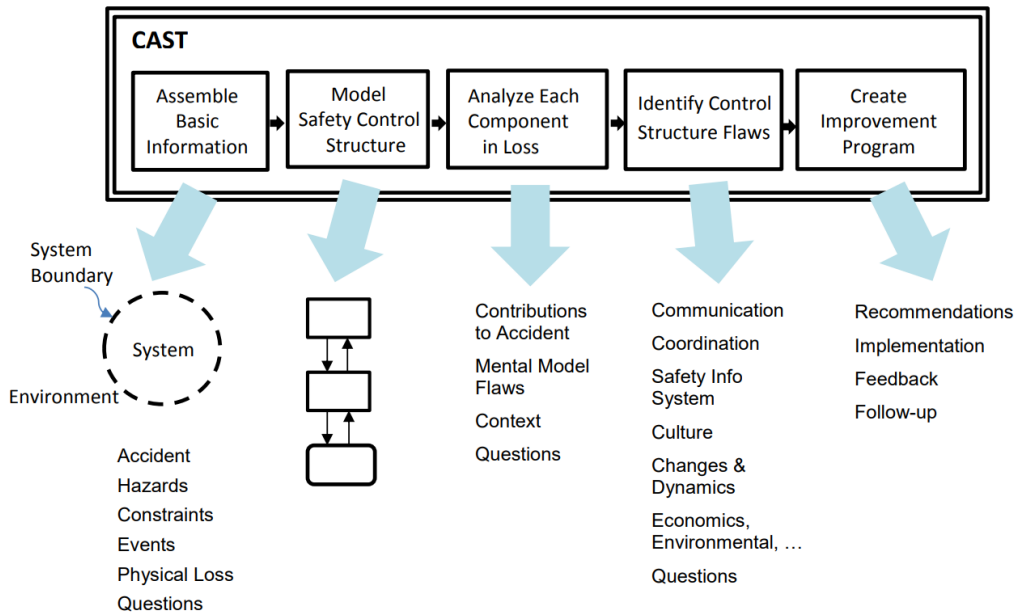


Figure 14 – Five steps of CAST analysis [24]

CAST comprises of five parts (see Figure 14). Firstly, the basic information is collected to perform the analysis, system boundaries are set, the loss and system-level hazards are defined, and the event is described without any conclusions. Secondly, the existing safety control structure for this type of hazard is modelled. Thirdly, the analysis goes from the bottom to the top and explains the behaviour of all components in the control structure which are examined to determine why they were not effective. Fourthly, generic systemic factors are detected, and flaws are identified in overall system control structure. Finally, recommendations and proposal of new constraints for changes to the control structure are created, and the results of the analysis are documented and can be schematically displayed in control structure as system deficiencies.

3.3.3 Active STPA

Active System-Theoretic Process Analysis (Active STPA) is an implementation of STPA into Safety Management System. Active STPA is a proactive approach working during time of operations of a system. It is a hazard analysis that keeps a live update of an existing STPA. In Active STPA, an STPA performed during system development becomes a structure that will constantly be evolving as it is revisited during the lifetime of a system. The output of this active hazard analysis helps the organisation adapt to its dynamic reality. [20]

The Active STPA was developed to identify leading indicators of increasing risk using feedback from operations throughout the system's lifetime, continually updating the STPA. To apply the Active STPA, the organisation needs to:

- Create an original STPA or use an existing one;

- Implement the controls recommended by the STPA;
- Collect operational data;
- Run the Active STPA.

The Active STPA starts by analysing an input message, such as a voluntary report, to determine whether the hazard analysis is incomplete or procedures in practice are ineffective. Conversely, when the analysis is complete, but constraints are violated, an investigation shall take place to figure out why the rules are not followed to adapt the procedures or to enforce the current ones. In Active STPA, defences are safety risk mitigations, or more specifically, actions that control the implementation of changes to operating procedures, equipment, or infrastructure.

The Active STPA is divided into three phases (see Figure 15). The first phase searches for ineffective procedures and inspects the STPA to identify incorrect or missing parts of the hazard analysis. The second phase is composed of tasks to guide safety manager on reasoning about the assumptions that were violated in operational incidents. The third phase helps guide the decision-making process as it relates to the identification of the optimum solutions for system defences, their implementation, and the update of the STPA. [20]

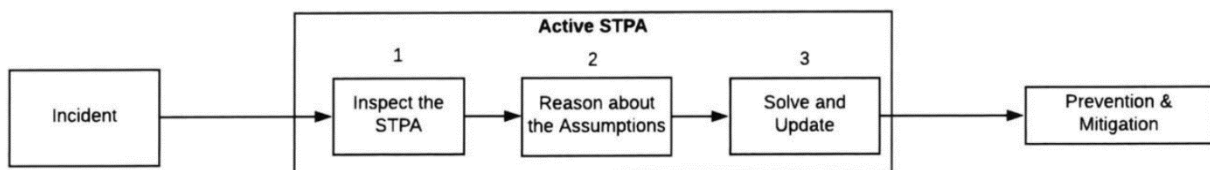


Figure 15 - Active STPA process [20]

Dynamic complex systems evolve in lifetime of a system and the environment, conditions, and procedures are changing. This migration of a system is inevitable and system design needs to be updated because assumptions about the system can be no longer valid. Assumption-based leading indicators shall be established which will monitor changes of system principles and will serve as a trigger. Assumption-based leading indicator is a warning sign that can be used in monitoring a safety-critical process to detect when a safety-related assumption is broken or dangerously weak and when action is required to prevent an accident. Alternatively, a leading indicator is a warning signal that the validity of an assumption is changing. These indicators shall serve as advice that safety requirements can be insufficient after the violation of an assumption and invite the safety manager to refine the system control structure as soon as possible. [20]

STPA does not provide any quantification of risks in comparison to traditional analysis, but the use of the Active STPA allows the observation of the most common mistakes and failures.

Qualitative arguments explaining the cause of incidents are stronger for decision-making than statistics, which only describes the frequency of occurrences in the past. Qualitative data better describe why something is wrong and how it happens. The results of hazard analyses can be displayed in safety information system. Safety information system is a critical component in managing safety. It acts as a source of information about the state of safety in the controlled system so that controllers' process models can be kept accurate and coordinated, resulting in better decision making. Setting up a long-term information system can be costly and time consuming, but the savings in terms of losses prevented will more than make up for the effort. [15]

3.3.4 STAMP-based Software

The increase in the usage of STAMP methodologies has fostered the need for developing a support tool to assist safety engineers in performing hazard analysis as well as accident analysis. STAMP-based software tools are being developed to support systemic data processing. Such platforms are supporting tools designed specifically to serve the widespread adoption and use of STPA, to facilitate STPA application to different systems, and to be easily extended to include different requirements and features. STAMP-based software also includes support of the application of CAST for accident analysis. Tools that support STPA, Active STPA, and CAST in integration into system engineering are for example XSTAMPP⁶, STAMP Workbench⁷, RM Studio STPA Module⁸, and STAMP-based Investigation Tool (SBIT)⁹. SBIT seems to be the most user-friendly STAMP-based software from existing programmes and is suitable for performing database of air incidents and accidents because SBIT is an investigation tool covering ICAO ADREP/ ECCAIRS taxonomy (dropdown menu to classify the occurrence according to stated taxonomy). [21] [22]

⁶ <https://github.com/SE-Stuttgart/XSTAMPP>

⁷ https://www.ipa.go.jp/sec/stamp_wb/manual/index.html

⁸ <https://www.riskmanagementstudio.com/stpa-software-project/>

⁹ SBIT has been developed by Czech Technical University in Prague.
[<https://www.inbas.cz/sbit-demo>]

4 Assignment: STAMP-based Database

The practical part of this diploma thesis comprises of two assignments. The first assignment is to create a safety database of incidents and accidents in air operations, process these data in existing STAMP-based software tool using hazard analysis, and interpret the results that current STAMP-based safety dashboard provide. The second assignment follows the established STAMP-based database. The goal of the second assignment is to put forward a proposal how to visualise safety outputs of STAMP-based analyses and perform validation of the outputs. For this assignment, software STAMP-based Investigation Tool (SBIT) is used since the reporting tool is based on aviation taxonomy and the environment is user-friendly.

4.1 SBIT

STAMP-based Investigation Tool (SBIT) was programmed by researchers of Czech Technical University in Prague and is being continuously developed. The aim of this new tool for Safety Management System is to present statistics in interactive safety dashboard, where the deficiencies of the analysed system are considered as a control problem. All displayed data are based on model STAMP. In addition to graphical section of the programme, SBIT can be used as a reporting system where incidents and accidents are classified and stored in database.

SBIT is a web-based software. SBIT supports safety occurrence investigation for aviation organisations. The system and its database serves as storage for investigated occurrences using systemic approach, and can be used by analysts, safety managers, and decision-makers. Processes that serve as input to SBIT are described by Business Process Model and Notation (BPMN) because BPMN enables to associate controller to each process which builds the control structure. The processes can be amended by unsafe control actions which are one of the key outputs of STAMP-based hazard analysis. Unsafe control actions are denoted as “deviations” and they may express causal factors, deficiencies in control structure, and deviations from safe operations.

SBIT requires the format of BPMN¹⁰ to be uploaded into the software. BPMN is a graphical representation for business processes with assigned responsible person. Processes are modelled and shall correspond to processes accomplished in real operations. The model includes performers (controllers) that control each subprocess and list of deviations from standard procedures (unsafe control actions). Subprocesses are denoted as “activities” which make each process description more detailed. An example of a modelled process in BPMN can be seen in Figure 16. When complete control structure of system’s processes is made, the overall model of processes is uploaded into SBIT where analyst can initiate filling the investigation report with system-thinking by processing the data of reported incident or accident.

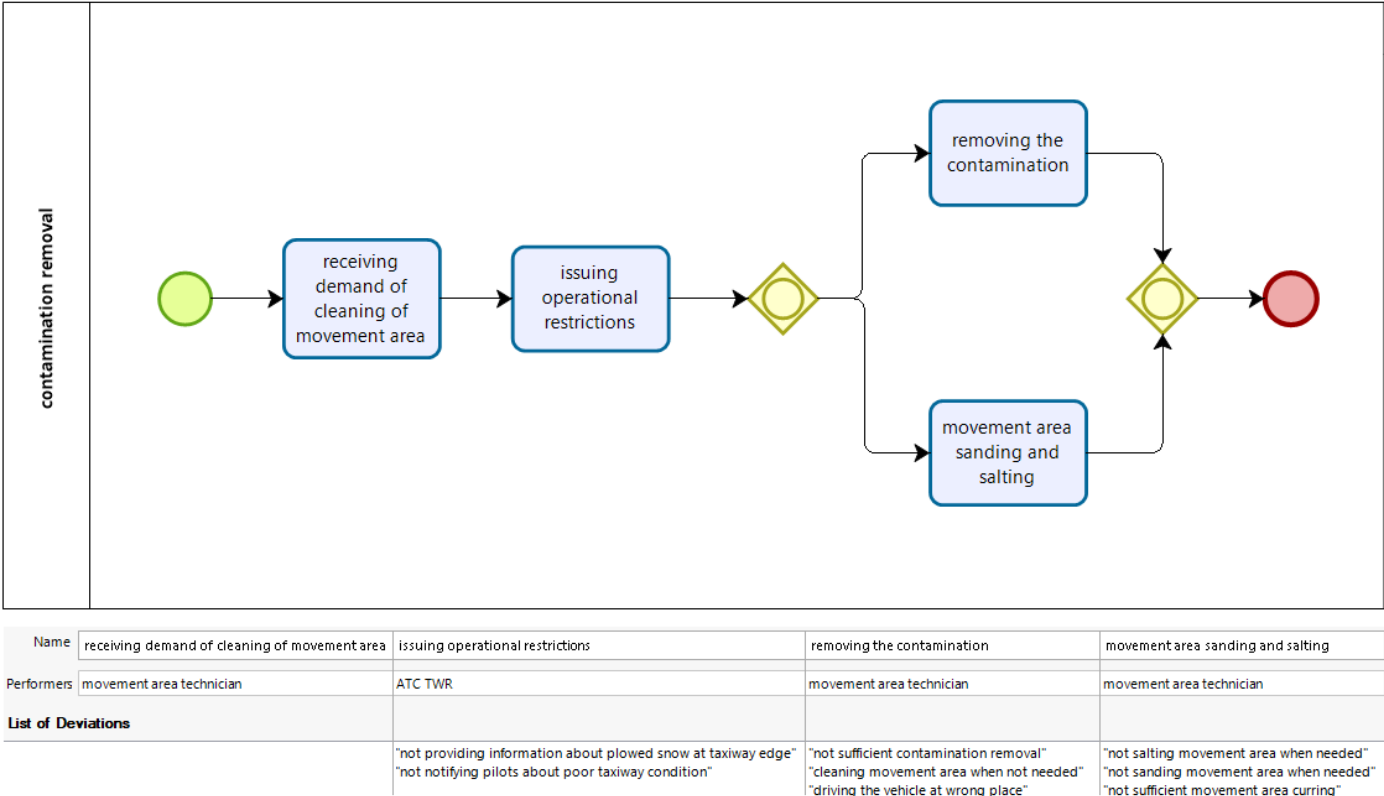


Figure 16 – Screenshot how modelling of processes in BPMN looks like; at the bottom part, controllers and unsafe control actions to each activity are added

After incident or accident notification, an analyst must fill the head of the report with available information about the event in SBIT. Information describing the accident is sorted to appropriate category and classified by Loss event type (hazard) based on ICAO ADREP/ ECCAIRS common taxonomy. Consequently, analyst creates sequence of processes (flow) how the event happened, and which unsafe control actions occurred. At the time of report completion, the report is saved to database. Information received from accidents and incidents

¹⁰ Processes were modelled by Bizagi Modeler. [https://www.bizagi.com/en/platform/modeler]

are displayed in safety dashboard. SBIT presents type of accident and contributing factors based on unsafe control actions so that safety managers have knowledge about causes of failure considering involvement of inadequate control structure.

4.2 Source of Data

A trustworthy source of historical safety data for filling the database is needed. It is essential to fill the database with data that are used in the real SMS database of an aviation organisation. These data serve for testing, validation, and verification of how systemic software SBIT works, what are the outputs, and how could future STAMP-based safety dashboard and visualization look like. The best source of data would be from real operations however these data are not available for private, legal, and security reasons and so cannot be provided for research purposes.

As the source of data for the database, Aviation Safety Reporting System (ASRS)¹¹ is used. ASRS belongs under American Federal Aviation Administration (FAA) and all reports are voluntary. A reporting person is usually pilot or air traffic controller (ATC). That is a big advantage since it enables us to look at the event from operator's point of view. ASRS is convenient for searching accidents and incidents and looking up in the list of reports. Significant contribution of voluntary reports is a free text where operator describes his situational awareness. It is worth information to avoid hindsight bias. Last but not least, another advantage of ASRS is a possibility to filter safety occurrences. Occurrences are classified into quite a lot of categories according to aircraft type, phase of flight, flight conditions, event type, or even contributing factors.

SBIT can be used as a part of SMS of various aviation organisations. To focus on one specific SMS, this safety database aims at aerodrome operations. Processes were limited to incidents and accidents that are connected to airport infrastructure and aerodrome procedures. Limitation of number of aviation processes reflects actual scope of current SMSs. Airport SMS database of reports is simulated in this diploma thesis. Great number of reports related to operations at the airport has been found. For this safety database, following filters have been used in ASRS for finding most relevant safety occurrences that take place at airports:

¹¹ <https://asrs.arc.nasa.gov>

- Aircraft model: Passenger or cargo aircraft, turbofan or turboprop engines (especially of following manufacturers: Airbus, Boeing, Embraer, ATR)¹²;
- Contributing factor: Airport;
- Event type: Ground incursion, Ground excursion, Ground conflict, FOD, Wildlife, Pavement conditions, Confusing airport design, ATC deviations.

4.3 Model of Processes

To maintain systemic approach, it is important to look at the system as a whole and focus on control structure. The model must not go too deep and should not analyse single components of the model. For keeping model simple as reasonably practical, borders of the system have been stated. The content of aerodrome processes, that are crucial for airport SMS, starts at final approach, includes whole airside, and ends up with successful take-off. Processes that are connected to aircraft operations on aerodrome infrastructure are part of the system. Here are the borders of the system – these processes are excluded from airport model because they are in responsibility of another SMS (i.e. maintenance, handling, air traffic control, airline), or are neglected (too specific process):

- Scheduled and non-scheduled aircraft maintenance;
- De-icing and anti-icing;
- Baggage and cargo handling;
- Dangerous goods handling;
- Aircraft fueling;
- Aircraft rescue and firefighting in case of emergency;
- Air traffic services provided by other units than Tower.

The model is comprised of sixteen basic processes. Every process is described by subprocesses (activities) more in detail to imply the flow of the process. These activities are based on procedures of airport operations. Activities can be in serial order, as well as parallel order. Each

¹² Aircraft models that frequently occur at medium and large airports are selected. To cover various aircraft models, different manufacturers are chosen since the top-selling aircraft type of each manufacturer comes up with different hazards.

subprocess has its assigned controller that controls the activity. An example of how a modelled process in BPMN looks like is shown in Figure 18.

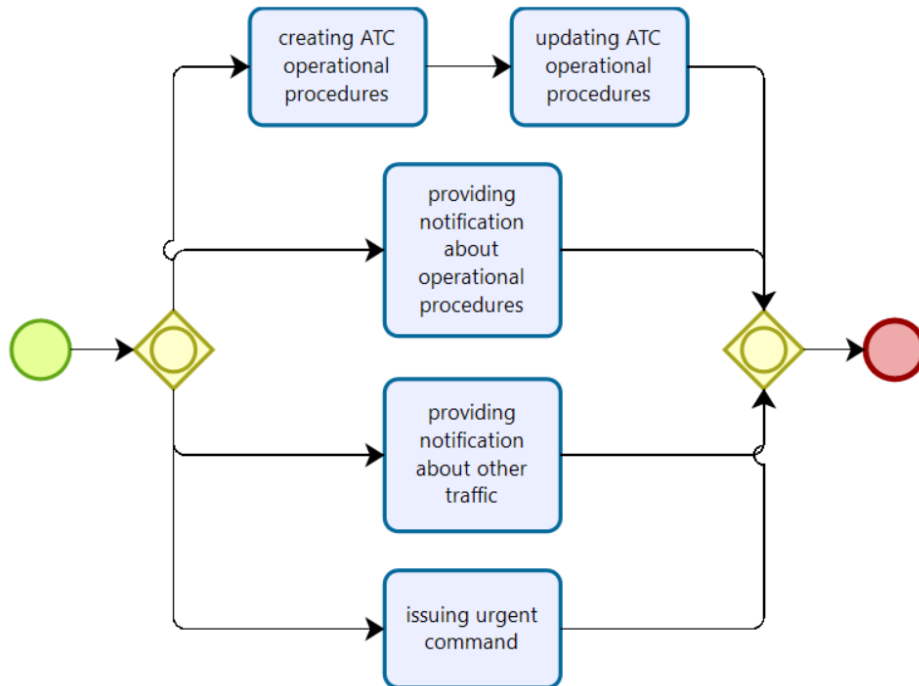


Figure 18 - Process "ATC procedures" comprises of five activities (subprocesses); BPMN format uses graphical elements (start, end, gateways) in the flowchart diagram, gateways specify serial or parallel order of the flow

The model composes of the following processes:

- Aircraft maintenance¹³;
- Approaching the stand and stopping;
- ATC procedures;
- Contamination removal;
- Ground handling¹⁴;
- Hazard and risk management;
- Infrastructure maintenance;
- Landing;
- Line-up and take-off;
- Movement area serviceability check;

¹³ Especially includes activity of manipulating the aircraft nearby hangar.

¹⁴ Especially includes activity of driving on a service road.

- Network administration;
- Pushback;
- Security assurance;
- Taxiing and crossing holding position;
- Vacating runway and taxiing;
- Wildlife control.

4.4 Data Processing

In the beginning, the BPMN model of all processes is uploaded into software SBIT. The model of processes can be updated whenever any changes in procedures are experienced or whenever new unsafe control actions need to be attached to deviated activities. Now, analyst (safety manager) needs to get to know what had happened in reported safety occurrence, investigate the event, and analyse possible contributing factors. Since accidents are considered as control problem, STAMP-based hazard analysis is performed to identify unsafe control actions and hazardous scenarios that lead to mishap. After the hazard analysis is done and outputs of the analysis are understood, safety manager is aware which process failed or which one contains deficiencies in control loops.

At this time, SBIT data processing can start. Firstly, safety manager fills the basic information like Occurrence class (e.g. accident, serious incident, incident, occurrence without safety effect, observation), Occurrence category (e.g. runway excursion, aerodrome, ground collision), and Loss event/ Hazard type (e.g. taxiway excursion, apron marking deficiencies, poor runway condition). These classifications are chosen from ICAO ADREP/ ECCAIRS common taxonomies.

Secondly, safety manager finds process which contains unsafe control action (in simple terms, deviation from standard procedure or not effective enforcement of safety constraints) and inserts it into the SBIT reporting window. The flow of the process consists of activities (subprocesses) that are in serial or parallel order (based on BPMN model of processes). Unsafe control action with specific context has been found during investigation (thanks to STAMP-based safety analysis) and consequently it has been updated in list of deviations in BPMN model. Safety manager matches unsafe control action with appropriate activity with insufficient control. After adding all detected unsafe control actions into the process, the unsafe control actions are connected to each other and ultimate one goes to Loss event. There are two

possibilities of links (connections) - link Causes and link Contributes to. Connection Causes is strict and means that Loss event is entirely caused by that one deviation. Connection Contributes to is looser, deviations only made contribution on arising problem. At this time, the report is finished, data are stored in database, and results are shown in safety dashboard based on SBIT logic (see Figure 21). The SBIT logic is a schematic representation explaining how deviations that fall under particular activities are calculated and linked to others.

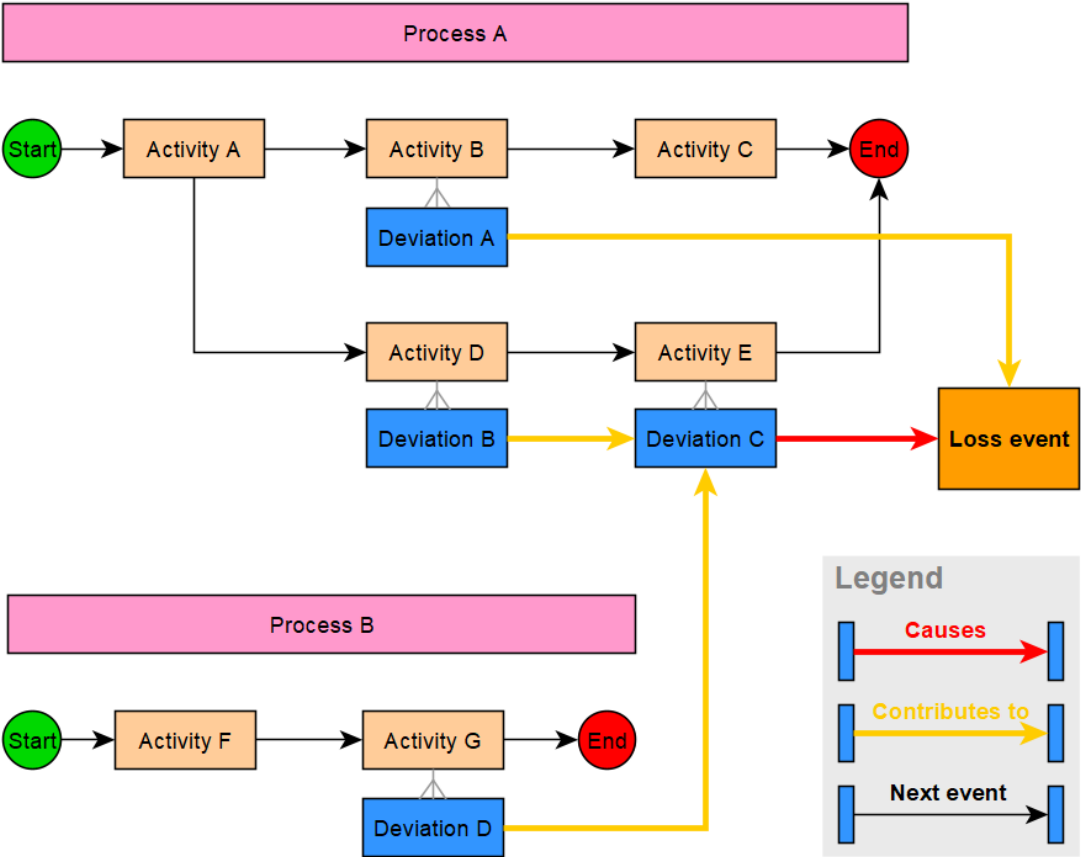


Figure 21 - Scheme of SBIT logic; the scheme is comprised of two processes and several unsafe control actions that cause or contribute to Loss event (unsafe control actions are modelled as deviations)

4.5 SBIT Dashboard

SBIT safety dashboard is currently the only one visualization of STAMP-based data therefore achievement of the results is described. SBIT counts the Causes and Contributes to links and remembers which unsafe control action is matched with which activity. SBIT records all links leading to Loss event. When the database contains dozens of reports, statistics shows the sums of unsafe control actions mentioned in all reports. Thanks to counting numbers of occurrences from the list of reports, we can see which controller (organisation) causes majority of unsafe control actions and understand in which processes and activities deviations from standard procedures usually happen.

Software SBIT brings worthy information based on model STAMP. The contribution is in highlighting the processes that cause Loss events frequently. SBIT does not look at failure of one activity in isolated way but notices negative influences from other activities. The schematic map shows mutual chains of events and guides safety manager to focus on activities involving unsafe control actions. The map visually highlights the connections with higher quantity (multiple links). The inferred results are weaknesses of the control structure and a lack of safety enforcement in procedures. These outputs are supportive for decision making in safety management.

The safety dashboard of SBIT provides a table of all reported data. The data in the table are categorised into four classes assumed from control structure: controlled process, activity (subprocess), deviation (unsafe control action), and controller. The four classes enable safety manager to sort the data and learn about possible causes of unsafe control actions. The table is a great tool for deep analysis of system weaknesses and insufficient control structure. The current picture of SBIT safety dashboard is shown in Appendix 1. Information inferred from STAMP-based database that is shared and visualised by current means of statistical dashboard is described in the following chapter.

4.6 Results Interpretation

Since theory related to model STAMP is continuously developing and its utility in practise is disseminating, this database in SBIT simulates airport Safety Management System. Research associated with visualization of systemic data struggles to reach worthier outcomes (better safety information) that provide nonnegligible system hazards and actual state of safety. SBIT currently provides the only visualization of STAMP-based data globally. The knowledge received from the outputs is described. How to follow up on STAMP-based visualization and improve the safety information gained from the data is the content of the second assignment.

My aim in the first assignment is to simulate airport database of SMS using ASRS reports. All the voluntary reports in ASRS comply with above described rules (filters) and principles for selecting incidents and accidents. I filled 200 aviation reports into SBIT reporting tool which resulted in creating STAMP-based database. The aim of filling the database was to check out how STAMP-based software works and what can be interpreted from the visualization. This sample of reports was processed by SBIT and results are presented in safety dashboard. The distribution of the classification of the reports used in this assessment is shown in Figure 22. We can read from the graph that most of the reports are minor incidents. Serious incidents take around a quarter of the pie and accidents are quite rare. Distribution roughly corresponds with Heinrich’s pyramid (the ratio between accidents and minor incidents) which means that the sample of reports is in a practicable range (no abnormal values). The reports from ASRS were taken one by one without selecting particular events which ensures objective filling of database without manipulating data.

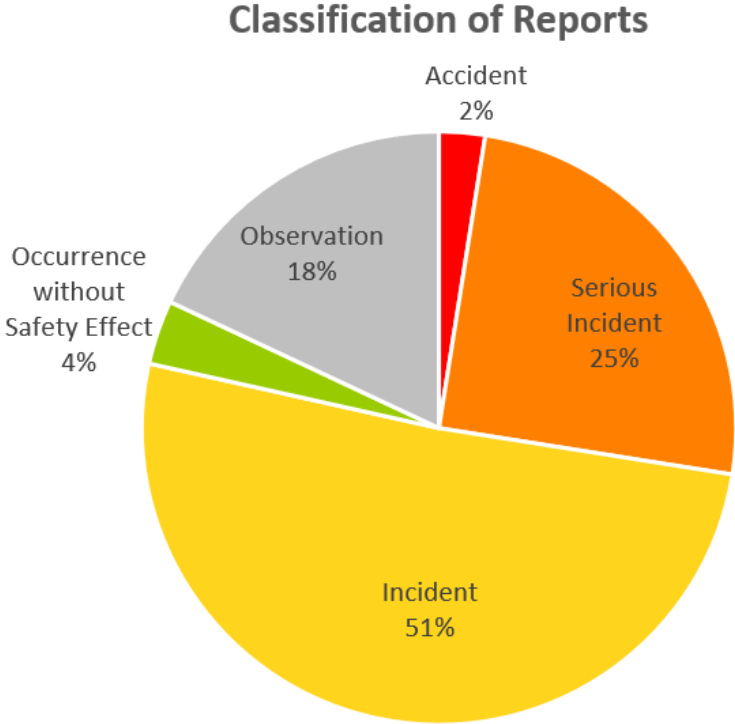


Figure 22 - Pie diagram shows the distribution of Occurrence class across all reports

The Figure 23 shows a statistical dashboard presenting deviated processes and their frequency in the database. The table shows Loss events (hazards) arranged according to number of repetitions. The most frequent Loss event in this database is “runway incursion by an aircraft” where process “vacating runway and taxiing” usually includes unsafe control actions. The second most repetitive Loss event is “taxiway excursion” where process with the highest number of unsafe control actions is “movement area serviceability check”.

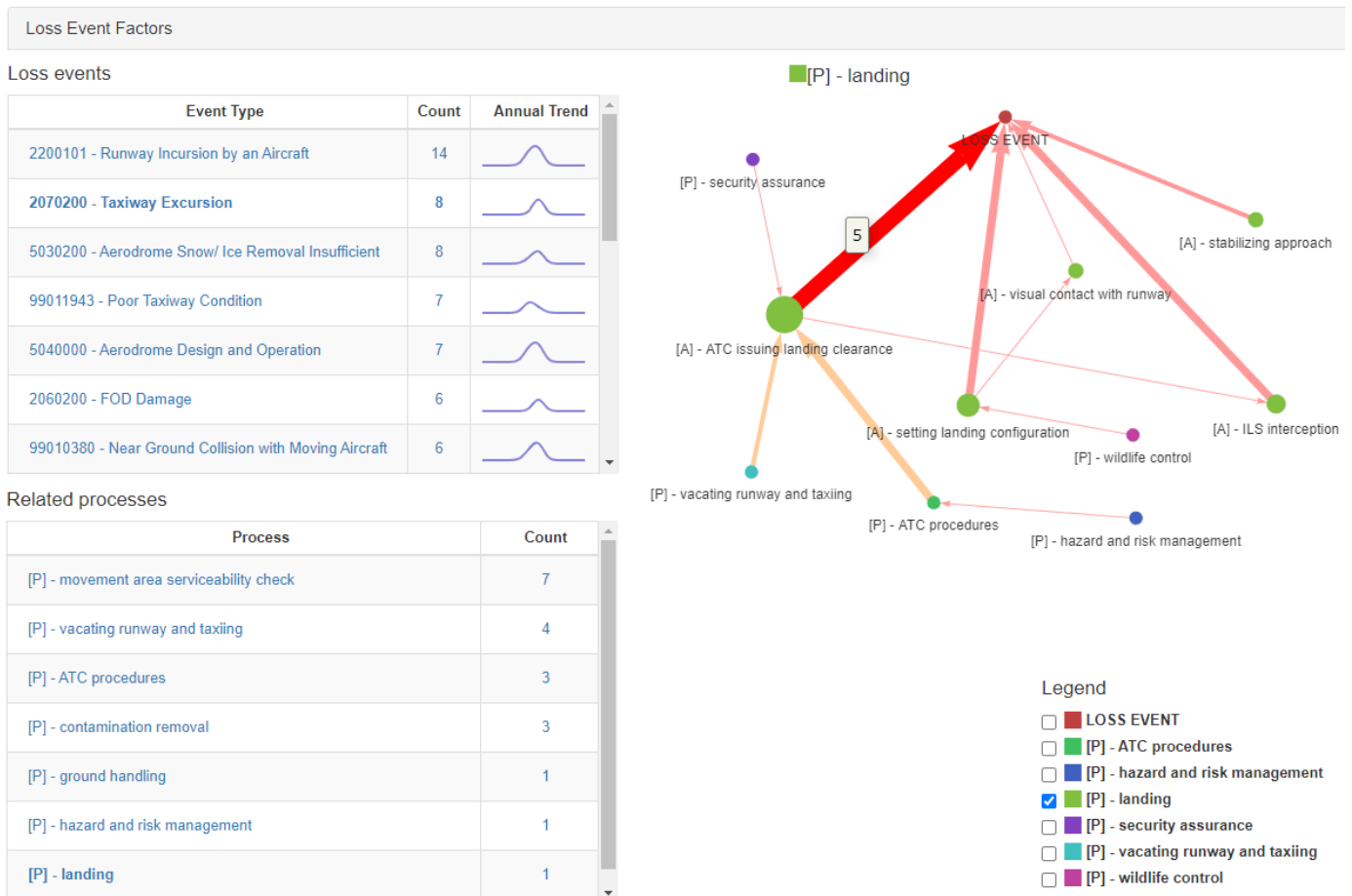


Figure 23 - Safety outputs based on model STAMP and BPMN displayed in safety dashboard of SBIT

The schematic map of connections reveals which processes and activities contribute to the Loss event the most. Sequence leading to mishap can be found and signals where undesired interactions are present. The schematic map graphically shows deviated activities in process “landing” that actively participated in accident or incident. Unsafe control actions in activity “ATC issuing landing clearance” caused Loss event five times and shall be examined. It could be interpreted that ATC gives wrong commands, correct commands at wrong time, or misses feedback from pilot. This tool supports safety managers to focus on specific part of the control structure.

The formatted table (see Figure 25) displays various orders of following classes: controlled process, activity (subprocess), deviation (unsafe control action), and controller. Ranking gives the information about the frequency of unsafe control actions in the database. The most deviated process in this database is “movement area serviceability check”. Activities (subprocesses) that contain unsafe control actions are for example “pavement structure check” and “searching for FOD”. The table shows which controllers are responsible for particular activities and a list of unsafe control actions contained. Safety manager can examine every process that deviates from stated procedures, focus on specific unsafe control actions, or monitor which controller produces significant number of unsafe control actions. The formatted table makes discovery of system design deficiencies possible and advises where safety constraints shall be applied or reinforced. This database can be publicly seen in demo version of SBIT software on website¹⁵ and a whole list of unsafe control actions linked to processes is attached in Appendix 2. A list of “Top 10” elements in each category is displayed in Appendix 3. Current SBIT abilities in presenting STAMP-based outputs are worthy but not definitive. Next chapter is focused on searching for the way how to provide new visualization of STAMP-based data or how to supply/improve the present ones.

The screenshot shows a web interface titled "Event - Control Loop". At the top, there are five dropdown menus for filtering: "controlled process", "activity", "deviation", "controller", and "Sub Dimension...". To the right is an "Export CSV" button. Below the filters is a table with the following columns: "controlled process", "activity", "deviation", "controller", and "count". The table data is as follows:

controlled process	activity	deviation	controller	count
[P] - movement area serviceability check				77
	[A] - pavement structure check			13
		[H] - ignoring damaged pavement	movement area inspector	5
		[H] - not detecting damaged pavement	movement area inspector	5
		[H] - not informing pilots about damaged pavement	movement area inspector	1
		[H] - not detecting rough pavement that causes shaking to aircraft	movement area inspector	1
		[H] - not detecting insufficient strength of pavement	movement area inspector	1
	[A] - searching for FOD			13
		[H] - not detecting FOD	movement area inspector	9
		[H] - ignoring frequent FOD occurrence	movement area inspector	3

At the bottom left of the table area, there is a pagination link: "1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25".

Figure 25 - The table counts the frequency of occurrences and can be variously adjusted to users

¹⁵ <https://www.inbas.cz/sbit-demo>

5 Assignment: Visualization of STAMP-based Outputs

Current literature does not contain any study or scientific research involving visualization of STAMP-based data except for safety dashboard provided by SBIT where the visualization is based on Business Process Model and Notation (BPMN). It is the field of study that needs further research and applying new methodologies as visual representation of the results is usually more illustrative for analysts or managers. The theory of systems engineering is developed, and several techniques inferred from model STAMP are validated. Many hazard analyses of complex systems have been performed and the results always found more safety information than traditional methods. Systemic approach considering all negative outcomes as a problem of control structure requires different point of view. Model STAMP has been already used in high-risky industries (for example establishing requirements and constraints for planning space missions) and its positive contribution is confirmed by Professor Nancy Leveson. [16]

STAMP-based methods are used especially in the phase of development while implementing these methods to ongoing operations is quite rare. In civil aviation, traditional models and methods are recommended by ICAO for managing safety. STAMP is still considered experimental although the contribution is positive. This diploma thesis can expand the knowledge about STAMP-based hazard analyses which supports the utility of systemic approach. Proposal of STAMP-based safety dashboard could lead to facilitation of model STAMP implementation into SMS of aviation organisations.

5.1 Safety Outcomes from STAMP-based Hazard Analyses

Three fundamental STAMP-based hazard analyses are taken into consideration. STPA is a proactive hazard analysis technique to analyse control structure of a system at early stage of development. Based on analysis' outputs, requirements and constraints for the system design are established. Active STPA is proactively performed during operations and it verifies validity of constraints when system migrates toward a state of higher risk after violation of assumption-based leading indicators. New requirements are included into original STPA and system's control structure is updated. CAST is an accident investigation method that reacts on serious incidents and accidents. CAST examines control structure flaws that had led to loss and learns a lesson for future avoidance. Again, STPA is updated and control structure reinforced.

To summarise the most important results of STAMP-based analyses, a set of unsafe control actions with context is revealed and various scenarios leading to the specific unsafe control action are provided. These results are presented in a form of spreadsheet. It is a text information for safety manager to be aware of mentioned unsafe control actions. System design and control structure shall be subsequently refined and verified whether safety constraints are enforced and control structure flaws are handled.

The outputs of STAMP-based hazard analyses give sense as an entire text including context (description of environmental conditions). Hazardous scenarios are linked to unsafe control action as they give better explanation of why undesired mishap can happen. Such an output is a text (sentence) that shall not be decomposed or somehow reduced otherwise it would lose its essential context and distort the meaning¹⁶.

Active STPA tends to become a part of Safety Management System in organisation. The safety information provided by STAMP-based analysis is worthy for SMS as it gives a possibility to proactively improve the system. However, SMS is based on safety dashboard that is composed of graphically-displayed data and charts monitoring trends. To monitor safety performance, aviation organisations prefer quantification of various occurrences. Number of repetitions of specific event/ occurrence can be compared in time to analyse progress in safety. STPA, Active STPA, and CAST outputs are all qualitative data that are hard to visualise. This is a challenge to resolve in order to promote model STAMP and derived methodologies to incorporate into organisations.

5.2 Difficulties of STAMP-based Qualitative Data Visualization

STPA does not provide any quantification of risks, nevertheless the use of the Active STPA allows the observation of the most common mistakes and failures. Qualitative arguments explaining the cause of incidents are stronger for decision-making than statistics, which only describe the frequency of occurrences in the past. Qualitative data have its advantage in providing more complex information. The disadvantage is the ability to create satisfactory graphical representation as it is preferred by analysts that manage large systems. To display trend of processed data, the values must be numerical. To visualise qualitative data, they must be converted into quantitative data. The conversion is sophisticated method by sorting data into classes which makes counting the data possible. It might be advantageous for safety

¹⁶ Example of unsafe control action with context: The pilot flying does not lower the landing gear during the approach for landing (H1). [20]

management to have both types, quantitative and qualitative, included for analysis of actual system’s safety. The former is represented graphically but with only superficial information, the latter provides deeper knowledge of a specific problem, but it is limited by its impossibility to display trends. [20]

The output of Active STPA is a solution that updates and enhances rules and procedures already in place, suggests testing activities, or even modifications to the design of system components. The new defences update the system's information flow, bringing it to a safer state. However, effective management demands an understanding of the operator's needs and difficulties. The application of new defences needs to consider how and when critical information should be delivered to operators and appropriately assimilated. [20]

The scheme in Figure 27 displays safety outputs of STPA arranged with links. A controller (C) controls a process via control action (CA). An unsafe control action (UCA) can be observed, and possible scenarios (S) describe how they may happen. Unsafe behaviour leads to low-level hazard (H*), continuing to system-level hazard (H), and loss. As mentioned above, these results are valuable as an entire text information with provided context to better understand the issue. To have better oversight what unsafe control actions are repetitive, numbers of unsafe control actions are counted in safety dashboard of SBIT which indicates frequent deviations in control actions.

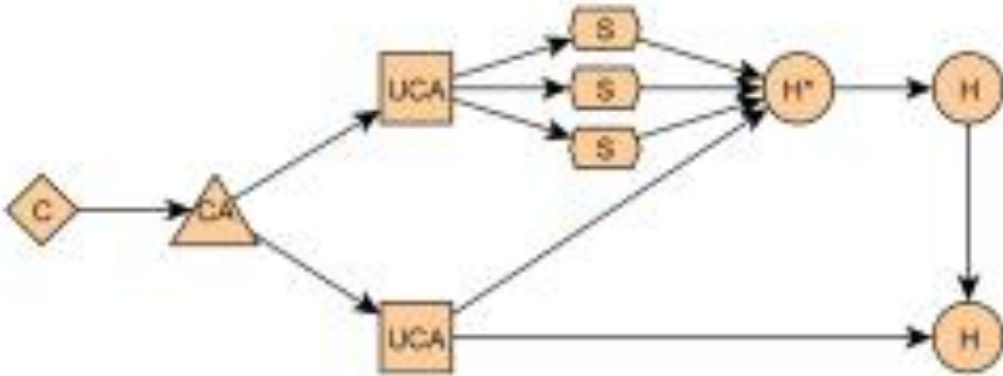


Figure 27 - Scheme of STPA outputs linked to each other (adopted from [23])

5.3 Control Loop

The goal of STAMP-based hazard analyses is to design an effective control structure that eliminates or reduces adverse events. Aviation is dynamic complex system that evolves with fast pace where rules, environment, and expectations change a lot. Also, assumptions that were a milestone for original system design are changing in time and sometimes are no longer valid.

Therefore, new requirements for control structure originate during time of operations. Some parts of the safety control structure must be analysed and refined. [20]

Control structure consists of many feedback control loops. Controllers send commands to and receive feedback from their controlled processes. Complex system may include several overlapping and interacting control loops. A control loop is only one form of active control of processes in a system. An active control requires a hazardous condition to be detected and corrected by controller. [20]

Control loop is a loop that includes controller (generator of control actions), controlled process, and feedback channel. Each control loop consists of following elements:

- Control algorithm;
- Actuator;
- Controlled process;
- Sensor;
- Process model.

Controller affects the behaviour of the process by applying control actions. Control actions are generated based on control algorithm and are implemented via actuator. Controller receives feedback about the current state of the process via sensor. Feedback is important update for controller's process model that processes various inputs. Based on these variables, control algorithm is updated or new one is generated and loop's cycle repeats.

Hazardous scenarios come from deficiencies in control loop. Possible component failures, lack of information on feedback, absence of feedback, incomplete requirements, lack of requirements, and design errors are the causal factors of a loss. The failure or hazardous state may not be detected or it may be detected but not corrected or it may not be corrected in time to prevent a loss. The mapping of actions applied to a controlled process, and the analysis of the feedback that the operator is receiving, provide a qualitative understanding of the real issues

behind the unsafe behaviour. The Figure 28 shows all possible deficiencies in a control loop that directly influence safety performance. [19]

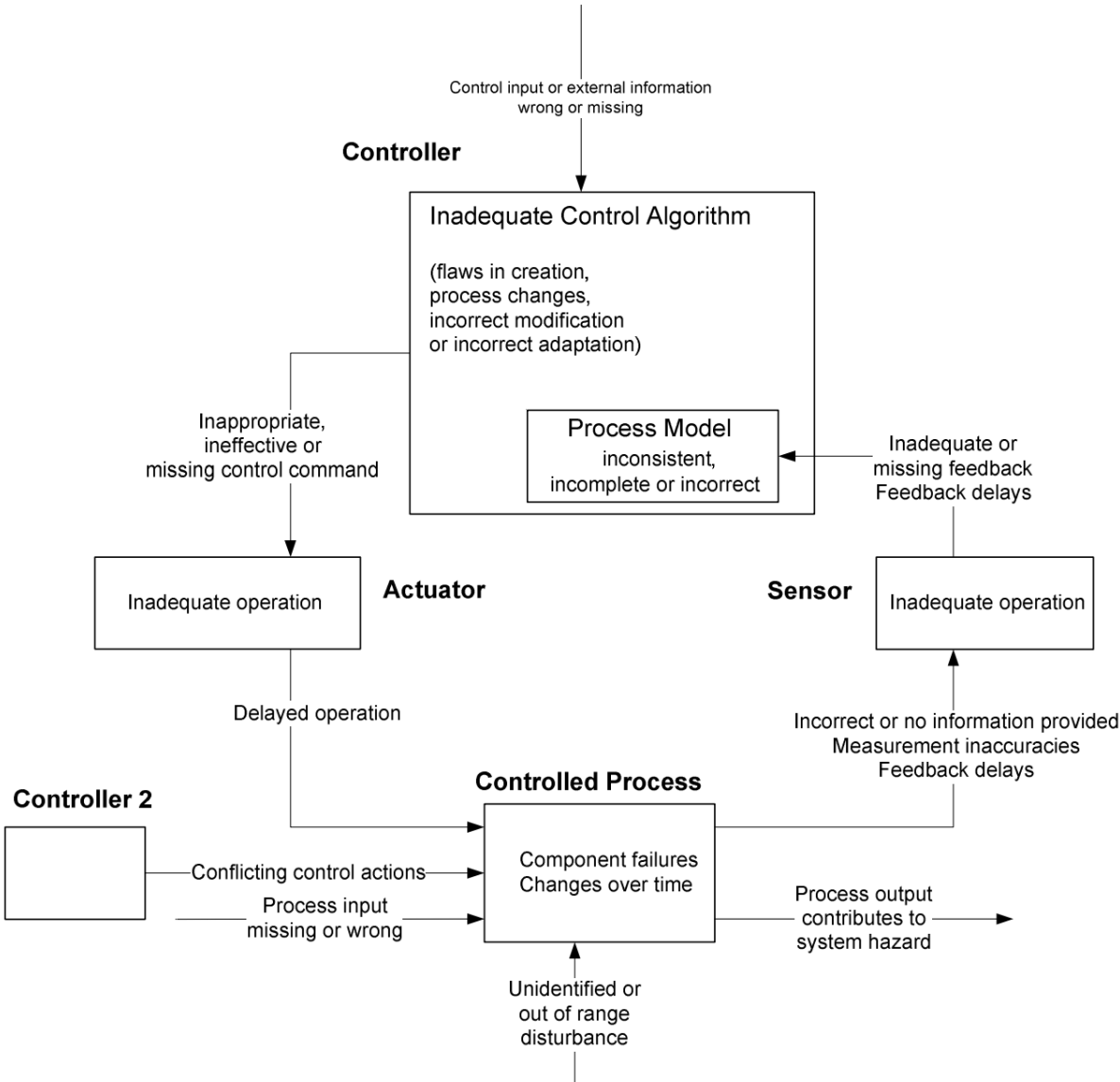


Figure 28 - Scheme of control loop supplemented by various deficiencies in each part of the loop [15]

5.4 Introduction to Proposed Solution

This thesis proposes an assessment of specific control loops in aviation operations which function can be visualised. This detailed analysis examines a set of similar control loops of a process. A process which is further analysed and of which functionally needs to be checked, is selected by safety manager based on general knowledge of system weaknesses. Proposed analysis monitors correct, delayed, or incorrect function of each element of the control loop/ set of similar control loops. Proposed visualizing method can be used for proactive as well as reactive purposes.

The idea of proposed STAMP-based visualization is to perform an analysis that focuses on functionality of each element in control loop based on data information received from investigation of incident or accident. The visualization aims to display how each element of control loop works considering more measurements (information from more occurrences). Observed outputs have the ability to display correlations among various measurement of a control loop or of a set of control loops. Resulting visualization notices whether process is performed correctly and whether feedback channel works. It gives a better understanding of how hazardous scenarios happen.

The scope of analysis should not be focused on single control loop only where applicable. In order to not have isolated insight, a set of similar control loops can be examined. Control loops that are part of one superior process or are controlled by the same controller may produce the same type of deviations. These correlations in behaviour of a set of similar control loops are revealed after the analysis is performed and results visualised. If there are any negative influences from other control loops, the visualization displays downgraded functionality.

5.5 Source of Data

The proposed visualization of STAMP-based outputs requires data from real operations. It means that the proposed analysis can be used as a part of SMS to update control structure during operations rather than using it at the development phase when data from operations are not available. SMS can use the visualization of control loops' functionality for detailed analysis of selected processes. The utility of monitoring trends in time is described later in this thesis.

The visualization of control loop elements can be run during or after data collection. Visualization can be performed in a system that has undergone STPA and the control structure is known. The visualization requires outputs from STAMP-based investigation method as SBIT provides. The proposed analysis and consequent visualization might be performed whenever there is a suspicion that some control loops do not work as intended.

The visualization further processes information received from STAMP-based database. It depends on the particular aviation organisation whether they use proposed method to analyse the control structure exclusively retrospectively, exclusively proactively, or combination of both. Retrospectively means that the organisation studies only historical reports from the database, proactively means that the organisation continuously collects data (on-site inspection), fills the spreadsheet at the same time, and monitors changes in functionality of control loop displayed in the proposed visualization. Combination of both approaches is

possible, depending on safety manager's intention. Retrospective analysis can be performed on a regular basis and results compared which is a fundament of continuous monitoring approach. There are more possibilities how to collect data and feed the database:

- Obtained from mandatory or voluntary reports;
- Obtained from accident or incident investigation reports¹⁷;
- During performing A-STPA (after violation of assumption) or CAST;
- An inspection, audit, or observation is done¹⁸;
- Using automatic recording of digital data¹⁹;
- As a part of management of change.

Inspections are systematic ways to observe if the system is running as planned. Inspections can be used for proactive more-detailed collection of data about specific process. They are usually on-site (observations of conducting procedures, listening to ATC frequency) and flight data monitoring system can support with providing information. To assure comprehensive inspections, the frequency must be high enough to be considered routine, but not so high as to interfere with performance. Audits are another form of safety inspection performed by an internal company division or third-party experts. For the purpose of this thesis, database of incidents and accidents created in SBIT (as described in chapter 4 Assignment: STAMP-based Database) is used to validate the proposed method. [20]

5.6 Data Transformation

In the beginning, qualitative data (outputs from STAMP-based hazard analyses or investigation methods) need to be transformed into simpler representation (values that are easier to count). The visualization of functionality of control loop needs an analyst to fill in simple spreadsheet by assessing how each element works. Analyst evaluates whether the element of control loop works correctly (value: "1"), correctly but with delay (value: "1*"), or incorrectly (value: "0"). These values are filled for each of five elements in control loop: control algorithm, actuator, controlled process, sensor, process model. This is one measurement that shall be repeated – the more times, the more precise results will be.

¹⁷ For example, analysing data from „black boxes“ or interviewing pilots.

¹⁸ For example, inspecting pilots in cockpit or listening on frequency to air traffic controllers.

¹⁹ For example, checking how processes in cockpit are performed and timing of performed activities. Flight data monitoring expands significantly and more data are expected to measure and store in the future.

Analyst is supposed to understand analysed process and to use all data available to particular incident to have broader view of what had happened. Transforming information into digits enables to apply maths operations, use statistics, and infer conclusions about the filled data in spreadsheet. Using sophisticated formulas to process and count inputs is a way how to gain deeper knowledge about analysed control loops as a part of control structure. In addition, the data after transformation are quantitative and so graphical visualization of numbers can be provided.

5.7 Evaluation of Control Loop Elements

Propositional logic is used to assess a control loop. There are only three possibilities how to assess each element of control loop. The value can be “1”, “1*”, or “0”, where “1*” is a subset of value “1” so in fact, there are only two groups. The upper index of star of value “1” means that element function is correct but delayed. They follow binary logic so software may compute it easily. They are subsequently automatically processed by designed formulas that are described later. The filling form is displayed in Table 1 and shows five measurements performed in one specific control loop. The inserted values are illustrative, practical example is provided later as a part of validation of proposed method and visualization.

Table 1 - Filling form for evaluation of control loop; each row symbolises each measurement (filled values are illustrative only)

column:	A	B	C	D	E
ID	control algorithm	actuator	process	sensor	process model
1	1	1	0	1	1*
2	1	1*	1	1	1
3	0	0	0	1	1
4	1	0	0	1	1
5	1	1	1*	1	0

One row means one measurement. Only measurements that include any deficiency or delay are recorded. There cannot be any single row filled exclusively with values “1”. In any row, there must be at least one element “1*” or “0”. Value “1” is positive, value “1*” is positive but delayed, and value “0” is negative. These values are further processed. The column of each element is counted up, and the result is a percentage of positive or negative outcomes from all recorded measurements mentioned in Table 2. Measurements where no element had deviated or had been delayed are excluded from the spreadsheet and are neglected for this analysis and

visualization²⁰. The percentage expresses number of values related to number of measurements that are filled in the spreadsheet. Number of delayed functions is also shared in percentage.

Table 2 - The table skipped inserted data and shows the results of measurements; percentage of positive functions, negative functions, and delayed functions of each element are displayed

column:	A	B	C	D	E
ID	control algorithm	actuator	process	sensor	process model
⋮	⋮	⋮	⋮	⋮	⋮
total 1+1*:	76%	72%	56%	44%	72%
total 0:	24%	28%	44%	56%	28%
total delay:	4%	8%	16%	4%	4%

Following bullets further describe exact meaning of positive or negative evaluation of each element and provide instructions how to assess elements of examined control loop:

- Control algorithm

Every controller generates control actions based on received information (mental model). The way how controller determines command to apply on process is called control algorithm. If an operator clearly chooses which control action to perform and the solution is appropriate, the value is “1”. As an operator has no idea how to control the process, does not control the process at all, or applying control actions in totally inappropriate situation and context, the value is “0”.

- Actuator

Actuator is the means how to apply a control action. A command is forwarded from actuator directly to process. If controller knows how to use some equipment, communication, or controlling software and control action is applied from actuator on process, the value is “1”. If an operator executes command incorrectly, does not know how to realise the control action, or actuator fails, the value is “0”. In case when control action is provided within wrong context (bad timing), the control algorithm is evaluated as “0” meanwhile actuator is

²⁰ Reaching an approximate number of measurements where no deviations in control loop had occurred is almost impossible as it is majority of the performance and current data monitoring is oriented especially on negative outcomes.

evaluated as “1” because the command works as intended and controls process as desired.

- Controlled process

A process is a productive part of a system. It is an activity bringing benefits to a system and it is a core of operations. If the process works as intended and does not bring any other negative outcomes, the value is “1”. If the process does not work or works differently and does not reach its purpose, the value is “0”.

- Sensor

Sensor measures variables coming from process. Sensor is a feedback element that informs controller how the process was executed. If the variables match with outcome of the process or if sensor detects wrong function of the process, the value is “1”. If the measured variables are distorted or wrong, no feedback is provided, or if sensor does not detect faulty function of controlled process, the value is “0”.

- Process model

Process model collects various inputs, especially feedback from sensor, and forms entire situational awareness that will consequently influence generating of control algorithm. Process model processes feedback about how controlled process works. If an operator interprets feedback information correctly or detects deviation of the process even without any alert of sensor, the value is “1”. If the feedback is incorrectly interpreted, misunderstood, or is not received, the value is “0”.

If a function of any element delays significantly, a time lag exists, or the activity takes too long time, but in the end the element complies with its function, the value is “1*”. Delayed function of elements decreases effectiveness of control structure and brings potential to deviate or fail. The positive but delayed functions are monitored in all elements and after performing more repetitive measurements, a percentage of delay frequency of each element is calculated.

5.8 Evaluation of Control Loop Characteristics

In distribution of values “1” and “0” across elements in one measurement of control loop (one row), we can observe dependence (correlation) among some elements. These correlations bear

additional information further describing a particular measurement. Summarising all recorded characteristics provides total number of a specific correlation expressed in percentage. Percentage emphasises predominant properties of the control loop per determined period.

To find some correlations in one row (called “characteristics”), formulas are established to count particular property when determined conditions are met. Characteristics are processed by formulas and are counted per each row to better describe what happened in one measurement of control loop. Delayed function “1*” falls under value “1”. Definition of “effective feedback” is as follows: both, sensor and process model, must work as intended (sensor must provide correct feedback which is correctly interpreted). Feedback is considered effective even if it is delayed.

To better arrange columns, elements of control loop are marked by a letter that will be used in formulas to detect characteristics: control algorithm “A”, actuator “B”, controlled process “C”, sensor “D”, process model “E”. Processed data outputs are “1” or “0”. “1” means that the conditions are met and so the characteristics is valid for that one certain measurement. “0” means that the characteristics is not met and so not valid. Monitored characteristics are sorted into three tables (Table 3, Table 4, Table 5) that displays used formula, name of characteristics, and values calculated from original spreadsheet. The results in following tables are based on measurement inputs filled in Table 1.

Table 3 - Percentage of these characteristics shall be as high as possible

formula:	$(A \wedge B \wedge C \wedge D \wedge E) \rightarrow 1$	$C \rightarrow 0 \wedge (D \wedge E) \rightarrow 1$	$D \rightarrow 0 \wedge E \rightarrow 1$
ID	loop works well but contains delay	process does not work but feedback is effective	resilience of controller
1	0	1	0
2	1	0	0
3	0	1	0
4	0	1	0
5	0	0	0

Following bullets describe characteristics mentioned in Table 3:

- Loop works well but contains delay

All elements in the control loop worked correctly but there was a lag in time in one or more elements. The more measurements comply with this rule, the more acceptable are the outcomes because nothing failed there.

- Process does not work but feedback is effective

The process failed or was not executed but this issue is reliably detected by sensor and correctly understood by controller. The more detections of flawed process, the better.

- Resilience of controller

Sensor did not inform about actual state of process, but controller revealed this deficiency and interpreted situation correctly. The more controllers react properly on process with faulty sensor, the more resilient is the control loop.

Table 4 - These characteristics indicate which element or affiliated link fails and provide possible cause

formula:	$A \rightarrow 1 \wedge B \rightarrow 0$	$B \rightarrow 1 \wedge C \rightarrow 0$	$C \rightarrow 1 \wedge D \rightarrow 0$	$D \rightarrow 1 \wedge E \rightarrow 0$
ID	inappropriate command	technical problem	faulty sensor	incorrect interpretation
1	0	0	0	0
2	0	0	0	0
3	0	0	0	0
4	0	0	0	0
5	0	0	0	0

Following bullets describe characteristics mentioned in Table 4:

- Inappropriate command

The thought what control action to provide is correct but the way of executing command is incorrect. Controller probably does not know how to perform the activity which makes the actuator to fail.

- Technical problem

The control command via actuator is executed correctly but process does not work. It may signalise technical problem as there can be undesired disturbances and interferences with environment.

- Faulty sensor

The process was executed correctly but sensor did not detect it. There may be deficiencies in measuring of control variables or communication that does not provide feedback.

- Incorrect interpretation

Sensor measured the state of process well, but the feedback was not interpreted by controller's process model (mental model) correctly. Controller did not understand the sensor, was inattentive, or experienced misunderstanding of transmitted data.

Table 5 - These characteristics measure when control algorithm is wrong and if it is detected by feedback loop

formula:	$A \rightarrow 0 \wedge B \rightarrow 0$		$A \rightarrow 0 \wedge B \rightarrow 1$	
ID	controller does not control process	of which identified by effective feedback	controller controls process when should not	of which identified by effective feedback
1	0	0	0	0
2	0	0	0	0
3	1	1	0	0
4	0	0	0	0
5	0	0	0	0

Following bullets describe characteristics mentioned in Table 5:

- Controller does not control process

Controller does not plan to control any activities, so the control action is not provided. The process shall be controlled but controller is not aware of it. Percentage of how many feedbacks were effective to alert the controller about his inactivity is calculated.

- Controller controls process when it should not

Controller provides control action when it is not adequate. Controller's control algorithm is applied at wrong time and context, but actuator is commanded to start executing the process. Percentage of how many feedbacks were effective to alert the controller about his unsafe behaviour is calculated.

There are three additional properties that can be inferred from calculated characteristics. There is a correlation found among resulting characteristics (mentioned above) therefore they are shared as other possible figures to monitor. Some characteristics imply the same possible causal factor of deviated function of control loop. Hence, these additional characteristics are composed of correlating characteristics that are consequently averaged, and new three indicators are established. These indicators can be shared as a part of safety dashboard as well as other bar charts which express characteristics described above. The calculated percentage of "combined"

characteristics shows how many rows from all measurements the particular characteristic is valid for (see Table 6). They can be considered as causal factors.

Table 6 - Characteristics inferred from previously calculated outputs that give a better view on causal factors of deficiencies in the control loop

inadequate training, inappropriate procedures:	30%
component failure, faulty transmission:	15%
average delay per control loop:	14%

Following bullets describe additional characteristics mentioned in Table 6:

- Inadequate training, inappropriate procedures

This property is an average value of following characteristics: wrong control algorithm, inappropriate command, and incorrect interpretation. All these characteristics are strongly tied to controller that makes decisions and cooperates with other elements of control loop. If there is a significant number of deviations in these characteristics, attention shall be focused on experience of the operator (training), operational procedures, and ergonomics of interface between human and sociotechnical elements.

- Component failure, faulty transmission

This property is an average value of the following characteristics: technical problem and faulty sensor. Both characteristics measure if commands to and from controlled process are forwarded reliably. If the input or output is distorted and does not match reality, it might be a sign of component failure or faulty transmission of information. Then, the focus shall be aimed on a function of actuator, sensor, and communication links.

- Average delay per control loop

This property is an average value of all delays in each element (delay in control algorithm, actuator, process, sensor, process model). Delays and lags are not severe defects of control loop because element’s function is correct in the end. However, delay in performing function of any control element is a precursor of deficiencies embedded in control structure that could lead to not performing activity one day. Delays also decrease efficiency. Frequent delays deserve attention on this phenomenon since a delay can become unacceptably long lag.

5.9 Results of Control Loop Characteristics

Results of analysed control loop are expressed in relative numbers. They calculate number of occurrences assessed with “1” divided by total number of measurements contained in the spreadsheet. All measurements (rows) include a deficiency or failure in its function: delay, wrong decision, faulty action, or incorrect feedback. Percentage can indicate frequency of noncompliance of some element, or in other words, how often specific characteristic of control loop occurs in the spreadsheet database.

Percentage describing function of each element shows distribution of positive and negative outcomes of the element (see Figure 29). A bar chart of each element is placed in the scheme of control loop. Positive function of the element is the left bar. Positive bar comprises of correct (green) and delayed (yellow) function. It must be noted that all measurements contain a deficiency in its function. Therefore, positive bar does not provide absolute performance of the element, but only positive ones recorded control loops which include deviations. Negative (red) function of the element is the right bar which shows the percentage of measurements in which the element fails. Analyst can study the loop how it works, where are deficiencies, and track coherences among elements. Detailed clues where the control actions are inadequate (ineffective) are offered by monitoring of calculated characteristics that are derived from function of each element across one measurement.

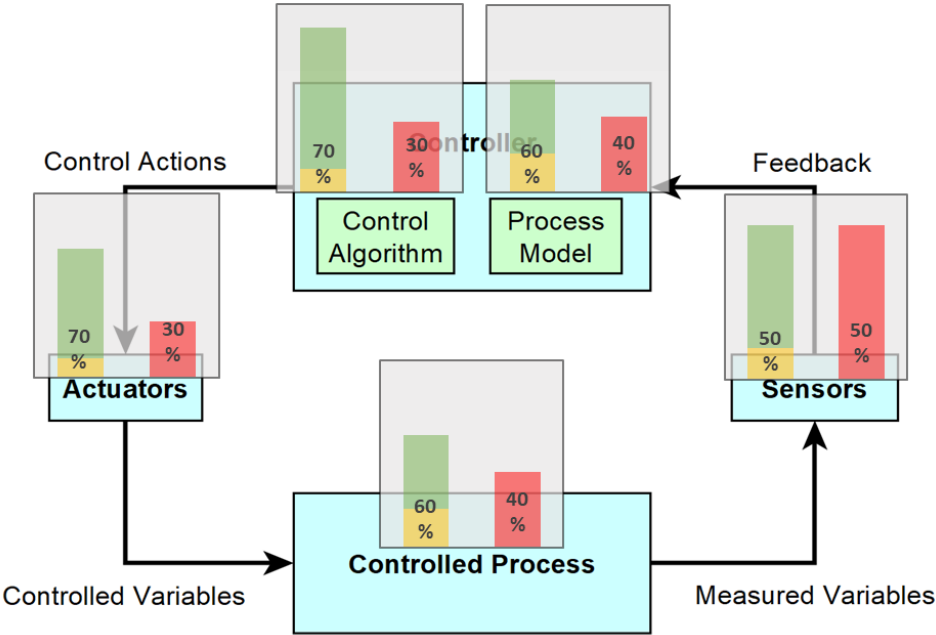


Figure 29 – Bar charts displayed on the scheme of control loop shows distribution of correct (green), delayed (yellow), and incorrect (red) functions of each element

Outcomes of characteristics are displayed in Table 7. They are expressed in percentage in relation to number of measurements. First three characteristics (green label) are positively oriented. They can be considered as resilient characteristics of the system. In the spreadsheet, there shall be as much of these measurements as possible. Measurements in this category are always correctly interpreted by controller which is crucial property in control feedback loops. Remaining four characteristics (red label) are negative. They specify in how many measurements the phenomenon had occurred. High rate of specific characteristics indicates a problem of particular area of the control loop.

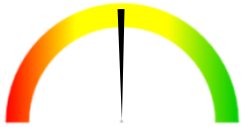
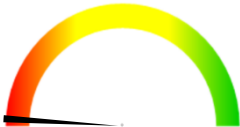
Table 7 – Results of processed data that indicate properties of the control loop

ID	loop works well but contains delay	process does not work but feedback is effective	resilience of controller	inappropriate command	technical problem	faulty sensor	incorrect interpretation
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
total:	20%	10%	20%	25%	5%	30%	10%

Last block of characteristics focuses on control algorithm (see Table 8). These characteristics analyse whether unsafe control action is provided or not, taking into account the correctness of context when the control action is provided. Both characteristics are negative, but it is important to detect the deviation because controller may update his control algorithm then and correct the mistake in next cycle. Therefore, indication of effective feedback is included. The indicator displays the percentage of incorrect control algorithm cases identified by sensor and understood by controller.

Table 8 – Characteristics describing deficiencies of control algorithm and the potential to successfully detect it by means of feedback

ID	controller does not control process	of which identified by effective feedback	controller controls process when should not	of which identified by effective feedback
⋮	⋮	⋮	⋮	⋮
total:	10%		20%	
	identified:	0%	identified:	50%



5.10 Continuous Monitoring

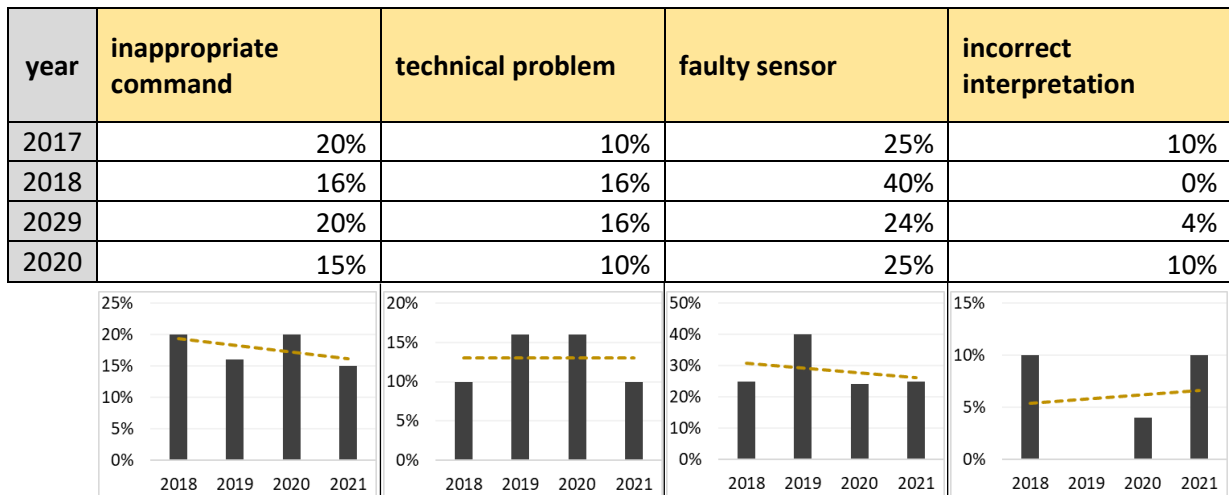
All the calculated characteristics of the control loop may be further monitored in time. Current Safety Management Systems in civil aviation are based on monitoring trends of specific occurrences or other precursors. Trend lines can extrapolate and estimate future behaviour of the system therefore safety manager is aware of actual progress in safety performance.

Outputs and characteristics based on model STAMP and focused on control loop can be monitored as well. Control loop is evaluated in percentage assessing how much are recorded elements functional or non-functional in these specific situations. Results of measurements of the control loop can be compared with measurements that were taken in different time. The progress in different measurement periods can be shown by trend lines comparing the percentage values.

The period of time when measurements are within one time-segment can be various. It can be recorded year by year, per quarters, every month, or different regular time period. It might be also used as an analysis for management of change. The measurements of control loop are performed before the change and new measurements are performed after implementing the change. The change can include modification of procedures or safety requirements. Calculated characteristics of the control loop enable analyst to compare possible change in functionality of loop elements. Trend lines indicate significant deficiencies in providing control actions and receiving feedback.

Table 9 records results of analysis yearly. Data used in this table are arbitrary and serves for description of how trends can be followed. It is focused on negative characteristics of the control loop. The progress of characteristics in time is visualised by bar charts with trend line. Trends may be monitored by safety manager. This visualization of STAMP-based data brings new systemic approach to SMS that is based on treating system by improving system design and enhancing control structure. The control loop is analysed in detail and its progress in functionality can be monitored per each period.

Table 9 - The table monitors results of analyses of a control loop performed year by year in last four years



All characteristics proposed in this thesis can be monitored by bar chart with trend. The chart can be enhanced by other features that add information to visualised data. It might be for example triggers of desired performance or alert level stated by safety objectives of SMS. Advanced view that monitors average delay of elements in whole control loop is based on data in Table 10. Triggers are established to delineate limit level that should not be exceeded as well as target results that are desired to achieve. In this case, a line chart was chosen to emphasise the variability of delayed function (see Figure 30). Similar charts extended for alert and target levels can display various characteristics of the control loop in time.

Table 10 – Advanced monitoring of characteristics of control loop is possible

year	average delay per control loop	alert level	target level
2017	7%	8%	4%
2018	9%		
2019	7%		
2020	5%		

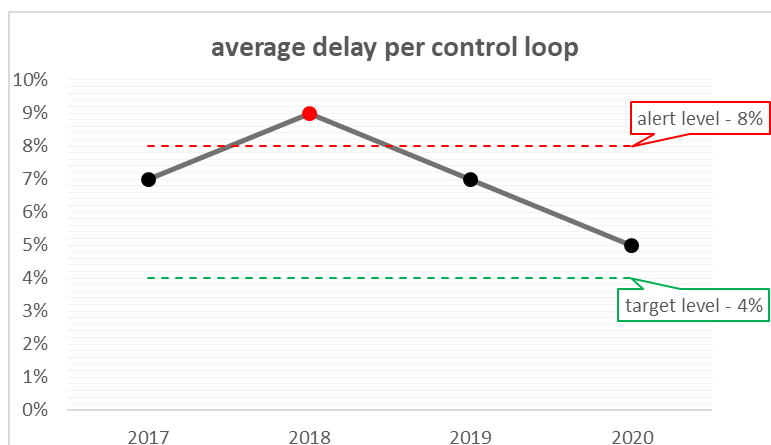


Figure 30 – Line chart upgraded for alert and target levels

5.11 Use of Proposed Method Based on SBIT Database

This chapter explains how to use the proposed method together with SBIT software where the input information is stored. The analysis is based on reports of incidents and accidents stored in SBIT safety database (described in chapter 4). Particular reports from SBIT database serve for validation of the presented method. The analysis of functionality of control loop is performed and visualization of the information is explained. Let us consider, that aviation Safety Management System has performed STPA at the development phase of designing a system. During operations, this SMS observes increasing number of incidents that usually happen during specific phase of operations. It signals that some process deviates more often which shall raise safety manager's attention. This process calls for deeper analysis to find where the problem is. According to STAMP, any mishap is caused by inadequate control therefore control structure shall be checked.

The process that requires more attention by safety manager can be identified in SBIT safety dashboard by tools presented in the previous chapter (schematic map of deviated processes or table which counts unsafe control actions). Now, when the deviated process and activities in it are identified, a control loop or a set of similar control loops is selected for further analysis. Performing proposed method helps to find deficiencies in control structure and clarifies hazardous scenarios leading to mishap. To reach spreadsheet results and subsequent visualization, involved reports processed by SBIT must be found.

To correctly evaluate functionality of a control loop, information from SBIT about the report is needed which indicates how the unsafe control action happened. If more detailed information about the occurrence is available²¹, analyst can use it to better understand the hazardous scenario. Information from each report describing hazardous scenarios serve as a single measurement to fill one row of the spreadsheet. In case of continuous data collection, when numerous measurements are performed and a sample of measurements contains sufficient amount of rows for the spreadsheet, the proposed analysis can start²².

When all SBIT reports involving examined control loops are transformed into values 0, 1, and 1*, spreadsheet is complete. The input data are automatically processed to receive characteristics of the control loop. When control loop's characteristics are calculated, results are shown in arranged table and visualization is displayed. For continuous monitoring, these

²¹ More detailed data can be reached from flight data monitoring systems, observations, inspections, or by querying the pilots.

²² These data must be processed by SBIT to become STAMP-based before entering the proposed analysis.

results may be compared with results of previous analysis of this control loop or can be compared with future analysis of this control loop. The frequency to repeat the measurement should be stated by safety manager.

5.12 Practical Examples of STAMP-based Visualization and Interpretation

The method described above is verified on practical example to validate the proposed method of processing the STAMP-based data. The process of validation finds contributions and limitations of resulted visualization. There are two practical examples performed in this chapter that present how the proposed method can be used in SMS of aviation organisation in practise. Both examples are based on reports from SBIT database. The process selected for further analysis is named “vacating runway and taxiing”. With this process, a reasonable number of incidents and accidents are a part of the database (44 deviations, multiple controllers), so this one is appropriate process for validation and interpretation the results. The two examples vary in controller who controls the process. The first example is fully described, the second one briefly interprets the visualised results.

5.12.1 First Example – Controller Pilot

Let us assume that aerodrome SMS organisation notices growing trend in number of occurrences of process “vacating runway and taxiing”. The proposed method enables analyst to analyse how control loops work and if there is some prevailing property of examined loops that poses hazard. SBIT signalises which unsafe control actions repeat in this process. Analyst chooses specific control loops in the process “vacating runway and taxiing” that should be examined.

In the first example, two control loops from activities (sub-processes) “selecting appropriate exit” and “crossing runway” are chosen because they include several unsafe control actions according to SBIT statistics and both are controlled by pilot. These control loops may correlate as there is the same controller within the same process at similar area of infrastructure. All reports concerning unsafe control action within these control loops are generated from SBIT database. There is 15 of them which means we have 15 measurements to fill in the spreadsheet.

All rows are filled based on instructions provided in Chapter 5.7 (Evaluation of Control Loop Elements). An example of how the report is assessed is explained on report number 5 which is named “vacating runway on adjacent runway”. Pilot controls activity “selecting appropriate exit” and causes unsafe control action “choosing exit not in compliance with aerodrome chart”

which leads to system-level hazard “runway incursion by an aircraft”. Circumstances mentioned in the event description are investigated and the analyst understands the hazardous scenario. Analyst assesses each control loop’s element and fills the results into the spreadsheet. Pilot landed on runway and decelerated successfully. However, pilot selected wrong exit without knowing that it is inappropriate way (it was adjacent runway). So, pilot’s control algorithm was wrong because his command was given at wrong place/ time (value: 0). The actuator’s function was correct because pilot used steering to turn as should do (value: 1). The steering worked well so process of turning out of the runway worked as intended (value: 1). ATC did not detect the deviation of vacating to adjacent runway at all. ATC²³ should be important sensor for pilot’s taxiing since ATC is responsible for monitoring ground movements and pilot did not detect deviation in time as well (value: 0). Fortunately, pilot realised his deviation of vacating to wrong way and immediately stopped the aircraft. Pilot’s process model detected the problem right before entering adjacent runway (value: 1*). Results are following: control algorithm (0), actuator (1), process (1), sensor (0), process model (1*). The values are added into spreadsheet and in this manner whole form is filled.

The Table 11 shows filled spreadsheet where inputs are counted up for each element of the examined control loops. On the right side of the spreadsheet, there are additional information to each row that come from SBIT. Each ID number of a measurement is paired with unique ID number of a report from SBIT database. A name of activity which is connected to unsafe control action (deviation) is written down. If there is any preceding unsafe control action that influenced the examined control loop, its controller is noted for further possible study of why control loop elements do not work as intended. The information about preceding unsafe control action can be found in reporting form in SBIT describing incident or accident, classifying the occurrence and displaying flow of the process. Graphical scheme of interactions is provided by current SBIT safety dashboard.

²³ Including ATC surveillance and alerting systems that support controller to conduct his duties in time.

Table 11 - Inputs from 15 measurements are filled into spreadsheet and functions of elements are counted up; table on the right side shows which report from SBIT is noted, which control loop is examined, and which controller caused prevailing unsafe control action that influences this control loop (footnotes to references (a), (b), (c), (d) are in right bottom corner)

ID	control algorithm	actuator	process	sensor	process model	report ID	activity (control loop)	influenced by controller
1	0	1	1	1	1	report 4	selecting appropriate exit	(a)
2	0	1	1	0	1*	report 5	selecting appropriate exit	
3	0	1	1	1*	1	report 25	selecting appropriate exit	(b)
4	0	0	0	1	1	report 52	crossing runway	
5	1	1	0	0	0	report 67	crossing runway	
6	0	0	0	1	1	report 69	crossing runway	
7	1	0	0	0	0	report 83	crossing runway	
8	0	0	0	1	1	report 84	crossing runway	
9	0	0	0	1	1	report 137	crossing runway	
10	1	0	0	0	1	report 149	selecting appropriate exit	
11	0	1	1	1*	1	report 155	selecting appropriate exit	(c)(d)
12	0	1	1	1	1*	report 167	crossing runway	(c)
13	1	0	0	1	1	report 170	crossing runway	(b)
14	0	0	0	0	0	report 175	crossing runway	(c)
15	0	0	0	0	1*	report 200	crossing runway	(b)(c)(d)
total 1+1*:	27%	40%	33%	60%	80%			
total 0:	73%	60%	67%	40%	20%			
total delay:	0%	0%	0%	13%	20%			
total 1:	27%	40%	33%	47%	60%			

(a)	ATC TWR
(b)	safety manager
(c)	movement area inspector
(d)	infrastructure maintenance personnel

The visualization of the results calculated in spreadsheet is shown in Figure 31. The scheme of examined control loops displays distribution of correct (green), delayed (yellow), and incorrect (red) function of each element. The resulted percentage is related to all 15 measurements and summarises how elements work.

Possible interpretation of visualization focused on control loops of activities “selecting appropriate exit” and “crossing runway” is provided. According to the visualization, the control algorithm is often inadequate. It means that the pilot is not aware how to control the process, how to generate command, or the process is controlled by pilot in inappropriate situation. For instance to examined control loops, consequence of inappropriate control algorithm might be passing assigned exit to vacate runway or crossing runway without clearance. Actuator is performed correctly in 40 % of measurements where a deficiency occurred, in the residual 60 % the command is not adequately/ not correctly applied to control the process. The process works well in less cases than when actuator provides correct control action. According to the bar chart, sensor detects how the process was complied, but the detection is not too reliable. Final interpretation by pilot’s process model is satisfying in 80 % of deviated reports which is quite a good merit of the feedback as two thirds of processes deviate. We can observe few circumstances when feedback is correct but delayed.

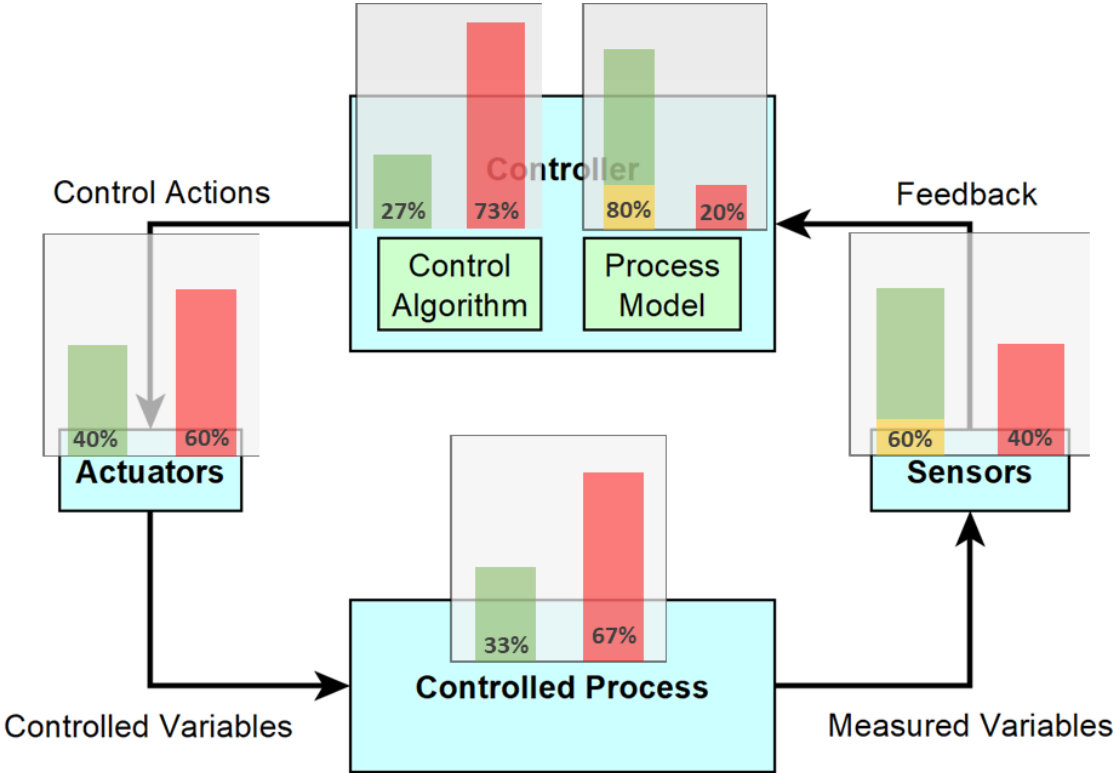


Figure 31 - The scheme of control loop displays whether function of the elements work as intended or not

Characteristics of the submitted control loops are shown in Table 12. The characteristics highlight that when the process is deviated, the sensor and process model are usually able to detect it. The pilot is quite vigilant to detect how control action is fulfilled even when sensor is faulty. In 20 % of cases, pilot knows what control action to provide but the way of providing is wrong. There is a rare case of technical problem and faulty sensor. There is no case of incorrect interpretation of the sensor by controller.

Table 12 - Characteristics of the examined control loops

ID	loop works well but contains delay	process does not work but feedback is effective	resilience of controller	inappropriate command	technical problem	faulty sensor	incorrect interpretation
1	0	0	0	0	0	0	0
2	0	0	1	0	0	0	1
3	0	0	0	0	0	0	0
4	0	1	0	0	0	0	0
5	0	0	0	0	0	1	0
6	0	1	0	0	0	0	0
7	0	0	0	1	0	0	0
8	0	1	0	0	0	0	0
9	0	1	0	0	0	0	0
10	0	0	1	1	0	0	0
11	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0
13	0	1	0	1	0	0	0
14	0	0	0	0	0	0	0
15	0	0	1	0	0	0	0
	0%	33%	20%	20%	7%	7%	0%

The Figure 32 shows that the control algorithm is inadequate in many cases. Sometimes the reason is forgetting to perform a task, sometimes controller performs task at wrong time or place according to context and situational awareness. It is important that these unsafe control actions are detected and understood so corrective action (new control algorithm) will be provided. The speedometer chart indicates on the coloured scale how much the feedback is effective – which means in how many cases sensor and process model correctly captured the control loop’s function. In this example, the feedback is effective when pilot gives wrong command, but he is warned about it and understands what mistake had been made.

ID	controller does not control process	of which identified by effective feedback	controller controls process when should not	of which identified by effective feedback
1	0	0	1	1
2	0	0	1	0
3	0	0	1	1
4	1	1	0	0
5	0	0	0	0
6	1	1	0	0
7	0	0	0	0
8	1	1	0	0
9	1	1	0	0
10	0	0	0	0
11	0	0	1	1
12	0	0	1	1
13	0	0	0	0
14	1	0	0	0
15	1	0	0	0
40%			33%	
identified:		67%	identified:	
			80%	



Figure 32 - Characteristics express the frequency of performing control action in wrong context or not performing control action when required; success of detection of this mishap is expressed in percentage of effective identifications; coloured scale of speedometer chart indicates success of feedback where red means 0 % of deviations detected and green means 100 % of deviations detected

Finally, example of continuous monitoring is provided. The Figure 33 shows three general properties of examined control loops that are based on calculated characteristics and summarise the loop. The results refer to high percentage of occurrences that involve inadequate training or inappropriate procedures. This property could be further monitored in time. Let us assume that the same analysis of the identical control loops is performed year by year. Progress of this value can be monitored in a bar chart and trend line defines the evolution of this property. The

percentage for years 2022, 2023, and 2024 are illustrative. The chart displays downtrend which can be observed across 4 years of measurements.

inadequate training, inappropriate procedures:	31%
component failure, faulty transmission:	7%
average delay per control loop:	7%

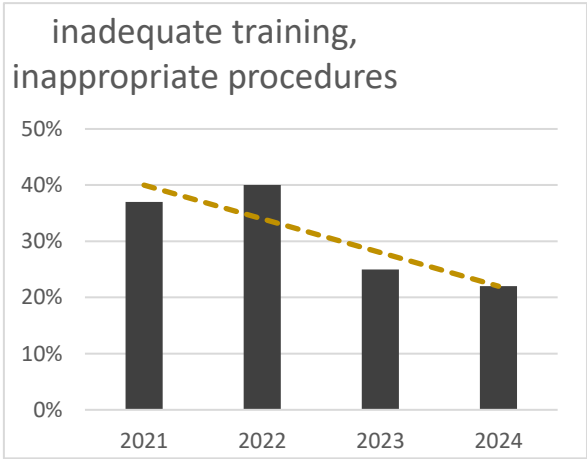


Figure 33 - Three additional characteristics and example of bar chart for continuous monitoring are provided; values for years 2022, 2023, 2024 are random

5.12.2 Second Example – Controller ATC

The second example is briefly explained and is related to the same process “vacating runway on adjacent runway”. The controller is different from previous example and so different control loops are selected. The controller is ATC and analysed control loops are from activities “ATC issuing clearance to cross runway” and “ATC assigning taxi route”. There are 5 related reports found in SBIT database which are crucial for analyst to fill in the spreadsheet (see Table 13).

Table 13 - Spreadsheet of 5 measurements (controller is ATC)

ID	control algorithm	actuator	process	sensor	process model	report ID	activity (control loop)
1	0	1	1	0	1*	report 67	ATC issuing clearance to cross runway
2	0	1	1	0	0	report 78	ATC assigning taxi route
3	1	0	0	0	0	report 83	ATC issuing clearance to cross runway
4	0	1	1	0	0	report 98	ATC assigning taxi route
5	0	1	1	1*	1*	report 188	ATC assigning taxi route
total 1+1*:	20%	80%	80%	20%	40%		
total 0:	80%	20%	20%	80%	60%		
total delay:	0%	0%	0%	20%	40%		
total 1:	20%	80%	80%	0%	0%		
inadequate training, inappropriate procedures:						33%	
component failure, faulty transmission:						30%	
average delay per control loop:						12%	

Visualization of the function of control loop's elements can be seen in Figure 34. The results display that even though control algorithm is usually provided at wrong time or inadequately, process in the end works. The problem of this set of control loops is its feedback. Sensor is ineffective and interpretation by controller is often wrong or delay. That is a worthy information for safety manager to concentrate his attention to sensor and understanding of the situation. ATC lacks feedback to confirm their process was executed. ATC needs to improve sensors to verify their decision that they had provided.

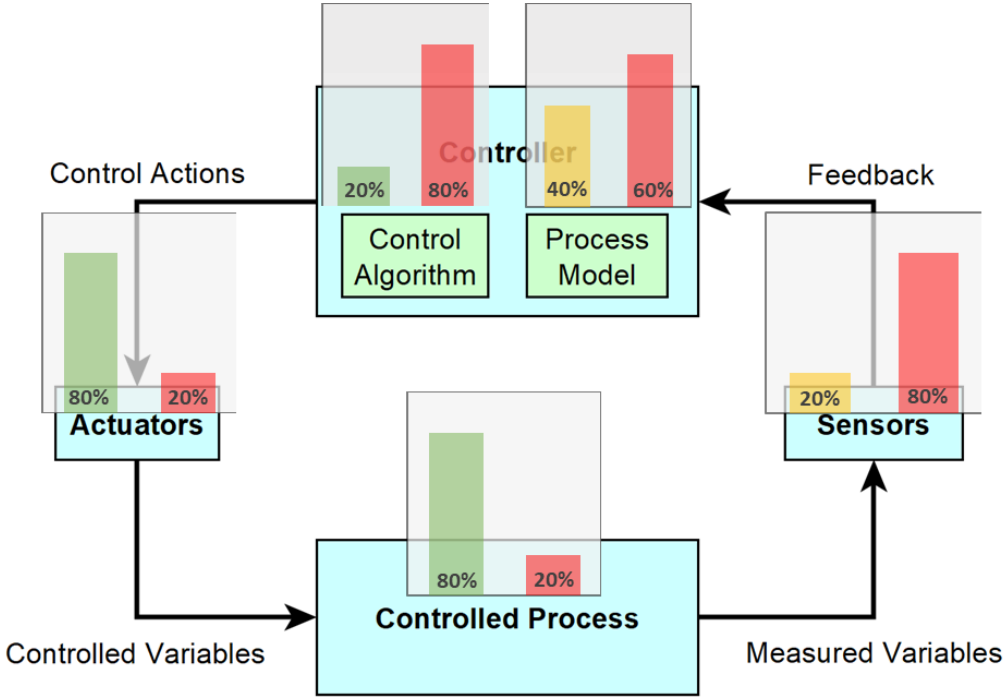


Figure 34 - Characteristics of control loop express what works correctly and what contains some deficiencies

6 Discussion

Additional method based on model STAMP and system's control structure has been introduced. It is focused on a control loop which is selected for further examination to better understand why the hazardous scenario happen. Control loop is identified by safety analyst to perform detailed analysis which reveals deficiencies in functionality of controlling a process, including feedback channel. The method can be used either retrospectively, or proactively. Retrospective method uses reports from accidents and incidents, proactive method uses data from inspections that focus on desired process.

Data from real operations are needed which are further investigated with STAMP-based safety analyses. Analyst inserts data consisted of binary numbers to a spreadsheet and the data are automatically calculated based on elaborated formulas. The outputs are expressed in percentage from all deviated measurements so they can be compared in time with data measured in different period. The analysis covers component failures, human factors, undesired interactions, and unsafe control actions.

This analysis enables analyst to see visualised functionality of elements of examined control loops which is based on information provided by reports from STAMP-based database. The proposed method focuses on control loop elements and monitors whether they work as intended or not. Graphical visualization describes distribution of correct and incorrect function across the loop. The analysis can be also used for continuous monitoring if the collection of data is performed in regular periods. Then, trends are monitored to indicate how deviated functions of elements propagate in the control loop. Proposal of a complete STAMP-based safety dashboard can be seen in Appendix 4 (tool for performing analysis and interpreting results) and visualization for continuous monitoring can be seen in Appendix 5.

6.1 Requirements for Performing Visualization

A detailed analysis of control loop can be performed only in a system that underwent STPA previously. STPA described the system (identified processes), modelled the control structure, identified control actions in control loop, and found scenarios leading to hazards. If safety manager is not sure whether some process is controlled effectively, the proposed method is appropriate to examine the control loop/ set of similar control loops. Analyst should perform this analysis, if the system is experiencing design changes, if there is a rising trend in deviations of the process, or if inspections, audits, observations, mandatory or voluntary reports indicate

that safety constraints are not enforced or followed. If assumption-based leading indicators are established, their violation is also a trigger for performing this analysis. If the data are collected automatically, collection may run continuously or information might be taken from safety database of incidents and accidents, in other cases analyst's presence is needed to collect the data. Data can be collected in real time during operations or retrospectively which is not preferred as there could be some gaps in data completeness.

Reliable data collection is crucial input for the analysis. The collected data are processed by SBIT on which is the proposed method based. Analyst follows the proposed assessment of each element using values "1", "1*", and "0". Analyst should detect every deviation, inadequate control action, noncompliance, or distorted feedback. Measurements of control loop that did not contain any deficiency in functionality are disregarded for keeping the spreadsheet reasonably arranged. The intention of the proposed method is not to predict probabilities. The analysis' aim is to find deficiencies that repeat frequently and concentrate on enforcing safety constraints, generating adequate control actions related to context, and ensuring effective feedback according to theory of model STAMP.

6.2 Limitations of the Proposed Method

The proposed method generates a lot of binary data to monitor from deviated control loops. They would not be probably identified using other non-systemic analyses. In return for this, there are some limitations coming in hand with proposing new visualization of STAMP-based data. The limitations are especially in data collection, the evaluation of control loop can be affected by analyst's subjectivity, and one analysis is focused mainly on one process which can be a bit isolated view in case of interactions with other processes.

Following bullets further describe identified limitations of the proposed method:

- Lack of collected data

There could be lack of collected data especially in smaller aviation organisations. There are some processes where unsafe control actions take place extremely rarely. There might be not enough reports in the safety database to analyse them retrospectively. In case of proactive (on-site) inspection, an analyst that personally measures the data would spend unreasonably long time to collect sufficient sample of deviated data. In some processes, it is possible to measure data by digital means of monitoring which make the data collection much easier.

- Lack of detailed information collected

If narrative of the report which describes the context and scenario is not complete or detailed enough, it is hard to precisely evaluate the control loop's elements by the analyst. Especially process model (= interpretation by controller whether process was carried out) can be hard to evaluate without completed narrative. The best way to receive information needed is to interview the controller about his point of view to reveal the scenario leading to hazard.

- Distorted evaluation of control loop

Although there are instructions provided how to assess each element in the loop, it is impossible to avoid subjectivity of analyst's opinions during evaluation. Proposed instructions struggle to mitigate divergence from the most accurate evaluation when the same control loop is assessed by various analysts in different time.

- More sensors are considered as one

In control loop where there are more sensors to measure variables of controlled process, these individual sensors are considered as one set that provides feedback. The detail of each sensor's function cannot be seen. The general function of set of sensors is crucial. It means that if there are three sensors to measure variables but only one of them works, it is sufficient for controller to understand it and sensor in general works as intended which is important. The same assumption is valid for the case of more actuators.

- Distortion of the results when analyst's focus is changed

If analyst repeats proposed analysis of a control loop as a part of continuous monitoring process, the measurements should be performed in the same manner as previous measurements. There could be a case that analyst changes his emphasis or records different data than previously which causes distortion of the results of loop's characteristics. For example, if reporting system or analyst records many more cases of delayed functions in the control loop, the spreadsheet is filled with values "1*" and overall percentage is distorted (lower than the previously performed analysis).

- Focus on one particular process

The proposed method is concentrated on functionality of particular process. It means that the analyst does not search for other sources of undesired interactions but focuses on how the control loop works within the system. If emergent properties cause deviations in the examined control loop, degraded performance of the loop is reflected in visualization as incorrect function of some element. The method follows systemic approach to some degree. If there is some preceding unsafe control action which influences the examined activity (control loop), its controller is mentioned next to spreadsheet. Interactions are not explicitly expressed in visualization. In current SBIT database, the schematic map which shows exclusively undesired interactions among processes can be seen and followed up.

6.3 Advantages of Visualization

This analysis is additional to tools for visualization contained in SBIT dashboard²⁵. The thesis suggests a method of visualizing STAMP-based data which could support implementation of model STAMP and derived methodologies into operations. The analysis might be used in any field of aviation where Safety Management System exists (that is airport, air service provider, air operator, maintenance, handling, manufacturer). The proposed method could be also used at the regulatory level (national and international) that would monitor specific phenomenon and would have access to more data from operations.

The proposed method can be used based on one of two approaches – retrospectively or proactively. Retrospective analysis is based on investigated reports of incidents and accidents that are stored in STAMP-based database. Proactive analysis intentionally collects data during inspections to find deficiencies in examined control loops. These data are processed by SBIT and continually analysed by the proposed method.

Performing this analysis is not too demanding for resources. Hazard analysis (STPA) is required to be performed in the system. STAMP-based software which provides reporting system and occurrence database is needed. Only one analyst²⁶ or one expert team is needed to convert observed data into values “1” (correct, adequate), “1*” (correct, adequate but delayed), and “0” (incorrect, inappropriate). The evaluation of control loop is performed based on rules proposed in this thesis. The rest of data processing is fully automated using formulas in spreadsheet. The

²⁵ The proposed method does not have to be conducted in SBIT, other STAMP-based software can be used.

²⁶ If expert team is available, experts might cooperate together to bring more objectivity into assessment.

STAMP-based data visualization is automatic as well as monitoring of changes in functionality of the control loop.

The proposed method enables to collect information about hazardous scenarios that would be normally lost or not visualised. The method analyses control loop which involves deficiencies. In the spreadsheet, negative data are recorded as well as positive data about correct function of loop's elements. Recorded data come from day-to-day operations and processed data are not strictly focused on negative outcomes.

Monitoring of delays as precursors of degraded functionality is a great indicator which element should safety manager focus on. Characteristics of the control loop specify the prevailing hazardous scenario based on functionality of loop's elements. Characteristics important for safety manager can be determined as key safety performance indicators for continuous monitoring in time. The proposed method can be followed up and further developed by researchers to be more suitable for particular SMS. Charts of different characteristics can be monitored.

Systemic approach copes with interactions among components that are hard to manage. Sophisticated system design and thorough control structure can manage emergent properties. Undesired interactions are observed in control loops as well. That is why there is a feedback to verify if process was executed as previously planned. Enforcing constraints by control loop improves safety performance of the whole system. The proposed method emphasises the importance of feedback channel in contrast to other analyses. Sensor and process model are crucial elements that significantly influence generating new control algorithm which is, with incorrect interpretation of how process had been executed, a source of unsafe control actions.

The proposed visualization presents STAMP-based information graphically and by quantitative means. The outcomes of STAMP-based safety analyses are plain text (controller, unsafe control action, context, scenario). Some of the information provided by the proposed method is visualised which can better serve to safety managers and enables continuous monitoring. Additionally, visualization of STAMP-based data continuously monitors progress in functionality of the loop per period. Alert trigger and target level can integrate chart into current SMS safety dashboard. Trends and distribution of control loop deficiencies are graphically represented and thus they are easier to interpret. The analysis is a simple tool to analyse functionality of set of control loops in detail and encourages to propose new safety requirements for the system.

7 Conclusion

The purpose of this diploma thesis was to visualise outputs from hazard analyses based on System-Theoretic Accident Model and Processes (STAMP). To reach this goal, current safety management approach was described, and STAMP-based methods were studied. A safety database composed of air accidents and incidents that is compatible with model STAMP was created. The results provided by the current safety dashboard of software STAMP-based Investigation Tool (SBIT) were analysed and interpreted to understand which data could be further processed and visualised in the new proposal of visualization.

As the first assignment, the safety database was established in SBIT with focus on aerodrome processes. Model of control structure was modelled by graphical representation Business Process Model and Notation (BPMN) in order to import description of processes to SBIT. Unsafe control actions with context were identified thanks to System-Theoretic Process Analysis (STPA). After sufficient number of reports was processed by SBIT and stored in STAMP-based database, the SBIT database was ready for introducing proposal of new safety dashboard.

It was found out that results of STAMP-based analyses are qualitative data that are suitable for decision-making rather than statistics. Key outputs of STPA like unsafe control actions and scenarios are the worthiest in their essential form as a compact text. They are not appropriate for visualization. The focus moved to control structure which consists of control loops. A control loop is the only active means how to control processes. The second assignment proposed a method how to process STAMP-based data in different way that leads to visualization.

The proposed method analyses how control loops work. The method how to collect data about functionality of a control loop and process them was proposed. It is applicable in all aviation systems that had undergone STPA. If any process is identified as deviating by Safety Management System, or if assumption-based leading indicators are violated, the detailed analysis of appropriate set of control loops shall run. Knowledge received from analysis' outputs supports adoption of new safety requirements for the system to reinforce control structure.

The analysis examines all elements of a control loop, either retrospectively (based on incident reports) or proactively (inspections during operations). If there are any deficiencies, unsafe control actions, incorrect functions, or inadequate feedback, they are recorded by analyst. Deviated control loops are identified and relevant reports found. Information obtained from the

reports is converted into quantitative data which enables graphical representation of the outputs. Analyst evaluates functionality of each control loop's element (control algorithm, actuator, controlled process, sensor, process model) as correct (value: "1"), correct but delayed (value: "1*"), or incorrect (value: "0"). There is a proposed guidance (instructions) to keep the evaluation objective as much as possible. All deviated measurements are filled into automated spreadsheet (one measurement of control loop = one row in spreadsheet).

The outputs present distribution of correct, delayed, and incorrect function of each element. Some correlations were found in each measurement that further describe characteristics of the control loop. The results are presented in percentage related to number of deviated measurements. The effectivity of feedback is included. These outputs can be further continuously monitored to compare progress of control loop's functionality in time. Monitoring trends is what current aviation Safety Management Systems require.

Two practical examples of process "vacating runway and taxiing" were provided to better describe the method. The examples validated and verified effects of the analysis. The first example was focused on control loops controlled by pilot, the second example was concentrated on loop's controlled by ATC. Analyses for both examples were performed, and the results shared information which elements of the loops include control deficiencies. Visualization displayed the outcomes in graphical scheme. Some limitations as well as contributions were observed and described.

The analysis copes with human factors, component failures, system design, unsafe control actions, and undesired interactions. Its significant benefit is in monitoring of effectivity of feedback channel which influences subsequently generated control actions. The proposed safety dashboard displays processed STAMP-based data visually and provides a tool for continuous monitoring of selected control loops and their characteristics. The characteristics indicate why hazardous scenarios usually happen.

The limitations are associated with data collection in order to evaluate all elements in the control loop correctly by analyst. The proposed method is focused on specific process and does not visualise interactions coming from other processes. However, degraded functionality of examined control loop is always reflected.

The proposed method how to analyse a control loop promotes embedding STAMP-based techniques into aviation organisations to manage safety of operations more effectively. Systemic approach ensures finding deficiencies in system control structure. Visualization of

STAMP-based data enables deep analysis of specified control loops with information about properties of the loop. Regular measuring of control loop functionality provides monitoring trends in time.

This diploma thesis can be followed up by research focusing on control loops. The proposed method can be continued by searching for more correlations in the spreadsheet. There might be some correlating values within each measurement that were not identified but could be worth to monitor. Finding new correlations would lead to establishing new characteristics of the control loop or detecting new causal factors. Another idea that could be developed is to compare process model of previous control loop with new control algorithm in order to find out possible influence of information available for controller. It would clarify in which cases controller provides inadequate control action based on missing/ wrong feedback. Last future prospect is to apply proactive approach in practice (real operations), that is, to select problematic process, run inspections for collecting data, process the data to STAMP-based database, conduct the proposed analysis, repeat the inspections after specific time period, compare the results, and monitor the trend lines in safety dashboard.

References

- [1] B. Disaster Management Institute, “The Domino Theory,” [Online]. Available: <http://www.hrdp-idrm.in/e5783/e17327/e24075/e27357/>.
- [2] A. Safety, “Accident Causation,” [Online]. Available: <https://www.aviationsafetyplatform.com/pedia/understanding-safety/general/accident-causation>.
- [3] ICAO, “Document 9859 - Safety Management Manual,” 2018 (fourth edition). [Online]. Available: <https://www.skybrary.aero/bookshelf/books/5863.pdf>.
- [4] EU, “REGULATION (EU) No 376/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” 2014. [Online]. Available: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0376&from=CS>.
- [5] SKYbrary, “Safety Management,” 2021. [Online]. Available: https://www.skybrary.aero/index.php/Safety_Management.
- [6] P. Airport, “Safety Expertise,” [Online]. Available: <https://www.prg.aero/en/node/5188>.
- [7] ICAO, “Action Plan for the Establishment and Implementation of Safety Data Collection and Processing Systems (SDCPS),” 2018. [Online]. Available: https://www.icao.int/SAM/Documents/2018-SSP7/Action%20Plan_SDCPS.pdf.
- [8] S. M. I. C. Group, “Measuring Safety Performance Guidelines for Service Providers,” 2013. [Online]. Available: <https://www.skybrary.aero/bookshelf/books/2395.pdf>.
- [9] Britton and Tyler, “Aviation Safety Dashboard,” 2019. [Online]. Available: <http://aviationsafetyblog.asms-pro.com/blog/4-pillars-how-to-conduct-safety-performance-monitoring-and-measurement>.
- [10] ICAO, N. MURAD and M. MERENS, “M6 - Visualizations,” 2019. [Online]. Available: M6 - Visualizations (ICAO).

- [11] E. Commision, "Aviation Safety Dashboards - Future Sky Safety," 2019. [Online]. Available: <https://safeorg.eu/2019/07/19/aviation-safety-dashboards-paper/>.
- [12] A.-6. Workshop, "Safety Performance Measurement - SPI & ALoSP Developement," 2015. [Online]. Available: https://www.icao.int/APAC/Meetings/2015%20APRAST6/07%20-%20SIN_SPM%20Presentation.pdf.
- [13] Eurocontrol, "Systems Thinking for Safety: Ten Principles," 2014. [Online]. Available: <https://www.skybrary.aero/bookshelf/books/2882.pdf>.
- [14] K. M. Adams, "Systems Theory as the Foundation for Understanding Systems," 2013. [Online]. Available: <https://onlinelibrary.wiley.com/doi/epdf/10.1002/sys.21255>.
- [15] N. Leveson, *Enineering a Safer World*, MIT Press Ltd, 2011.
- [16] N. Leveson, "Engineering a Safer and More Secure World," 2019. [Online]. Available: <http://sunnyday.mit.edu/workshop2019/STAMP-Intro2019.pdf>.
- [17] N. Leveson, "A New Accident Model for Engineering Safer Systems," 2003. [Online]. Available: <http://sunnyday.mit.edu/accidents/safetyscience-single.pdf>.
- [18] J. Ladyman, "What is a compex system?," 2016. [Online]. Available: https://www.researchgate.net/publication/50210075_What_is_a_complex_system.
- [19] N. Leveson and J. Thomas, "STPA Handbook," 2018. [Online]. Available: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf.
- [20] D. S. Castilho, "Active STPA: Integration of Hazard Analysis into a Safety Management System Framework," 2019. [Online]. Available: <https://dspace.mit.edu/handle/1721.1/124172>.
- [21] A. Abdulkhaleq, "XSTAMPP 2.0: New Improvements to XSTAMPP Including CAST Accident Analysis and an Extended Approach to STPA," 2016. [Online]. Available: <https://elib.uni-stuttgart.de/bitstream/11682/8766/1/XSTAMPP%202.0-%20New%20Improtvements%20to%20XSTAMPP%20including%20A-CAST%20plugin%20support%20to%20CAST%20Accident%20Aanalysis%20.pdf>.

- [22] J. Thomas, "MIT's STAMP Research and STPA Applications," 2018. [Online]. Available:
https://www.amsterdamuas.com/binaries/content/assets/subsites/aviation/icsc/icsc2018/eswc-2018-presentations/eswc2018_session2_01_mit-stamp-research-and-stpa-application.pdf?1542643121824.
- [23] ICAO, "Safety Management System Overview," 2018. [Online]. Available:
<https://www.icao.int/MID/Documents/2018/Aerodrome%20SMS%20Workshop/M0-2-SMS%20Overview.pdf>.
- [24] N. Leveson, "CAST Handbook," 2019. [Online]. Available:
<http://sunnyday.mit.edu/CAST-Handbook.pdf>.
- [25] D. R. MONTES, "Using STPA to Inform Developmental Product Testing," 2016. [Online]. Available: <http://sunnyday.mit.edu/papers/Montes-Thesis-final.pdf>.
- [26] B. Antoine, "SYSTEMS THEORETIC HAZARD ANALYSIS (STPA) APPLIED TO THE RISK REVIEW OF COMPLEX SYSTEMS: AN EXAMPLE FROM THE MEDICAL DEVICE INDUSTRY," 2013. [Online]. Available:
<https://dspace.mit.edu/handle/1721.1/79424>.