CZECH TECHNICAL UNIVERSITY IN PRAGUE

Faculty of Transportation Sciences

Department of Air Transport

Safety Data Collection and Processing According to STAMP in Aviation Maintenance

Master's Thesis

Study programme: Technology in Transportation and Telecommunication

Study field: Air Traffic Control and Management

Thesis advisors: Ing. Andrej Lališ Ph.D.

Bc. Natalia Guskova

Prague 2020

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. Natalia Guskova

Kód studijního programu a studijní obor studenta:

N 3710 – PL – Provoz a řízení letecké dopravy

Název tématu (česky): **Sběr a zpracování dat o bezpečnosti dle teorie modelu STAMP v letecké údržbě**

Název tématu (anglicky): Safety Data Collection and Processing According to STAMP in Aviation Maintenance

Zásady pro vypracování

Při zpracování diplomové práce se řiďte následujícími pokyny:

- Cíl práce: Návrh sběru a zpracování dat o bezpečnosti dle teorie STAMP v organizacích letecké údržby
- Analýza provozní dokumentace a dat o bezpečnosti leteckých údržbových organizací
- Analýza systémového modelu bezpečnosti STAMP a metodik CAST/STPA
- Návrh a tvorba vybraných částí provozní dokumentace dle teorie STAMP
- Návrh postupu pro sběr a zpracování dat o bezpečnosti dle teorie STAMP v kontextu navržené provozní dokumentace leteckých údržbových organizací
- Vyhodnocení navrženého řešení

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.

Allweyer, T. BPMN 2.0: Introduction to the Standard for Business Process Modeling. 2nd Ed, Books on Demand 2016.

Vedoucí diplomové práce: **Ing. Andrej Lališ, Ph.D.**

Datum zadání diplomové práce: **17. července 2019**
(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: **18. května 2020**

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

L.S.

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní

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

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

Potvrzuji převzetí zadání diplomové práce.

Bc. Natalia Guskova
jméno a podpis studenta

V Praze dne.. 17. července 2019

CZECH TECHNICAL UNIVERSITY IN PRAGUE
Faculty of Transportation Sciences
Dean's office
Konviktská 20, 110 00 Prague 1, Czech Republic

K621 .... Department of Air Transport

MASTER'S THESIS ASSIGNMENT

(PROJECT, WORK OF ART)

Student's name and surname (including degrees):

Bc. Natalia Guskova

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

N 3710 – PL – Air Traffic Control and Management

Theme title (in Czech): **Sběr a zpracování dat o bezpečnosti dle teorie modelu STAMP v letecké údržbě**

Theme title (in English): Safety Data Collection and Processing According to STAMP in Aviation Maintenance

Guides for elaboration

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

- Thesis goal: Proposal of safety data collection and processing based on STAMP for maintenance, repair, and overhaul organizations
- Process documentation and safety data analysis of aviation maintenance, repair and overhaul organizations
- Analysis of STAMP systemic model of safety and CAST/STPA methodologies
- Proposal and creation of selected parts of process documentation according to the theory of STAMP
- Proposal of safety data collection and processing procedure based on STAMP in the context of the proposed process documentation of aviation maintenance, repair, and overhaul organizations
- Evaluation and summary

CTU CZECH TECHNICAL UNIVERSITY IN PRAGUE

Graphical work range: according to the instructions of thesis supervisor

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

Bibliography:

Leveson, N. Engineering a Safer World: Systems Thinking Applied to Safety. MIT Press, 2012.

Leveson, N., Thomas, J. STPA Handbook, 2018.

Allweyer, T. BPMN 2.0: Introduction to the Standard for Business Process Modeling. 2nd Ed, Books on Demand 2016.

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

Date of master's thesis assignment: **July 17, 2019**
(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 18, 2020**

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

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE Fakulta dopravní L.S.

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. Natalia Guskova
Student's name and signature

Prague .... July 17, 2019

Declaration

I hereby declare, that I did elaborate and write this thesis by myself and all used information and scientific resources are in line with methodological instructions for ethical preparation of university thesis.

I have no serious motives against using this educational work according to the § 60 of Act of the Czech Republic No. 121/2000, on Copyright and Rights Related to Copyright and on Amendment to Certain Acts (the Copyright Act)

In Prague, May 2020

Гуськова ....

Bc. Natalia Guskova

Acknowledgement

I would like to thank my supervisor Ing. Andrej Lališ Ph.D. for his professional advices, patience and supporting during thesis writing. Also, I would like to thank Czech Airlines Technics a.s., for professional consultations, advices and providing documentations needed for work developing.

Last, but not least, I would like to thank to my family and friends for the valuable support and faith in my strength during thesis creation.

Abstrakt

Cílem této práce je navrhnout systém sběru a zpracování bezpečnostních dat založený na STAMP pro organizace údržby letadel. Na začátku práce byly identifikovány mezery ve sběru měkkých bezpečnostních dat. Dále pro účely bezpečnostní analýzy byl vybrán model se systémovým pohledem na provozní bezpečnost (STAMP). Poté byly procesy údržbové organizace namodelovány pomocí jazyka BPMN 2.0. Taktéž modely byly rozšířeny o artefakty založené na STAMP. Navržené řešení bylo úspěšně ověřeno interními daty od údržbové organizace. Toto řešení lze také použít k vývoji panelu ukazatelů bezpečnosti a vytvoření kompletního nástroje pro řízení provozní bezpečnosti založeného na Safety-II.

Klíčová slova

sběr a zpracování dat o bezpečnosti, panel ukazatelů bezpečnosti, STAMP, CAST, STPA, MRO, BPMN

Abstract

The goal of this thesis is to propose safety data collection and processing system based on STAMP for maintenance, repair, and overhaul organizations. As first, gaps in soft safety data collection were identified. Next, STAMP systemic safety model was chosen for a safety analysis purposes. After that, MROs processes were modelled in BPMN 2.0 language extended by STAMP based artefacts. Proposed solution was successfully validated with internal soft data from an MRO organisation. The proposal solution can be used to develop safety dashboards and to create a complete Safety - II safety tool.

Keywords

safety data collection and processing, safety dashboards, STAMP, CAST, STPA, MRO, BPMN

Table of contents

Acronyms and abbreviations

AD	Airworthiness Directive
ADREP	The Accident/Incident Data Reporting system
AL	Airworthiness Limitations
AMO	Approved Maintenance Organisation
AMP	Aircraft Maintenance Program
BPMN	Business Process Model and Notation
CAMO	Continuing Airworthiness Management Organisation
CAA	Civil Aviation Authority
CAST	Causal Analysis based on System Theory
CMR	Certificate Maintenance Requirements
CSAT	Czech Airlines Technics, a.s.
CZE	Czech Republic
EASA	European Union Aviation Safety Agency
EC	European Commission
ECR	European Central Repository
EU	European Union
ECCAIRS	European Co-ordination centre for Accident and Incident Reporting Systems
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
IORS	International Occurrence Reporting System
MGS	Maintenance Steering Group
MOE	Maintenance Organisation Exposition
MPD	Maintenance Planning Document
MRBR	Maintenance Review Board Report
MRO	Maintenance, Repair and Overhaul
MSR	Maintenance Safety Report
NTSB	National Transportation Safety Board
SB	Service Bulletin
SBIT	STAMP Based Investigation Tool
SDCPS	Safety data collection and processing system
SPI	Safety Performance Indicator
STAMP	System-Theoretic Accident Model and Processes
STPA	Systems Theoretic Process Analysis
THC	Type Certificate Holder
UFO	Unified Foundational Ontology

Introduction

Nowadays, aviation affects almost everyone's life in many ways. That is why it is necessary to collect various data about it and analyse it.

For most, the data collected for analysis refer to economic indicators, destinations, aircraft types, passenger flow and etc. So, everything, what you can count and then do some statistics. Such data type is called hard data. However, there are some data which are necessary to collect but is not really possible to measure them. Such data is called soft data.

In aviation safety, soft data represent descriptions of occurrences. Those data contain almost all important information from a situation, for example occurrence analysis, root causes, contributing factors. Mostly, that data are collected in narrative text. It makes it difficult to measure them and do statistical evaluation.

ICAO requires that data which can have an impact on safety, have to be captured, stored, aggregated and analysed. The appropriate way how to resolve this, according to ICAO, is to develop an SDCPS – Safety data collection and processing system. [3] There are some SDCPS systems developed nowadays. However, there is a problem, that such systems do not have appropriate module, to aggregate and analyse data described in the narrative text.

There is a way, how to classify (collect) factors (part of soft data) from the narrative text from occurrence reporting. It is possible by dedicated taxonomies like ECCAIRS or ADREP, which contain definition of aviation events. Using taxonomies, in some SDCPS systems specific soft data can be recorded without loss of important information. However, not all air transport stakeholders can find suitable taxonomy to classify and store their data.

For instance, unlike airports or air navigation service providers, maintenance organisations cannot use ECCAIRS and ADREP in their SDCPS systems at all. That taxonomies are limited in their coverage of maintenance, that does not match the complexity of MRO operations. There are lot of different processes which are based on the type of labour, type of a check or, of course, on an aircraft type.

According to that problem with important soft safety data, I will try to propose the architecture or workflow of a new safety data collection and processing, that can be used in a new SDCPS system in maintenance, repair, and overhaul organisations in this thesis.

Soft data, which are described in the narrative text need a special view in safety dashboards. Nowadays safety dashboards contain safety performance indicators based on only part of them. Regarding the fact, that maintenance organisation is a sociotechnical system and contains different type of data (hard and soft), it is essential to choose some safety analysis, which can work with such a system.

On the other hand, safety theory offers some new models and methods, that are dedicated to this type of problem and can be used. Nowadays, new approach to safety (called Safety-II) can help find a solution how to analyse the soft data. Safety-II offers systemic models and methods, which can work with systems as a whole. This thesis will be focused on STAMP safety model, which is one of the systemic models.

STAMP has great potential to change existing approach to today's SDCPS as in the aviation, SDCPS systems are not using systemic approach today.

For the validation purposes my thesis was done in cooperation with the Czech Airlines Technics, a.s. (CSAT). CSAT is an important Czech maintenance company, with over 90 years' experience in aviation maintenance, repair and overhaul. Thanks to their permission, I could test data collection on their intern data.

Additionally, some parts from this thesis were performed during my support activity in a research project No. TJ01000377 – Research of Intelligent Components for Safety Data Collection and Processing Systems, funded by the Technology Agency of the Czech Republic. The goal of this project was to expedite, simplify and make more accurate the process of risk analysis and control as well as achieving more accurate safety performance monitoring for aviation organisations.

1. Theoretical Framework of MRO

Maintenance, Repair and Overhaul organisation (MRO) is an organisation, which is approved to provide maintenance activities to aircraft. The main goal of MRO organisation is to provide activities to continue aircraft airworthiness. According to ICAO document 9760 "Airworthiness Manual" 3rd Edition 2014, the Continuing Airworthiness means:

"The set of processes by which an aircraft, engine, propeller or part complies with the applicable airworthiness requirements and remains in a condition for safe operation throughout its operating life." [1]

1.1 Legislation

Activities, which are provided in aviation are mostly supported by aviation legislation. Depending on different factors, like a country, where activities are provided or a state, where organisation is certificated, aviation providers have to follow current legislation framework.

1.1.1 MRO world legislation framework

Requirements for aircraft airworthiness are written in different aviation documents. The main aviation regulation document in the Czech Republic is an Act. No. 49/1997 Coll., on Civil Aviation and on amendment of Act No. 455/1991 Coll., Trade Licensing Code, as amended. In chapter 2 there is an information about aircraft airworthiness. The most interesting for this thesis is Section 12a. The Civil Aviation Authority of the Czech Republic has to collect and process all the data relevant to aviation safety, which are related to the technical and operational condition of aircraft. This type of information is mostly received from the maintenance organisations. According to point "d", the data relevant to safety aviation has to contain particular attributes from the investigation of causes of accidents and incidents.

Act. No. 49/1997 Coll. is based on the Convention on International Civil Aviation. Annexes to the Convention then include details agreed with respect to various aviation operation domains. There are 19 Annexes today. Annex 6 "Aircraft Operations" and Annex 8 "Airworthiness of Aircraft" contains information about aircraft airworthiness and its continuing. According to these Annexes, MRO organisations have to send CAA related safety data. That data has to be collected, analysed and exchanged between states. More guidance on how to work with safety data is provided in Annex 19 and Safety Management Manual (ICAO Doc. 9859) [7] [8] [9] [3]

According to Annex 19, safety data is a defined set of facts or set of safety values collected from various aviation-related sources. They are used to maintain or to improve safety. Safety data are collected from accident or incident investigations, safety reporting, continuing airworthiness reporting, operational performance monitoring, inspections, audits, surveys or from safety studies and reviews. [10]

As stated in Chapter 5 ICAO Safety Management Manual (Doc. 9859) *"Service providers are required to develop and maintain the means to verify their safety performance with reference to their SPIs and SPTs, in support of their safety objectives by means of SDCPS. They may be based on reactive and proactive methods of safety data and safety information collection[1]".* Some of that data originate from occurrence reporting and investigation. Approved maintenance organisation is a one of such service providers. That means that MRO organisations have to maintain their own safety database, where they collect own safety data. [10] [3]

All in all, it is important to understand why ICAO requires the implementation of SDCPS. SDCPS provides fundamental safety data and safety information to safety performance management. Safety performance monitoring and measurement is the main part of the third SMS framework component - Safety assurance. There are four SMS framework components shown in table 1. [3]

As stated in Annex 19, states shall require the approved maintenance organisations to implement an SMS. That means that MRO organisations have to create their own SMS according to Annex 19 and Safety Management Manual (ICAO Doc. 9859). This SMS system has to obtain all SMS framework elements, including Safety assurance. Safety assurance is used to identify whether the SMS is operating according to predetermined expectations and requirements. [3] [10]

---

[1] *"Safety data is what is initially reported and recorded as the result of an observation or measurement. It is transformed to safety information when it is processed, organized, integrated or analysed in a given context to make it useful for management of safety" [3]*

Table 1 "Components and elements of the ICAO SMS framework" [3]

Component	Element
1. Safety policy and objectives	1.1 Management commitment
	1.2 Safety accountability and responsibilities
	1.3 Appointment of key safety personnel
	1.4 Coordination of emergency response planning
	1.5 SMS documentation
2. Safety risk management	2.1 Hazard identification
	2.2 Safety risk assessment and mitigation
3. Safety assurance	3.1 Safety performance monitoring and measurement
	3.2 the management of change
	3.3 Continuous improvement of the SMS
4. Safety promotion	4.1 Training and education
	4.2 Safety communication

In fact, MRO organisations have to have their own SDCPS system. In figure 1 there is an explanation of how Safety performance management is connected with a data collection system.

Safety performance management has four steps, which are checked and controlled by appropriate safety analysis. This safety analysis takes relevant safety data and safety information from SDCPS. After that safety managers can identify trends, make decisions and evaluate safety performance. [3]

SDCPS is a generic term, which is used to describe processing and reporting systems, databases and schemes for exchange of safety information and recorded information. The view and construction of those systems are imaged by specialists. They evaluate which type of data and in which way an organisation has to collect and process. [3]

For Approved Maintenance Organisation typical safety data and safety information sources are: Mandatory occurrence reports, voluntary reports, risk assessment register, SPIs/trend analysis, internal audits, quality programme reports, training records, service difficulty reports (SDR), In-service occurrence reports, maintenance and operational experience reports, service information reports (faults, malfunctions, defects), unapproved parts reports. [3]

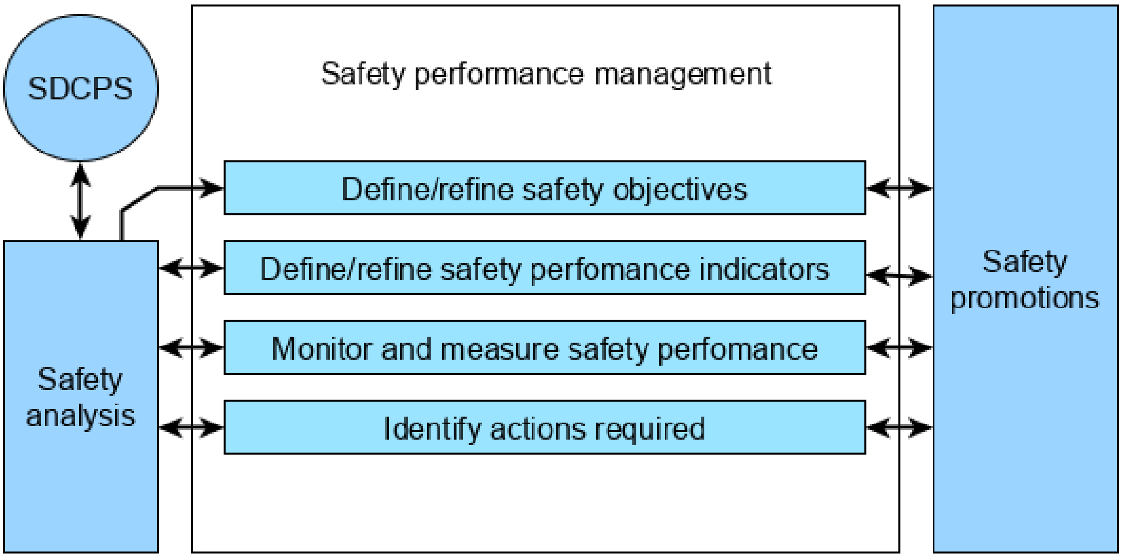

Figure 1 "Safety Performance Management Process" [3]

Talking about SDCPS, there are two types of reporting systems[2]: mandatory and voluntary. A mandatory safety reporting system should capture information about occurrences, including relevant information like what has happened, where, and when. Additionally, there has to be information about contributing factors from the accident. A voluntary system is established to collect safety data and information, which was not captured by the mandatory system. [3]

ICAO Doc. 9859 recommends using taxonomies and supporting definitions to categorize safety data. Using common taxonomies and definitions gives an opportunity to share and exchange safety data and information. ICAO offers three aviation taxonomies: (1) ADREP, which is an occurrence category taxonomy related to ICAO's accident and incident reporting system; (2) CAST/ICAO Common Taxonomy Team (CICTT), which is developing common taxonomies and definitions for aircraft accidents and incidents and (3) Safety Performance Indicator Task Force (SPI-TF), which develops globally harmonized metrics for service providers' SPIs[3] as part of their SMS. [3]

[2] Reporting for states and their service providers in EU falls under Regulation (EU) No 376/2014

[3] Safety Performance Indicators

Today safety data and safety information is more complex than some years ago. In the case of a thorough investigation, the safety manager gets detailed information about an occurrence. And, sometimes, common taxonomy cannot categorise all data and information. Especially when talking about MROs, they were not required to have SDCPS until late 2019[4], and existing taxonomy systems did not account for MROs very well.

1.1.2 MRO EU legislation framework

The Czech Republic's aviation segment has to implement not only ICAO requirements, but also requirements of the European Commission (EC). In 2002 EC created a special community body with responsibility for civil aviation safety. EASA - European Union Aviation Safety Agency is the main player in f aviation safety activities in the European Union. [11]

Regulation (EU) 2018/1139 describes what are EASA's duties. EASA mainly carries out certification, regulation and standardization and has to perform investigation and monitoring of aviation safety. Additionally, EASA has to collect and analyse safety data, drafts, and advises on safety legislation. The Agency has to coordinate with similar organisations in Europe and worldwide. [12]

MROs, which want to provide their services in the EU, have to be approved by EASA. The main regulation which MROs have to follow in the EU is a Commission Regulation (EU) No 1321/2014. This regulation applies to the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks. Until 24. March 2020, there were four main parts in regulation 1321/2014. After that date Commission Regulation (EU) No 1321/2014 was changed by the Commission Regulation (EU) No 2019/1383. That regulation changed the amount of parts in regulation No 1321/2014. There are 8 parts as of today, which are shown in table 2.

According to the EASA guide for transition to Part-CAO and Part-CAMO, Part-CAMO provides requirements for CAMO organisations. The new Part-CAMO [5]is compared with

---

[4] Annexe 19 2nd version came into force 7. of November 2019

[5] After 24 September 2021, there should be no more Part-M Subpart F and Part-M Subpart G organisations [17]

the Part-M Subpart G organisation, but the main difference is the introduction of SMS requirements. [17]

Table 2 "List of Parts in Regulation 1321/2014 for today" [17]

Annex	Description
Annex I, Part-M	Continuing airworthiness standards – other-than-'light aircraft' and aircraft used by licenced air carrier (Reg. (EC) No 1008/2008)
Annex II, Part-145	Maintenance organisation approvals
Annex II, Part-66	Maintenance licensing
Annex IV, Part-147	Maintenance training organisation
Annex Va, Part-T	Aircraft registered in a third country
Annex Vb, Part-ML	Continuing airworthiness requirements for other than complex motor-powered aircraft not listed in the air operator certificate of air carrier licensed
Annex Vc, Part-CAMO	Continuing airworthiness management organisation (all types of aircraft types and operation)
Annex Vd, Part-CAO	Combined (continuing airworthiness management and/or maintenance) organisation – non-complex aircraft and non-licenced air carrier

Part-M and Part-145 are the most important for providing aircraft maintenance. The organisation, which is certificated by Part-145, is called Approved Maintenance Organisation. AMO is qualified for the issue or continuation of approval for the maintenance of aircraft and components. Part 145 defines a scope of maintenance tasks, requirements for the working environment including aircraft hangars, component workshops and office accommodation. Also, there are requirements for personnel, equipment, tools, material. [14]

Last but not least, the AMO organisation shall have a Maintenance organisation exposition (MOE). MOE contains all information about the current organisation, including maintenance procedures. MOE shows how the maintenance organisation intends to comply with Part-145. Mainly, MOE contains responsibilities and duties of persons and procedures of different processes. [14]

Organisation, which is certificated by Part-M is called CAMO. Continuing airworthiness management organisation is responsible for aircraft airworthiness documentation. CAMO has to provide AMO with all necessary procedures and documents for maintenance, which is performing in AMO's hangar with AMO's mechanics. [14]

CAMO is qualified for the issue or continuation of a certificate for the management of continuing airworthiness of an aircraft and of components for installation. An organisation approved in accordance with Part-M mainly has to manage the continuing airworthiness of aircraft. [14]

There is a main difference between CAMO and AMO. CAMO is responsible for the management of continuing airworthiness of aircraft. This organisation working mainly with documentation revises and makes maintenance programs and monitors terms for revisions and checks. AMO, in line with the requirements from CAMO, is providing maintenance activities.

1.2 Procedures

Maintenance of each aircraft has to be organized according to AMP - Aircraft Maintenance Program. AMP is created by CAMO organisation[6]. Maintenance program must establish compliance with instructions for continuing airworthiness, additional or alternative instructions, approved by Type Certificate Holder (THC). Additionally, AMP has to be established according to instructions issued by the competent authority. [14]

AMP shall include details like a frequency of maintenance procedures, specific tasks and the specificity of operations. AMP has to contain a reliability program too. [14]

Maintenance programme contains a list of tasks, with intervals in which those tasks have to be executed. Intervals are based on aircraft's flight hours, flight cycles or calendar time. [18]

According to EASA and FAA, the maintenance program has to be based on Maintenance Review Board Report (MRBR) and Maintenance Planning Document (MPD). Original Equipment Manufacturer/Type Certificate Holder (THC), Maintenance

[6] According to changes from 24.03.2020

Review Board/Industry Steering Committee members are involved with the evolution and optimisation of MRBR tasks. MRBR contains minimal initial requirements for maintenance planning - tasks and maintenance intervals. MRBR is being developed by MSG-3 (Maintenance Steering Group) logic. The basic goal of MSG-3 is to identify the reliability of a system, find maintenance tasks, which are unnecessary for maintenance or duplicity cover the same maintenance operation and mitigate that. [18] [32]

An MPD contains additional tasks that are required to maintain the specific type of aircraft. MPD is provided by the aircraft manufacturer. This document provides the information, which is needed to define the AMP. MPD is based on MRBR, ALS Part 2: Damage Tolerant Airworthiness Limitation Items (DT-ALI), ALS Part 3: Certification Maintenance Requirements (CMR), ALS Part 4: System Equipment Maintenance Requirements (SEMR), ALS Part 5: Fuel Airworthiness Limitations (FAL), ETOPS Configuration, Maintenance and Procedures (CMP) Document.

Also, the Service Bulletin (SB) and Airworthiness Directive (AD) have an impact on MPD. When one of them is issued, MPD is amended by them. SB is a document used by TCH to provide modifications in an aircraft, engines or to the components. AD is a regulation issued to correct an unsafe condition in a product, like an aircraft, engine, propeller or components. One of the main differences between AD and SB is that AD always notifies aircraft operators and owners about potentially unsafe conditions that need special repair or inspection. SB informs about product improvement. Sometimes SB contains improvements that can resolve some safety - related problems too. [18]

To complete Maintenance Program, CAMO organisations have to use additional documentation and manuals. For instance, Aircraft Maintenance Manual, Component Maintenance Manual, Wiring Manual, Troubleshooting Manual, Structural Repair Manual, Aircraft Schematic Manual, etc. [19]

Also, for improvement of Maintenance Program CAMO can use Maintenance Planning Data Document, Master Minimum Equipment List, Service Bulletin, Service Inform Letter, Corrosion Prevention Manual, additional documents for specific procedures, Instruction Service, In Service Activity Report, Structural Item Advisory, etc. [19]

During maintenance revision, mechanics use particular maintenance documentation prepared for the check. Maintenance Planning department prepares a Workpackage, which represents a list of works for this revision maintenance tasks that have to be performed during a specified maintenance period. Workpackage includes information about the materials, labour, tools and skills required for the work. [19]

There is one additional document, which can be a part of Workpackage. It is named Work Order. It includes detailed information about necessary actions, which have to be carried out during the Check. Every Work Order has to have its own reference number. Then there is information about a part number or a serial number of a maintained component, aircraft number, manhours, customer information, ATA chapter information, etc. Important part of a Work Order is description of a complaint or planned work, and description of actions or work, which have to be performed. [19]

Some action or work from Work Order is referenced to the current Task Card. Sometimes, Task Card is named Job Card or Work Card. Task card is a instruction of a maintenance task. This description is prepared from the original maintenance documentation. Task Card contains information about labour, materials, service items, tools which are required to complete the work. Task Card has to contain all information, which is required to ensure the accomplishment of the complete maintenance task. [19]

2. Systemic view on aviation safety

According to ICAO Safety Management Manual (Doc. 9859), the progress in aviation safety is possible to describe by four approaches. First one was Technical, safety deficiencies were related to technical factors and technological failures. The main goal was to improve technologies. Second one was Human factors. Safety experts tried to resolve human behaviour, "man/machine interface". The focus was on the individual's errors. The third one, from the mid-1990s, was Organizational. Safety began to be resolved from a systemic perspective. It introduced new approach to organizational culture and policies to ensure safety. Safety data collection and analysis started to monitor safety risks and detect safety trends. [3]

The fourth one is a Total system. It is today's view on aviation safety. This approach is not only about Safety Management System and State Safety Program. It is about the complexity of the aviation. The total system approach pays attention to interfaces between aviation stakeholders that contribute to accidents and incidents. [3]

As mentioned in the previous chapter, Safety performance is a part of Safety Management System. A number of safety models and analyses have been created to assess factors related to safety performance measurement. And for every approach, there are specific types of safety models and methods.

The development was also captured by Eurocontrol in one of its white papers on Resilience Engineering for ATM (2009), within their effort to map Accident Analysis and Risk Assessment Methods. This is shown in figure 2.

As can be seen, most of models and methods are of the former three approaches: Technical, Human Factors and Organisational. Technical models resolve potential problems only in technologies. They are not appropriate for resolving other types of problems, for example human based. Human Factors models talk only about human individuality and its interaction with a system. Organisational approach addresses only management and organisation of a company. That is why the Systemic approach is the most interesting for future safety. It is based on the idea that it is important to resolve technical, human and organisational approaches together in a whole, with broader perspective.

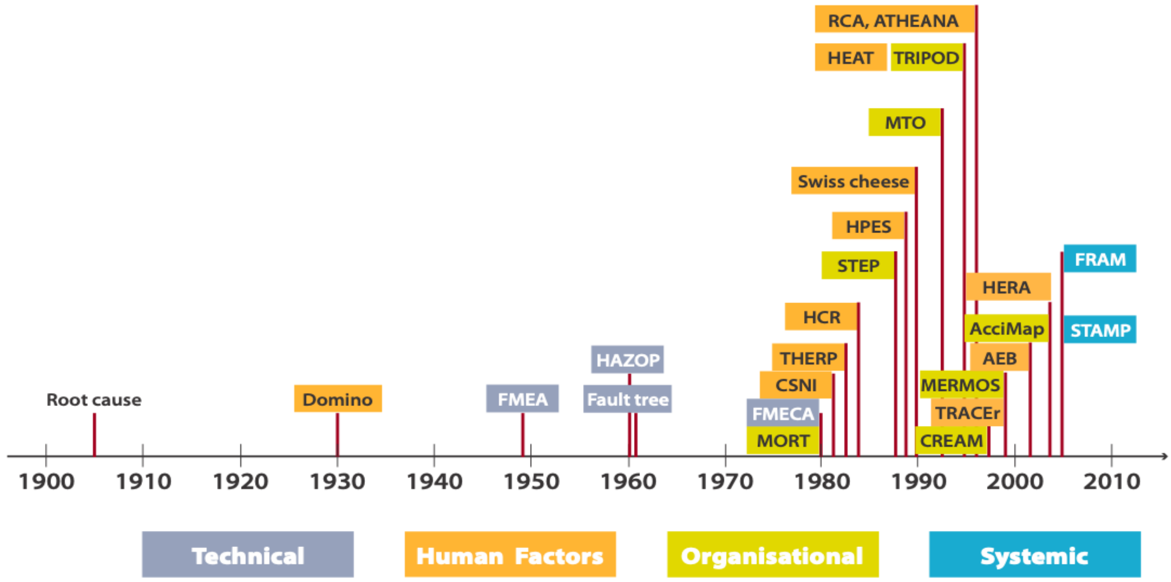

Figure 2 "The development of different Accident Analysis and Risk Assessment Methods" [20]

ICAO describes how to categorise factors, which contribute to accidents or incidents through these four approaches.

2.1 Safety-I vs Safety-II approach to aviation safety

Professor Erik Hollnagel from University of Southern Denmark was an inventor of the idea to split the term Safety to Safety-I and Safety-II. It was caused by necessity to change the whole approach to safety. [21]

According to Prof. Hollnagel, usually when people talk about safety, they refer to the opposite of the meaning of the term safety. They talk about absence of safety. Traditional view of safety is based on absence of incidents and accidents, on freedom from unacceptable risks, on focusing on unsafe system operations. And Prof. Hollnagel calls that view Safety-I. [21]

Safety-I is mainly based on the idea, that it is important to focus on "What goes wrong". For resolving safety deficiencies, Safety-I uses reactive approach. After an occurrence, it tries to identify incident or accident causes, set up rules, how to avoid such errors in the future and work with the question how to reduce losses. Safety-I contains 3 approaches to safety - Technical, Human factors and Organisational. [21]

Talking about Safety-II, it focuses on "Why things go right". Safety-II does not count bad things but rather emphasizes the idea "As much as possible goes right". This approach to safety is called proactive. Safety management is learning from successes, trying to understand what goes right and why. It tries to enforce successful behaviour and creating new processes on successful behaviour. [21]

Total systems approach is close to Safety-II. There are three known systemic models, to various extent compatible with Safety-II: System-Theoretic Accident Model and Processes (STAMP), Functional Resonance Analysis Method (FRAM) a Resilience Analysis Grid (RAG). These systemic safety models are created to resolve safety problems in complex sociotechnical systems. Also, systemic models work with the idea that there is emergence in operations of current, complex system. It means, that in such system, the final event is not only based on a loss factor chain. When safety inspector derives knowledge about an incident just from a factor chain, there is a possibility of losing important information from a wider perspective. Because of it, domain experts are asked for possible incident's contributing factors, which they identify only thanks to their experience. [21]

Systemic safety models give an opportunity to identify contributing factors, which are not a part of the main loss factor chain, identified by conventional approach currently used in the aviation. [21]

2.2 Selection of systemic safety model

MRO is a complex sociotechnical system. It means that for future MRO's SDCPS, it will be appropriate to use a systemic safety model. There are three models: STAMP, FRAM and RAG, which could be used for service provider's SDCPS.

2.2.1 STAMP

STAMP is a systemic model, which is partly compatible with Safety-II. STAMP is based on an idea that undesirable states can be detected and controlled in time. STAMP says that sociotechnical systems are complex and it is not really possible to aggregate every information about it. However, there is a possibility to control processes during all system flow activities. [23]

STAMP offers hierarchical control structure, which contains human and automatic controllers, sensors and actuators that can control given process. That structure helps to identify changes in a process in time and resolve them. If an organisation sets up control structure according to STAMP, there will always be a possibility to react to expected and unexpected events in time, without the necessity of losses. [23]

2.2.2 FRAM

FRAM is a systemic model, which mainly describes links and dependence between a system's functions. This model is based on an idea to analyse resonances from the variability of everyday processes within a system. FRAM tries to describe through function's communication the unpredictability of operational processes that can lead to an accident. According to FRAM, for identification of resonances in a system, is required to identify and describe system functions, characterize their variability and define how a system will react to the variabilities. [26]

2.2.3 RAG

RAG is a method that extends the ideas behind FRAM. FRAM describes how unwanted events are occurring. RAG attempts to describe how to minimise probability of unwanted events by building the so-called resilience into the sociotechnical systems. RAG tries to estimate presence of a resilience of sociotechnical system. [25]

2.2.4 Summary

MRO organisation is a sociotechnical system, so it is reasonable to build MRO's SDCPS with a Safety-II compatible model. Given the current situation in the aviation (way of thinking, existing infrastructure and process management), STAMP is the most suitable for that purpose today. Using this model will be the first step to connect current Safety-I approach to safety management with future systemic Safety-II approach.

By using STAMP in SDCPS, MROs will investigate all current processes, describe them and get knowledge about the current safety control structure inside the company. There will be an information about who controls the process, how the controller gets information about a process and which unsafe control actions could happen.

After that, in the future, MRO's SDCPS may be extended by FRAM and RAG, which both require a good understanding of system processes and their description, that STAMP can help to achieve.

For a better understanding of STAMP theory, the next chapter contains detailed description of STAMP that is needed to establish an MRO's SDCPS.

2.3 STAMP systemic model of safety

System-Theoretic Accident Model and Process (STAMP) is a safety model based on system theory. According to Prof. Nancy Leveson, the author of STAMP who is a professor of Aeronautics and Astronautics and also Professor of Engineering Systems at Massachusetts Institute of Technology (MIT), there is a necessity to address safety like an emergent system property. [23]

System theory was invented to cope with complexity in systems. The main goal was to go from analysing part of a system to analysing it as a whole, which contains different parts. According to prof. Leveson, to get an information about the whole system, it is needed to learn from the behaviour, which is specific for system-level. That behaviour may be different from component level. [23]

According to STAMP, the sociotechnical system consists of control structures, and problems inside that structures have an impact on system safety. Control structure of a system consists of network of control loops. In figure 3 there are a standard control loop as applied by prof. Leveson. [23]

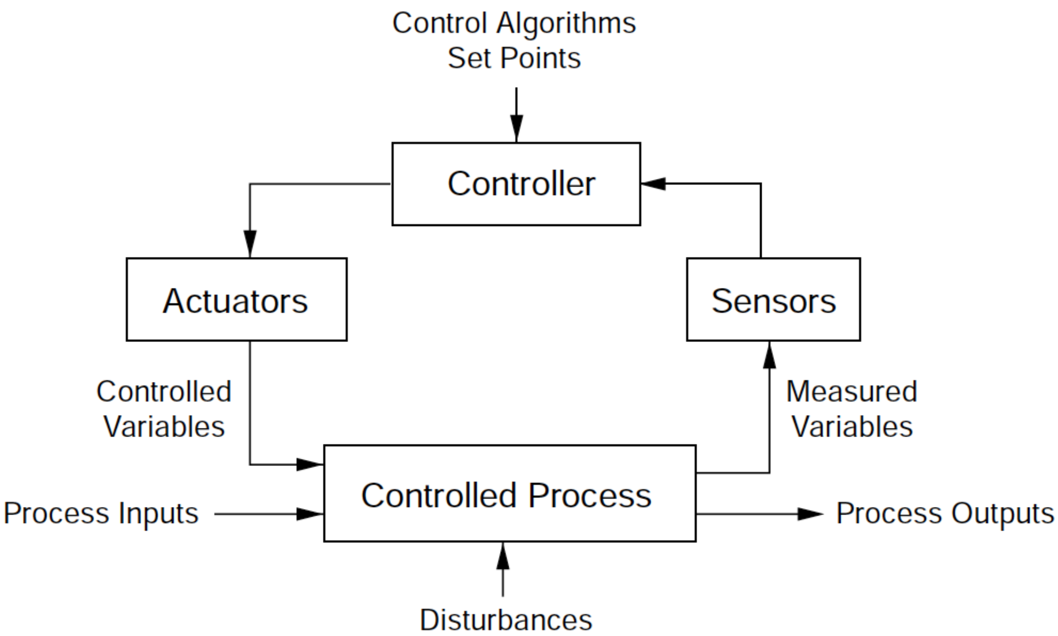

Figure 3 “A standard control loop” [23]

That control loop can be social, technical or a sociotechnical. The controller, which obtains information about the process state, can be human or a computer. Controlled process can be a technical process or another human in a system. The controller gets a feedback information (Measured Variables) by a sensor from a controlled process. According to feedback, Controller decides which step he has to provide and by an actuator he sends instructions to a Controlled process (to manipulate Controlled Variables). [23]

In STAMP, there is a possibility to describe every incident or accident by a network of control loops. After such description, safety expert has to find the causes why the system has failed as a whole. STAMP says that there no possibility for a system to fail without a problem at the level of the applicable control loops. [23]

Every Controller has two main parts: Process model and Control Algorithm. Thanks to them, controller determines which step in a process has to be taken with current process state. Process model contains information about the current state of a process. Process model analysis helps to understand, why accident occurs and why inadequate control was provided. Also, process model analysis helps to design safer systems. [23]

Control Algorithm is a set of rules for a controller to control a process. When talking about computer controller, an algorithm is a common way to describe process rules and normally is described by a computer logic. However, human controller is more complex. Human controller gets knowledge about how to control a process during a training or with gaining experience, but human controller also can occasionally change control algorithm in a process, as humans tent to experiment and refine their understanding of what they are doing. These changes sometimes help to prevent an incident or accident, but sometimes they lead to an occurrence. [23]

According to STAMP, there is a possibility to find why human controller failed, when it happened and understand why a human controller exhibited particular behaviour.

Important idea, which is described by STAMP theory is that some processes are controlled by more than one controller. That variation of a control loop is shown in figure 4.

There is a combination of an automated and human controller, both controlling one process. These controllers have the same model of the controlled process. However, human controller additionally has a model of an automated controller. This arrangement needs to be carefully analysed for conflicting or missing control, in addition to analysing normal issues of a control loop.

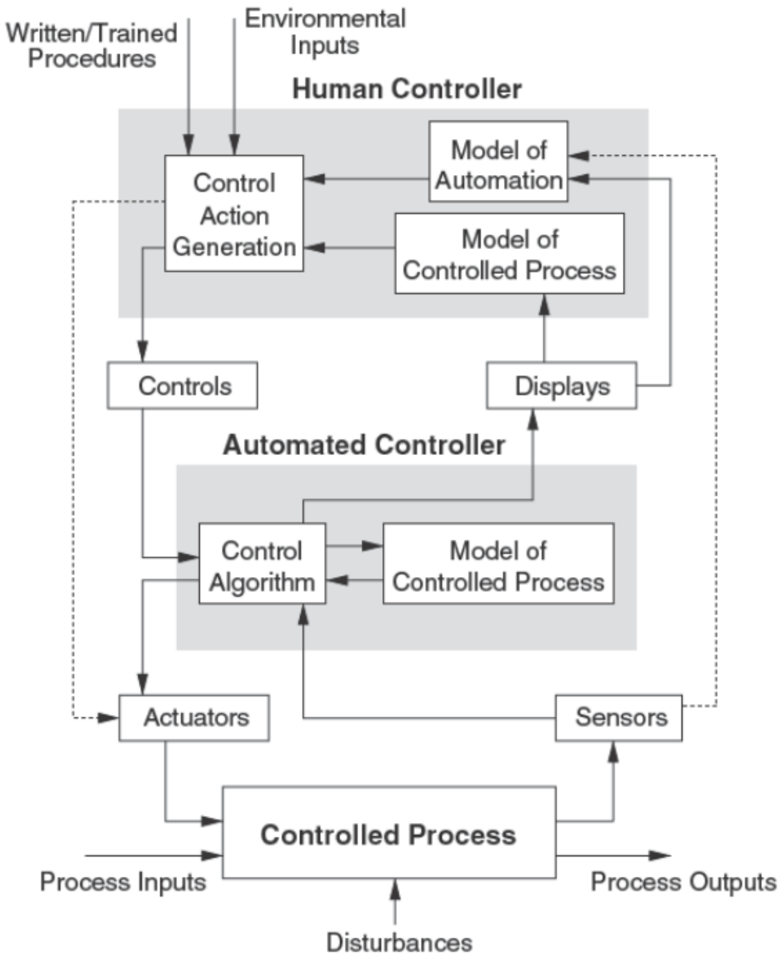

Figure 4 "A human controller controlling an automated controller controlling a physical process" [23]

Furthermore, for understanding how control structure of a sociotechnical system looks like, there is figure 5. It is called hierarchical control structure. In every sociotechnical system/organisation there are a lot of controlled processes and controllers. Each component of a system has an impact on other components. This is why, according to a STAMP, it is important to understand all the control structure in a system for problem identification. [23]

In STAMP, hierarchical control structure of a system can help go through the system control loops and find more contributing factors. Or, during designing a safe system, we can identify more safety constraints that can better assure safety in the system operations.

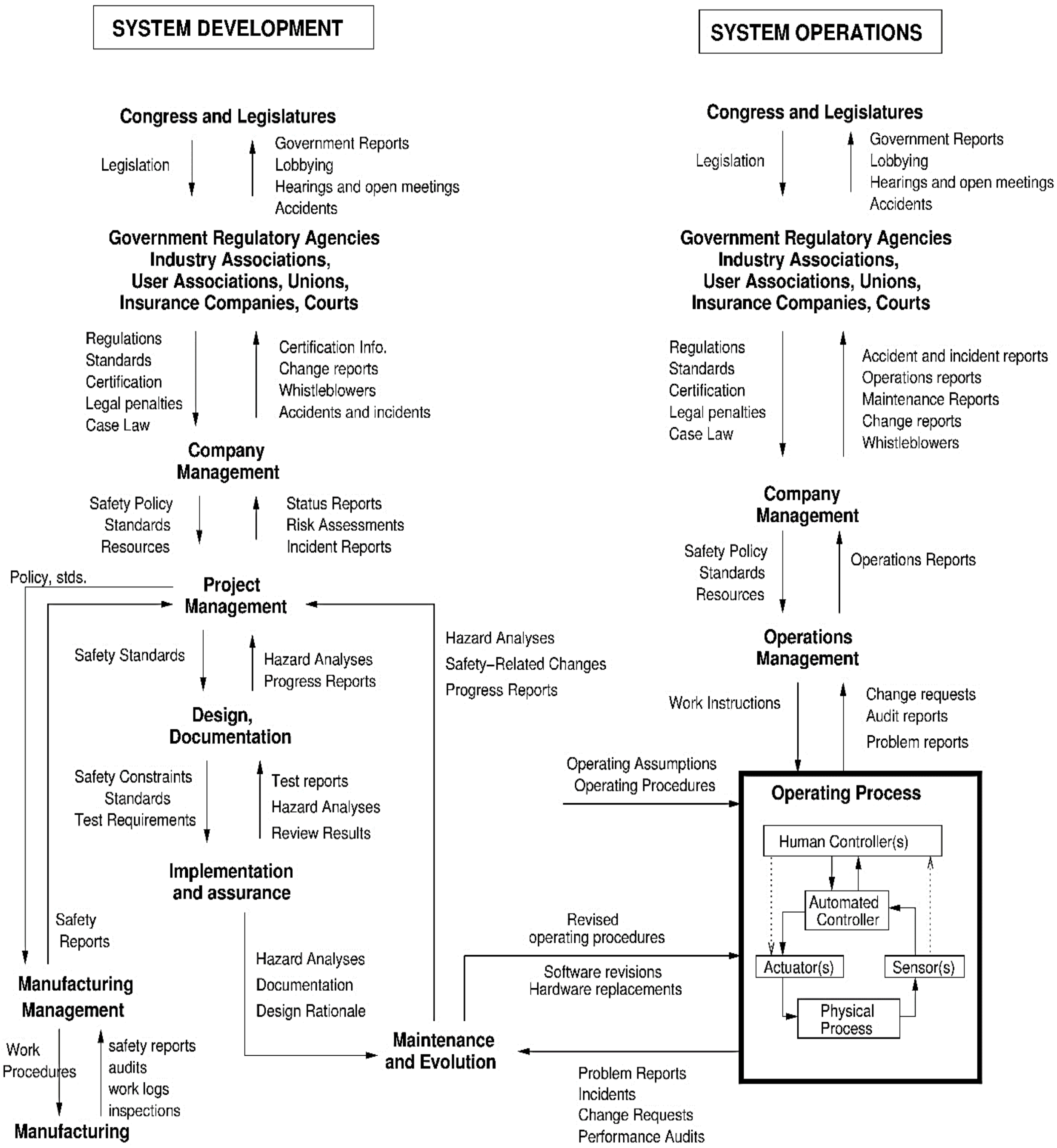

Figure 5 "An example of a safety control structure" [23]

Prof. Leveson offers for the purpose of identification systemic problems not only implementing safety control structures and their descriptions, but use of some analyses too. There are two STAMP-based methodologies: System-Theoretic Process Analysis (STPA) and Causal Analysis based on STAMP (CAST).

2.3.1 STPA methodology

STPA was invented to support hazard analysis. According to STPA, accidents are caused by unsafe interactions between system components, not only because of their failure. [22]

STPA can be used during inventing safety requirements and constraints. That is why STPA is a proactive analysis, which can help design safety into system's architecture. [22]

STPA can help to find potential factors, which can lead to an incident or accident during system operations. At the same time, it provides options to control that factor or eliminate it. [22]

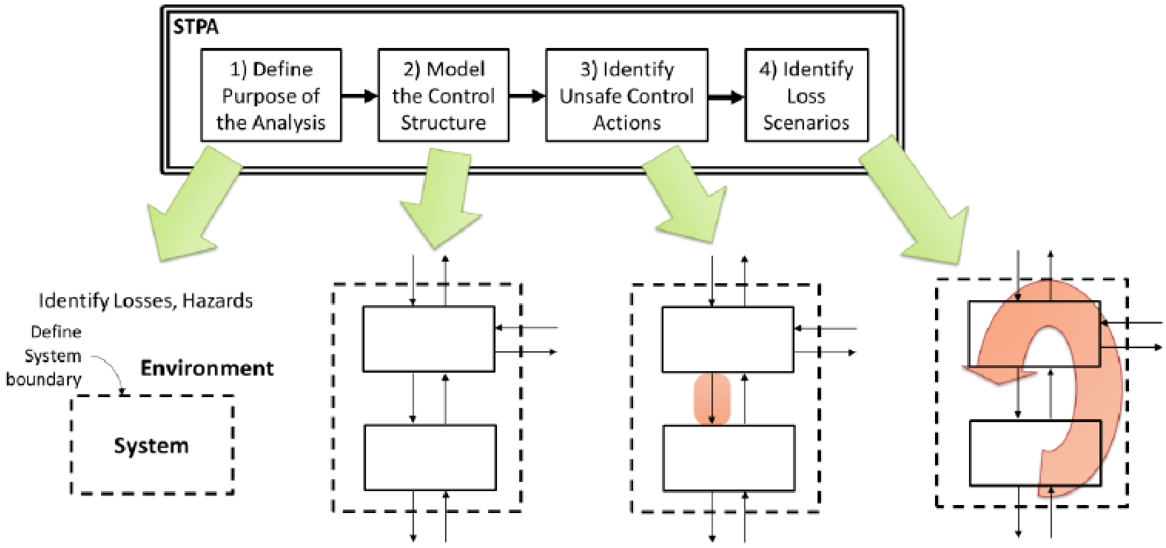

Figure 6 "STPA four basic steps" [22]

There are four main STPA steps in figure 6.

During the first step, it is important to define for what goal the analysis will be used and what kinds of losses the analysis will control. This step can be divided into four sub-steps: identify losses, identify system-level hazards, identify system limitations, and classify hazards according to whether they are relevant for analysis or whether they can be neglected and better used in another analysis. [22]

The second step is to model the control structure of the investigated system. STPA uses a standard control loop, which is shown in figure 3.

The third and fourth steps are the core steps of STPA. The third one is based on identification of the unsafe control actions. An unsafe control action is a control action that in a certain context can cause a hazard. This can happen when [22]:

1. *A control action required for safety is not provided or not followed*
2. *An unsafe control action is provided*
3. *A potentially safe control action is provided too early or too late, that is at the wrong time or in the wrong sequence*
4. *A control action required for safety is stopped too soon or applied too long*

Fourth step deals with identification of a possible development of losses. It allows proposing scenarios of possible losses and find out how dangerous states can occur. Causal factors that lead to hazards can be identified there. [22]

There are several tools to investigate a causal factor:

1. *Examination of a part of the control loop to see if these parts can cause unsafe control action.*
2. *If there are safety constraints in the system, then it is necessary to examine them. If they do not exist or they are old, it is necessary to create them or improve.*
3. *Identification of possible potential conflicts between controllers (Human and automated controller).*
4. *Observation of degradation of the proposed control over time. For this, it is necessary to use change management, audit of unplanned changes and also analysis of possible accidents.*

2.3.2 CAST methodology

CAST is a STAMP-based analysis of the cause of accidents. This method makes it possible to investigate into the occurrence of an accident and to identify the causal factors that caused the undesirable conditions.

The following points are defined by prof. Leveson with respect to CAST [22]:

1. *An accident is a complex event, it has no or several basic root causes. The same goes for STAMP, which claims that an accident will occur only due to a complex of several events.*
2. *Blaming is the main enemy of safety. Knowledge of who or what caused the accident is not enough to ensure that the danger is not repeated.*

It is always necessary to find out the reason why the dangerous condition occurred and then find a solution to prevent it.

3. *Human error is a sign that the system needs to be rebuilt. You cannot change human behaviour without changing the system itself that causes it.*
4. *Retrospective assessment prevents the study of the accident. If the safety manager approaches accidents from the point of view "if he did not do so, it would not happen", he will not find the basis of the event. It is necessary to think about why this situation occurred and why the controller did not follow the safety restrictions, or the subsequent restrictions were not sufficient.*

According to CAST Handbook, prof. Leveson defines five steps for a CAST investigation, they are shown in figure 7.

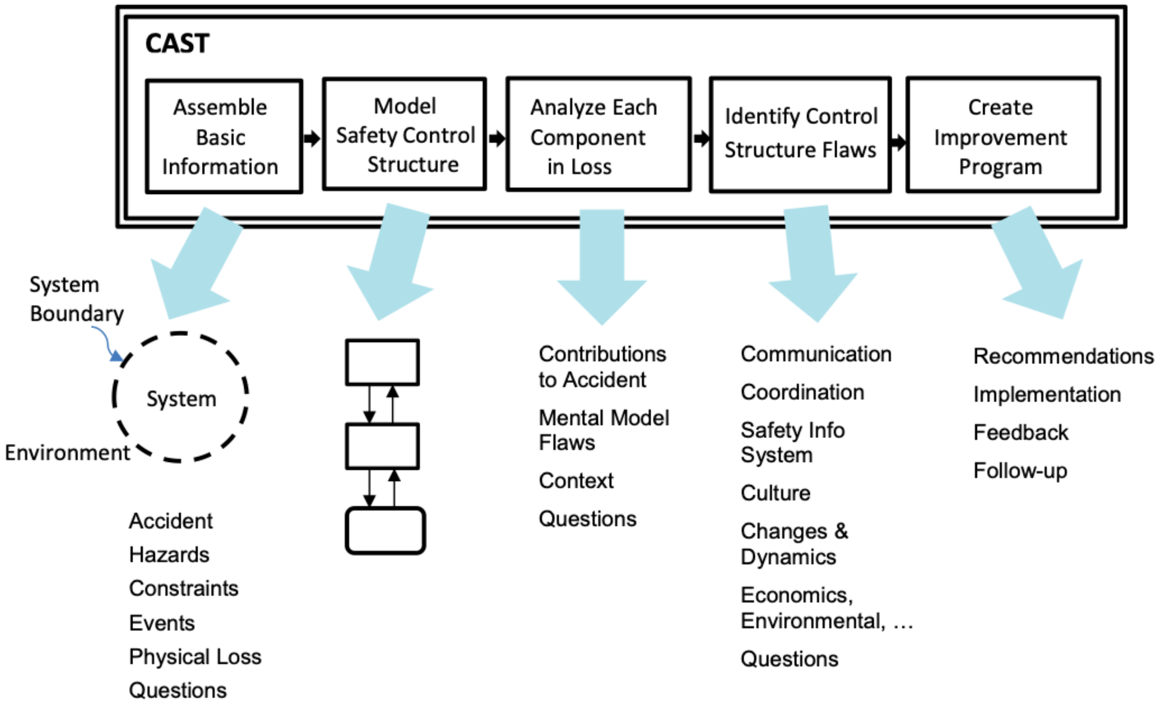

Figure 7 "CAST five basic components" [28]

First one is a Collection of the basic information to perform the analysis. This step is performed by five sub-steps [28]:

1. *Definition of the system involved and the boundary of the analysis,*
2. *Description of the loss and hazardous state that led to incident/accident*
3. *Identification of the system-level safety constraints required to prevent the hazard.*

4. *Description of what happened without conclusions or blame. Generate questions that need to be answered to explain why the events occurred.*
5. *Analysis of the physical loss in terms of the physical equipment and controls, the requirements on the physical design to prevent the hazard involved, the physical controls (emergency and safety equipment) included in the design to prevent this type of accident, failures and unsafe interactions leading to the hazard, missing or inadequate physical controls that might have prevented the accident, and any contextual factors that influenced the events.*

The second step is to model the existing safety control structure for identified type of hazard.

Third one is to examine the components of the control structure to determine why they were not effective in preventing the loss.

The fourth is to identify flaws in the control structure as a whole (general systemic factors) that contributed to the loss.

And the last one is to create recommendations for changes to the control structure to prevent a similar loss in the future. If appropriate, design a continuous improvement program for this hazard as part of your overall risk management program.

2.4 Summary

STAMP systemic model with STPA and CAST can support MRO's SDCPS to achieve Total system safety approach. Using STAMP, MROs can make sure that they have adequate hierarchical control structure in place and obtain detailed information about the way their processes are controlled. After that, using STPA, safety expert studies potential unsafe control actions and evaluates if problems in that control structure can lead to an incident or accident. When investigation will be needed, safety expert can use CAST to identify what and why happened, get more details about the situation occurred and generate recommendations, which will improve system's safety.

3. Current view of SMS tools with SDCPS block

To better understand the current situation with SDCPS systems, there are three SMS tools introduced in this chapter. Two of them (INBAS and The European Aviation Reporting Portal) were invented in Europe. SMS Pro was designed in the U.S.

3.1 INBAS reporting tool

It is a reporting tool software, which is suitable for reporting safety occurrences. INBAS can be used in different aviation organizations. Factor classification in INBAS uses ECCAIRS taxonomy. There are some extra classification glossaries, which were adopted in INBAS reporting tool. [33]

INBAS reporting tool functions are [33]:

- creation of a safety report
- classification with occurrence classes taxonomy
- analysis of the sequence of events, factors and their type classification
- evaluation of classified factors and events in a statistics module

CSAT was one of the partner in INBAS project, that released the reporting tool and the tool is currently available as SDCPS in the organization. I had a possibility to work with it during an investigation reporting.

Next are shown some statistics examples from the INBAS demo version in figure 8 and 9. That statistics are based on factors (soft data) classification. INBAS can show in relations between the occurrence factors as they happened and were processed into its database (see figure 9).

Event Type	Annual Count	Annual Trend
104 - GTOW: Glider towing related events	2	
106 - NAV: Navigation error	1	
103 - LOLI: Loss of lifting conditions en-route	1	

Figure 8 "Top of the Occurrence Categories" [33]

factor type	relation type	event type	count
Call-sign confusion	causes	Loss of separation	1
Apron/ramp congestion	contributes to	Inadequate separation	1
FOD Presence on aerodrome surface area	causes	Collision	1
Confusion	causes	Incorrect presence	1
Collision	causes	Foreign object detection	1
Smoke encounter	causes	Fire encounter	1
Foreign object detection	causes	Damage manifestation	1
Aircraft ground collision	causes	Damage manifestation	1

Figure 9 "Event – Factor chain" [33]

3.2 EASA's Aviation Safety Reporting tool

Aviation Safety Reporting tool was invented by EASA according to Regulation (EU) No 376/2014 on the reporting, analysis and follow-up of occurrences in civil aviation and Commission implementing Regulation (EU) 2015/1018 laying down a list classifying occurrences in civil aviation to be mandatorily reported. [34]

This reporting tool is called International Occurrence Reporting System (IORS). This tool is mainly used by state authority organisations. The safety data collected by IORS are stored in a database (in the European Central Repository (ECR)). The database is separate from the tool to collect and process data. [38]

The Aviation Safety Reporting is a common name of the website, that the user sees. In this website everybody can report an occurrence. There are forms for both mandatory and voluntary reports, and one can report as an organisation or individual. [34]

The reporting tool uses ECCAIRS taxonomy. Thanks to it, Aviation Safety Reporting tool classifies reports. However, soft data that the tool collects are again only in a narrative text form. [34]

Link[7] to that tool is well known and available to the aviation community through EASA website, CAA or in an Air Accident Investigation Institute website.

[7] https://www.aviationreporting.eu/AviationReporting

3.3 SMS Pro – SMS management tool

This software was designed for ICAO compliant SMS programs satisfying FAA, IS-BAO, EASA or Transport Canada requirements. It is payware commercial safety tool. [35]

SMS Pro offers different modules which follow aviation SMS requirements. Also, that tool is more based on hard data. For example, a safety performance module, in which I am interested in, provides the following performance indicators [35]:

- Total Number Issues Reported
- Average Days to Resolve Issue
- Number Months Reporting
- Average Number Issues Reported Each Month
- Total Cost of all Issues
- Average Cost per Issue
- Minimum Issue Cost
- Maximum Issue Cost

It means, that although SMS Pro can collect soft safety data using narrative text, they do not display such data in statistical modules. SMS Pro uses ADREP taxonomy to classify data in a Risk Management module. It gives an opportunity to a user to exchange safety data to with other databases, for example with a State safety database. [35]

4. Proposal and creation of selected parts of MRO's process documentation

Before using STAMP-based safety analysis, it is necessary to create a system description. Nowadays, basically all MRO's processes are written in text form and they contain the necessary system description. However, there is a way, how to transform procedures from text form to computer flow, that would be better usable with STAMP. This way is very common in big companies today, using Lean management to achieve this goal. Lean management experts normally use the BPMN language to describe company's processes.

4.1 Lean Management

There are some ways to reduce manufacturing costs. A company can produce the same product from cheaper materials and lose the quality of the product. Or, it can reduce processes that do not bring value to the end product. The second way is the main idea of Lean management. The Lean management was developed in Toyota in the late 1940s and is very popular now in all businesses from manufacturing to marketing. [4]

The goal of the Lean management is to improve the efficiency and quality of a system. Experts on Lean management work with the company's processes. They try to find a problem, map a company's workflow with all processes, activities and controllers of that activities. Sometimes there is additional information about costs or staff, which is used during activities. Then the experts look at continuous workflow and suggest what to do next. They think about how to change a process or, maybe, how to deal with labour in another way. [4]

A company can outsource Lean management services occasionally to resolve a current situation or the company can create its own Lean management department. Mostly, big corporations and manufacturers have such a department in their management structure. It is because of the necessity to develop and optimise large amount of processes every day. Economics is too unpredictable nowadays and it is important to be prepared to change processes in a short time.

4.2 BPMN

One possible way, how to collect and analyse processes in one application is to use BPMN software. Business Process Model and Notation is a modelling language, which allows transferring processes from paper-based documentation to an algorithmic flow. BPMN is a business process modelling language, which can be used in different areas of conceptual models. For example, to describe communication in an organisation, to research the impact of a process change, or to do a simulation of processes. [5]

The benefit of BPMN is that an expert can document, model, analyse, simulate and execute processes in one software. BPMN helps to build a bridge between human and computer and allows to work with a sociotechnical system. It is possible to build a process, which is controlled by a human or a computer and then research communication between them. [5]

BPMN language has four basic categories of elements: Flow Objects, Connecting Objects, Swimlanes and Artefacts. Some of them are explained in figures 10 to 13.

Figure 10 "Flow objects" [Author's figure]

In figure 10, there are base events on the left side. However, sometimes you have to define, which kind of start it was, or which decision-making gateway is better to explain a process in an appropriate way. That is why there is such start event, like a Message Start or a Complex Gateway (right side of figure 10). [6]

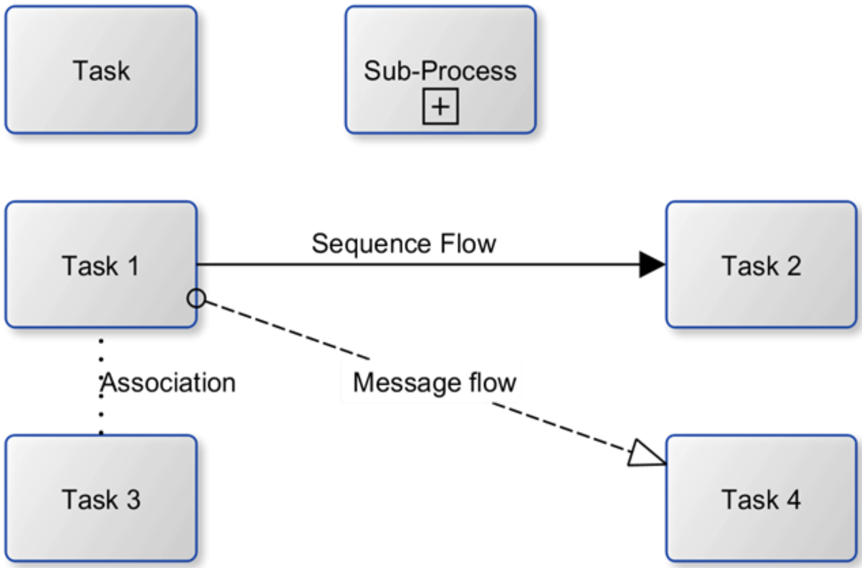

Figure 11 "Flow Objects –Tasks and Connecting Objects" [Author's figure]

In figure 11 in the upper part, there are the main Flow Objects – Task and Sub-Process. They enable the construction of activities in the process. There you can write the main information about the activity, for example a controller or other additional information, which will be described in the next chapters of this thesis. Of course, there are other (more detailed) types of tasks like a Send Task, Service Task, Manual Task and etc. [6]

Connection Object, which is shown in this picture, describes a type of flow between activities. Every flow except Association has "to" and "from", which is indicated by an arrow. [6]

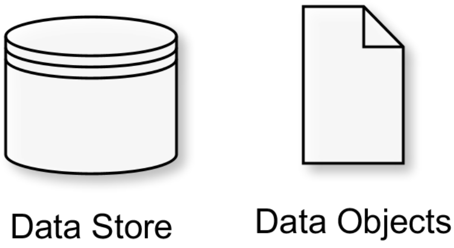

Figure 12 "Artefacts" [Author's figure]

Figure 12 shows Artefacts used to show that process has external resources with additional information. [5]

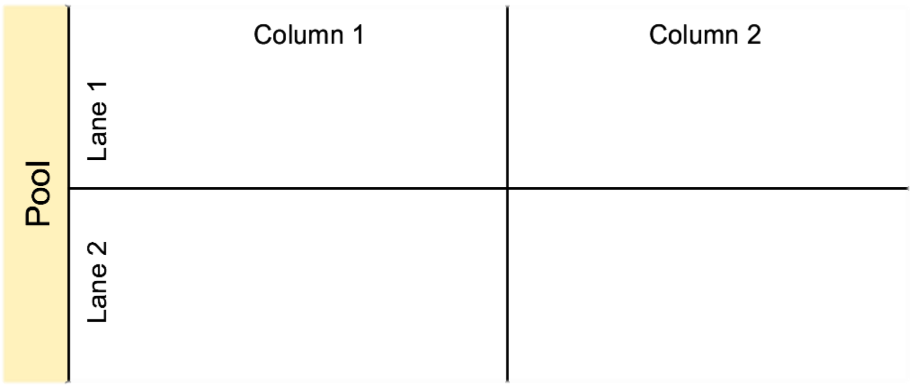

Figure 13 "Swimlanes" [Author's figure]

A pool, which is shown in figure 13, is the main part of a Swimlane. Pool shows which activities are done by the current participant. Lanes help to define which part of an organisation did current activities.

4.3 Proposal of Instructions for transferring MROs procedures to BPMN language

This part of the thesis was done in real conditions, in cooperation with Czech Airlines Technics (CSAT). The work was carried within my support activities to the research project No. TJ01000377 – Research of Intelligent Components for Safety Data Collection and Processing Systems, funded by the Technology Agency of the Czech Republic. Because of confidentiality restrictions, the procedures and figures in this chapter were anonymised. The work builds on a previous methodology, where similar issue was addressed in the domain of airports. [24]

In agreement with the CSAT, to help propose SDCPS for MRO organisations, two internal procedures were modelled in BPMN software. The first one was *Base Maintenance Administration* and the second one was *Repair procedures*. The *Base Maintenance Administration* consist of five main parts: *Calculation, Preparation, Meetings, Communication and responsibility* and *Administrative works after finishing of the check*. The *Repair procedures* consists of three main parts: *Evaluation of repair possibilities, AOG situation resolving* and *Repair*.

Next follows an anonymised example of a procedure with specifications, how it could be written in real conditions:

PROCEDURE

A general description of a procedure

1.1 Calculation

Activity 1 will be provided by Worker 1.

If there will be some additional requirements, Activity 2 will be provided by Worker 1.

Activity 3 will be provided by Worker 2.

In appropriate case Worker 3 will provide Activity 4.

Activity 5 and Activity 6 will be provided by Worker 1, if Activity 2 will be required.

1.2 Preparation

Worker 1 has to provide:

- *Activity 1*
- *Activity 2*
- *Activity 3*
- *Activity 4*

Worker 2 has to provide:

- *Activity 5*
- *Activity 6*

1.3 Meetings

Worker 1 has to be certificated by requirement A.

Worker 2 has to have tool 1.

Activity 1 has to be done.

1.4 Communication and responsibility

1.5 Administrative works after finishing of the check

1.5.1 Process 1

1.5.2 Process 2

As can be seen, the biggest problem for modelling processes is the variability of ways how processes are described in procedures. It is widespread not only in MROs, but in other aviation organisations too. According to that, for Lean managers is a challenge to find processes in the documentation, for safety inspectors it is a time - consuming work too. During the investigation process, inspectors need to understand a process in a short time. And due to variability and complexity of procedures, sometimes, it takes more time to identify processes in procedures than to find root causes of an incident.

During the analysis of the two anonymised procedures, three main process-making problems were found:

1. If procedures are written in a text form, the process flow is usually lost *(see point 1.1 Calculation)*. For example, from those procedures you can see, that after Activity 2 is required to provide Activity 5 and Activity 6. However, information about it you will find at the end of the procedure. This is not very convenient for the first procedure reading. There is a possibility of getting confused about the process flow.
2. Some processes lack their controller *(see point 1.3 Meeting)*. It can be caused by lapse or lack of time when compiling the procedure. Some are generally controlled by the whole department which means it is difficult to determine who is responsible for the actual performance of the process within that department. However, there is a possibility to ask the responsible department about who provides the current process.
3. Some procedures include a list of controller's activities *(see point 1.2 Preparation)*. In those situations, there is information about processes and controllers, but the flow of the activities is lost.

The above three points make visible imperfections in today's procedures. Not only a Lean manager has to deal with those problems when studying processes, but also a safety expert during occurrence investigation.

If a new MRO's SDCPS system would be based on STAMP, the organisations would have to establish their procedures in line with systemic approach, clearly defining who is responsible for which process. However, it may be a long way to achieve ideal procedure description, so it is necessary to think how to work with today's procedures, as they are.

To maintain compatibility with STAMP, models of procedures have to be aligned with safety control structure (control loops) and contain: name of a controller, controlled process (activity), sensors and actuators of a process. Also an activities flow (arrows) which connects separate activities.

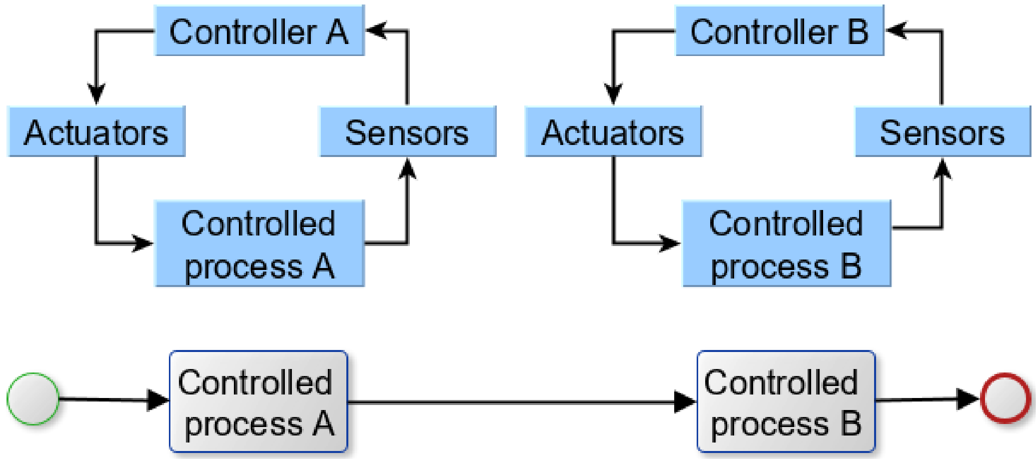

Figure 14 "Comparison of STAMP Control loops and BPMN process flow" [Author's figure]

In figure 14 there is a representation, which information every BPMN rectangle has to contain to be compatible with STAMP.

To model a procedure in a BPMN, it is first necessary to understand which level of abstraction is needed for the model. Safety expert has to choose, according to occurrence investigation, how much detailed process he needs. In some situation, the model can comprise only basic activities. Sometimes, it can be necessary to go down to detail in the process hierarchy. In that situation, activities from upper abstraction will be transformed into processes. Sub-processes inside new processes (activities from upper-level abstraction) will represent new activities.

Next follows an example how different levels of abstraction can be achieved in BPMN (for the purpose, there is a part from procedures above.):

1.5 Administrative works after finishing of the check

1.5.1 Process 1

Activity 1

1.5.2 Process 2

Activity 2

If safety expert needs just to know that this process contains *Process 1* and *Process 2*, he will use the model from figure 15[8]. In that case *Process 1* and *Process 2* will be present like independent activities.

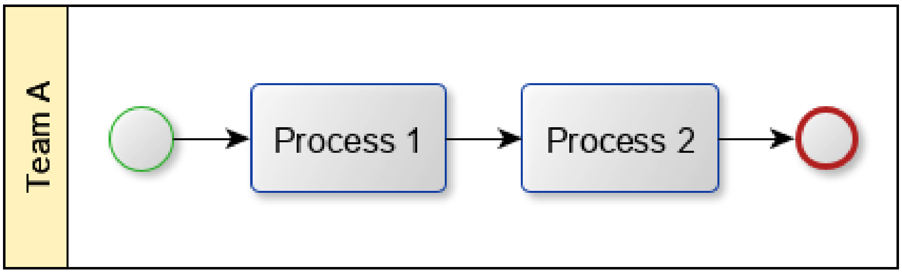

Figure 15 "Process of Administrative works after finishing the check with activities Process 1 and Process 2" [Author's figure]

However, if safety expert is interested, what could happened inside activities *Process 1* and *Process 2*, Lean manager will have to find additional information, how that activities are provided. In figure 16 there is an example, how such extension will look.

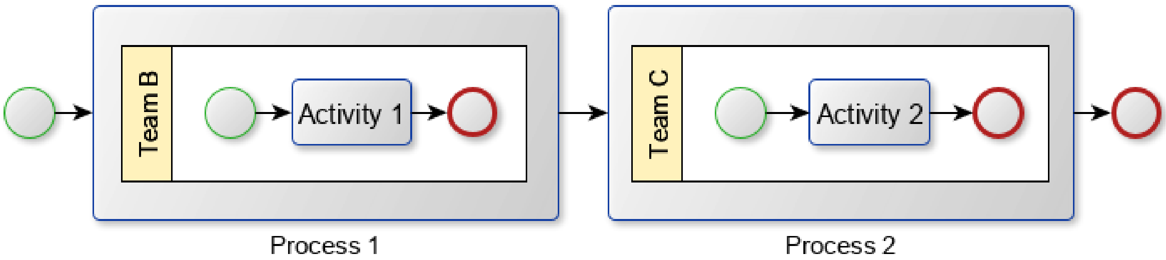

Figure 16 "Process of *Administrative works after finishing the check* with sub - processes *Process 1* and *Process 2*. Sub-processes contain activities *Activity 1* and *Activity 2*" [Author's figure]

Activities *Process 1* and *Process 2* will be described like a sub-processes (not activities now) and *Activity 1* and *Activity 2* like activities. In that case, Controllers will be assigned only to *Activity 1* and *Activity 2*, not to a *Process 1* and *Process 2*.

---

[8] Most of diagrams in this chapter were done in Bizagi Modeler (https://www.bizagi.com/en/platform/modeler).

This tool was the preferred solution at CSAT for the research purpose, but any other BPMN 2.0 compatible tool can be used for the purpose. This thesis does not promote usage of this particular software.

In figure 17 there is a BPMN model of a process *1.1 Calculation*. Blue rectangles show process activities, yellow triangles gateways. Objects are connected by arrows, which show process activity flow.

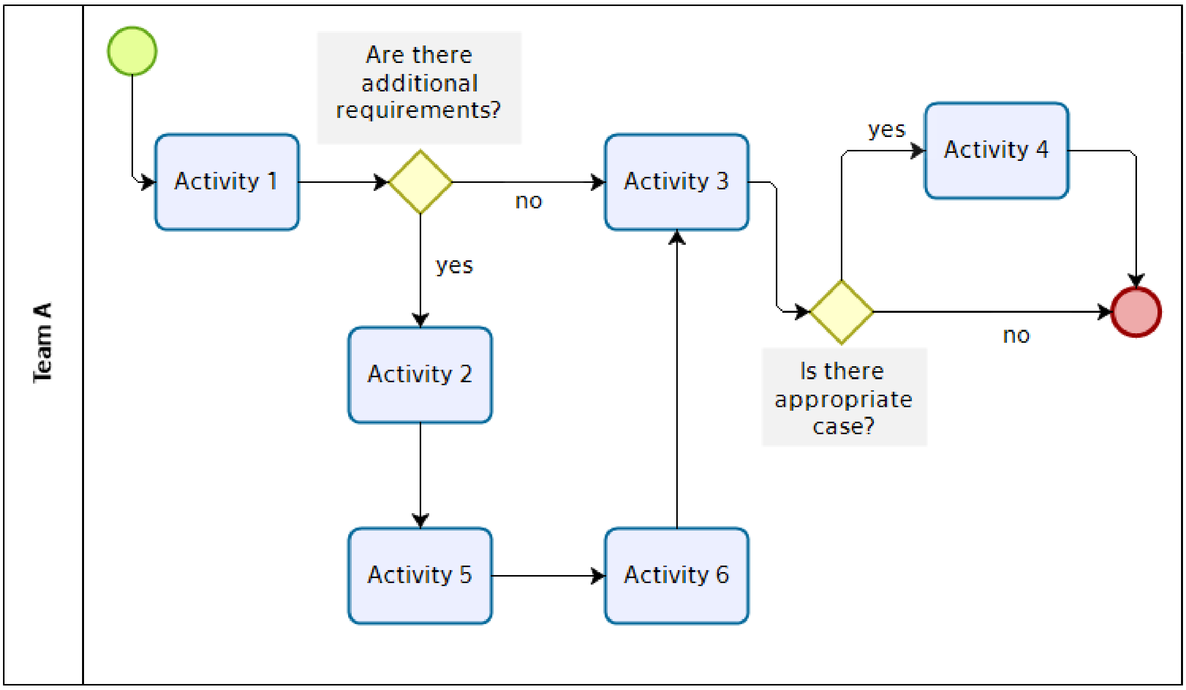

Figure 17 "BPMN model of 1.1 Calculation process (anonymised version)" [Author's figure]

Next is a description of some parts of the process from figure 17:

1.1 Calculation

Activity 1 will be provided by Worker 1.

If there will be some additional requirements, Activity 2 will be provided by Worker 1.

Activity 3 will be provided by Worker 2.

In appropriate case Worker 3 will provide Activity 4.

Activity 5 and Activity 6 will be provided by Worker 1, if Activity 2 will be required.

Before modelling, it is needed to go through the description and identify processes and activities. Then find controllers, which belong to that processes. If possible, try to identify sensors and actuators. However, for SDCPS purposes sensors and actuators are not required for now. And when we talk about mechanics and other hangar workers, almost of their sensors and actuators are human-integrated.

There are six activities in the *Calculation* process and three controllers. Controller *Worker 1* performs *Activity 1, 2, 5* and *6*. *Worker 2* performs *Activity 3* and *Worker 3* performs *Activity 4*.

How to model activities is shown in figure 17. Also, it is necessary to assign a controller to each activity, because in STAMP, every activity should have its controller. According to BPMN 2.0, the resource, which is responsible or performs an activity is called the Performer. The performer can be an individual, a group, an organization role or position, or an organisation. However, each activity may have only one performer. [37]

In figure 18, there is a way how to assign performer (controller) to activity. In Bizagi Modeler, "Performers" attribute can be used for the purpose, but other BPMN software may offer different options, including customized attributes. In case if there are multiple controllers of the same process, all need to be listed in the tool. However, according to BPMN 2.0, it is not possible to assign two or more performers to an activity. To solve this problem, I propose to choose one of the controllers, which has the most responsibility for the activity and define them in performer attribute. Other performers have to be described in the labels of unsafe control actions listed with the activity.

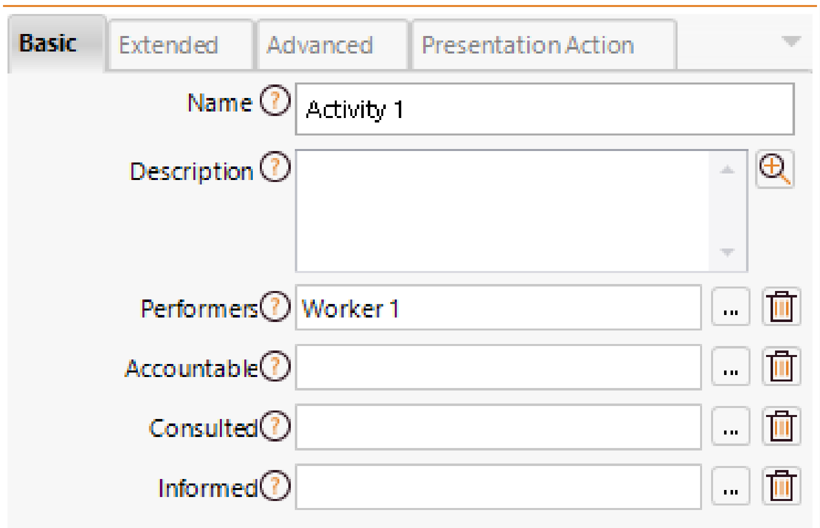

Figure 18 "Definition of a Controller in BPMN" [Author's figure]

Bizagi Modeler allows to create a list of performers (controllers) (*see figure 19*). This can be used to build a list of controllers in future SDCPS system.

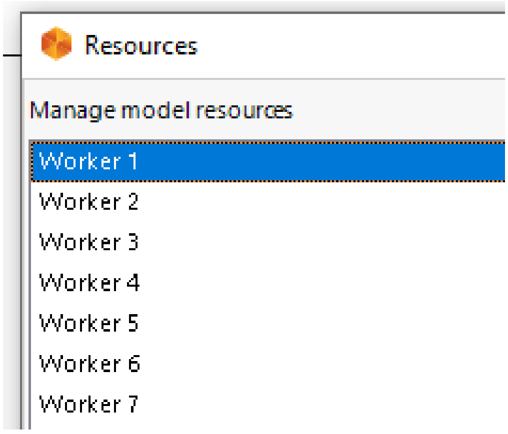

Figure 19 "List of Controllers" [Author's figure]

STAMP control loop contains not only process and controller, but sensors and actuators too. Using BPMN 2.0 language there is a possibility define Sensors and Actuators to a Controller using Artefacts (Data source). However, I used performer description in Bizagi Modeller for that purpose. It was better for STAMP, because every Controller has unique list of sensors and actuators. When for every activity with the same controller there will be new Data source, there is a possibility to lose information. In figure 20 is a proposal how to write down list of sensors and actuators to a current controller.

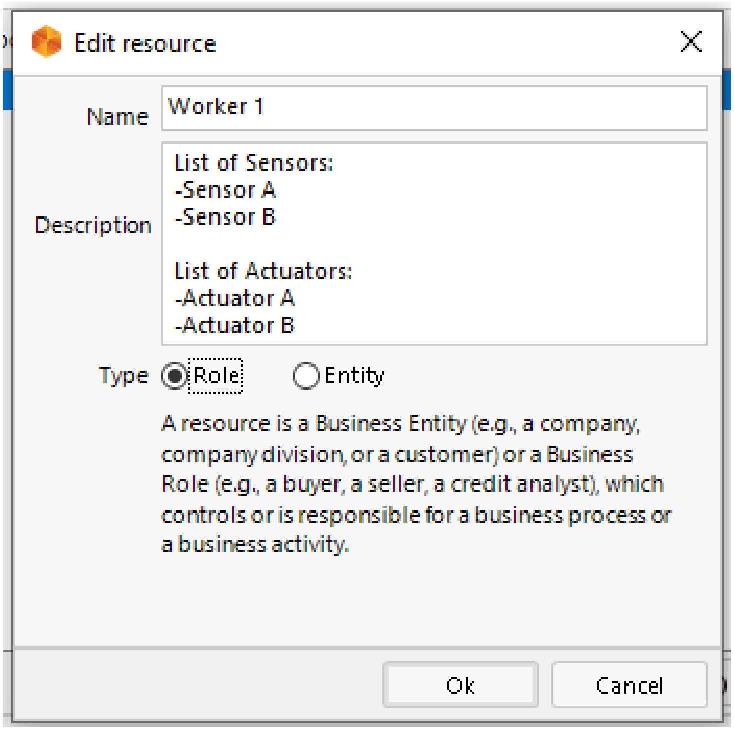

Figure 20 "List of sensors and actuators" [Author's figure]

After definition of a STAMP Control loop in BPMN software, there is a need to extend the model by application of STPA. This extension gives an opportunity to a safety expert to work with and collect not only positive activities, but potential unsafe control actions too.

In figure 21 there is a proposal how to use a part of STPA. Each activity (blue rectangle) contains a description or an extension window. Bizagi Modeler, for example, has an extension window where it is possible to list unsafe control actions. That actions are derived from an activity. For softwares, which do not have extension window, unsafe control actions can be described in activities description or using Data source attributes.

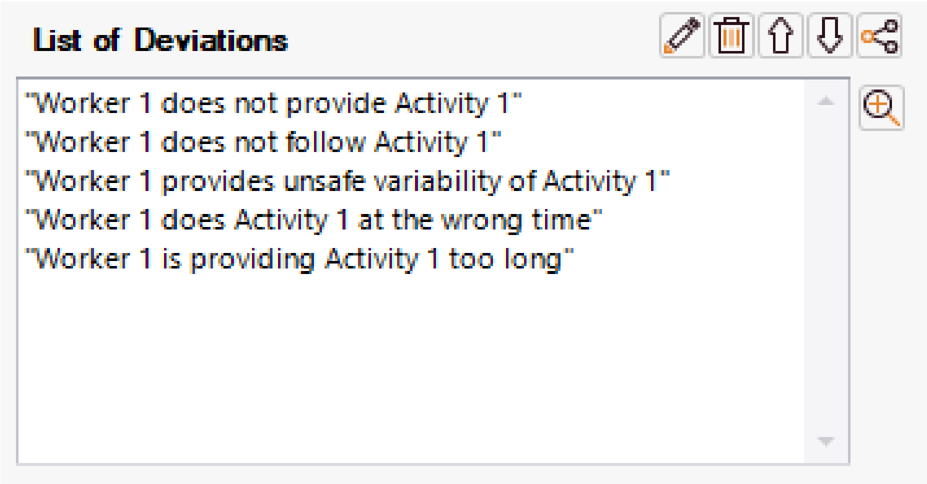

Figure 21 "List of Deviations" [Author's figure]

Also, according to my own experience I recommend to extend List of Deviations[9] (unsafe control actions) by elicitation of safety experts. Regarding my experience, there is a very small probability that STPA will not define all unsafe control actions, although not due to issues with the methodology as such, but due to some practical limitations in the industry. For example, some processes can be written incorrectly or information may be missing. Safety experts have in-depth knowledge about processes and so they can be asked in such cases.

[9] Deviation is a working title for the term "unsafe control action". This was used only for research purposes.

Summary of the modelling procedure

1. Define the scope of a procedure
2. Define the level of modelling abstraction
3. Identify activities in a process, including controller and their sensors and actuators.

   In case of loss of information:

   3.1. Ask responsible person about respective process

   3.2. Study additional documentation
4. Model the information using BMPN 2.0 language
5. Validate the process flow

5. Proposal of MRO's SDCPS based on STAMP and BPMN

ICAO action plan for the establishment and implementation of safety data collection and processing systems has three main phases [29]:

1. Initial diagnostic phase
2. Process design/review
3. Safety and Support software development/review

However, activities described in that phases are prepared for a State's SDCPS, not for MROs. Otherwise, it is applicable for MRO's SDCPS proposal too. Next are some of the activities and requirements, which are needed for SDCPS establishment:

1. Definition of technical specifications:

   1.1. Inputs (collection)

   Reactive sources

   - Causes and contributing factors
   - Safety investigation database
   - Hazard[10] identification

   Proactive sources

   - Hazard reports
   - Hazard identification through inspections and audits
   - Hazard identification through safety assessments

   Predictive sources

   - Hazards from operational changes,
   - Observation of hazards behaviour and their trends

   1.1. Processes (analysis)

   1.2. Outputs (exchange)

2. Definition of SDCPS structure
3. Setup of safety database
4. Assessment of accidents and incidents database
5. Assessment of mandatory and voluntary reporting system database
6. Assessment of safety oversight inspection and audit report/finding database
7. Ensuring compatibility with ECCAIRS

[10] *"A condition or object with the potential of causing injuries to personnel, damage to equipment or structures, loss of material, or reduction of ability to perform a prescribed function."* [3]

8. Ensuring possibility to import and export safety database
9. Implementation of Risk management

According to that points, the MRO's SDCPS has to be rather a complicated software, which will have its own database, analytical part and statistical module[11]. SMS's tools with SDCPS module described in chapter 3 fulfil those requirements. They are good for the purpose to collect hard data, and also their factors classification is based on required ECCAIRS taxonomy. However, such software does not work with systemic safety models and cannot collect and process detailed soft data, which describe organization in-depth.

5.1 Proposal of data collection and analysis

First thing, which has to be changed in an SDCPS for MROs to be based on STAMP is a process of safety data collection. Often information (safety data) related to an occurrence is described in Maintenance Safety Report (MSR). MSR always contains hard and soft data. In appendix 1 there is a Maintenance safety report form which is using by FAA and was designed by NASA.

As we can see, that form can be divided into two parts:

- The first part is on a page 1, there are fields designed for collecting hard data. From that part it is possible to collect different hard data for statistics, for example, a time of occurrence (assessment of the riskiest part of the day), factors related to a mechanic training (to find if some training is insufficient for safety), phase of maintenance, when the problem was detected, etc.
  Also, there are additional fields, which can be used for classification of safety data. They are similar to ECCAIRS taxonomy or originating from it. For instance, classification using occurrence class (Accident, Serious accident, incident, Occurrence without safety effect, Not determined), occurrence category (ADRM: Aerodrome, SCF-NP: System/component failure or malfunction, OTHR: Other and etc.). For MROs, there no appropriate Occurrence category for maintenance occurrences. It shows a gap in the current ECCAIRS taxonomy.
- The second part is on page 2 and 3. It is a place for narrative text. There has to be a description of the event, situation, occurrence. A safety expert can gather

[11] Statistical module is used here as a general term that refers to what is known as a safety dashboard in SMS

the necessary information by the event description, but he cannot process that data. In particular, when there are a lot of different reports, there is no possibility to remember all details from all reports. The description always contains important information about an occurrence, but there is no possibility how to process that information and do some analysis and statistics on it. For example, a reporting tool INBAS (described in chapter 3) gives a possibility to create a contributing factor chain, which can help to process narrative information. Safety expert can use the description to find the main factors of an occurrence and to write them down into INBAS using taxonomy (ECCAIRS and MEDA).

Regarding part 1, which addresses a collection of hard data, for safety performance goals that type of collecting and processing is sufficient as it is now. However, there is a need to change data collection and processing in part 2 (describing the occurrence).

Majority of occurrence descriptions contain structured information, which is close to procedures structure. There is information who performed what activity or which was omitted. Mostly, when safety expert investigates an occurrence, he uses procedures for identification if all activities were performed according to them, or not. It means that the appropriate way, how to collect soft data about occurrence description, is to use the approach from chapter 4.3.

Now three problems are resolved:

1. Weak parts of existing reporting forms – Narrative description
2. Definition of data types contained in narrative description
3. Transformation to computer-readable language and analysis definition

The next step is to define, how procedures from BPMN 2.0 language transfer to SDCPS system and how it can look like.

For that purpose, one of the advanced solutions capable of creating smart systems is to use ontology engineering. This approach was taken within the research project with CSAT, and I also studied this subject in my Bachelor's thesis "Conceptualization of Selected Parts of STAMP Safety Model". [36] Within the research project, my part was to test the STAMP ontology proposed by ontology engineers; details of the evaluation and analysis of its suitability for MRO's SDCPS done by me is provided in chapter 6 of this thesis.

Considering the fields for filling safety data, it has to look similar to a BMPN software pool interface. There has to be a space, where safety expert will put a process or processes, which he thinks were involved in an occurrence. After that, to each activity there has to be a list of predetermined unsafe control actions, which could happened.

According to ICAO and EASA, there has to be a possibility to classify data by taxonomies. Existing reports forms use taxonomies to define occurrence categories or classify data. These existing taxonomies can be used to define loss events, or general occurrence description in a new SDCPS.

For example, a safety expert investigates or just reports a situation, where there was a maintenance mistake with some aircraft component. In that case, the occurrence can be classified by ECCAIRS taxonomy like "Incorrect Repair of Component". Consequently, in a statistical module, safety expert will have a list of different unsafe control actions or procedure activities, which always cause Incorrect Repair.

To summarise the chapter, there are some main ideas what STAMP based SDCPS investigation and reporting tool has to contain:

- Space to work with process, its activities and unsafe control actions
- Possibility to work with several processes in one report
- List of ECCAIRS or other taxonomies to classify an occurrence or to define a loss event
- Versioning of the process models, because of the possibility of process update

5.2 Proposal of statistics module

Using STAMP in investigation and reporting gives an opportunity to improve existing statistical module. Thanks to STAMP and BPMN modelling, the SDCPS can have the following statistics blocks:

- The trend of the most problematic Processes
- The trend of the most problematic Controllers
- Specification in which process most of the unsafe control action occurred
- Specification which unsafe control actions and normal actions contribute to an occurrence
- The trend of problematic processes which caused a loss event without predetermined unsafe control actions. There is a possibility to determine if there is a procedure, which was designed unsafely.

- List of the problematic teams. Controllers which perform activities in the same process can be collected to one team. Internal SDCPS can contain a special list of controllers with their IDs. For that purposes information from the existing MRO software infrastructure can be used.
- List of problematic departments. If in MRO organisations BPMN model will contain an organisational chart, there can be a module with information in which department there are a majority of unsafe controllers.

Also, during an external audit, safety expert will not have to lose time during preparing information if problematic processes were improved after the last audit. That statistical module will show all detailed changes inside the organisation.

5.3 Example occurrence investigation using SDCPS based on STAMP

To show how the occurrence investigation can be performed by the proposed SDCPS, I used parts from a real accident safety report from National Transportation Safety Board (NTSB). Also for a short representation, how such investigation can be provided inside MROs, I prepared a short general representation in figure 22.

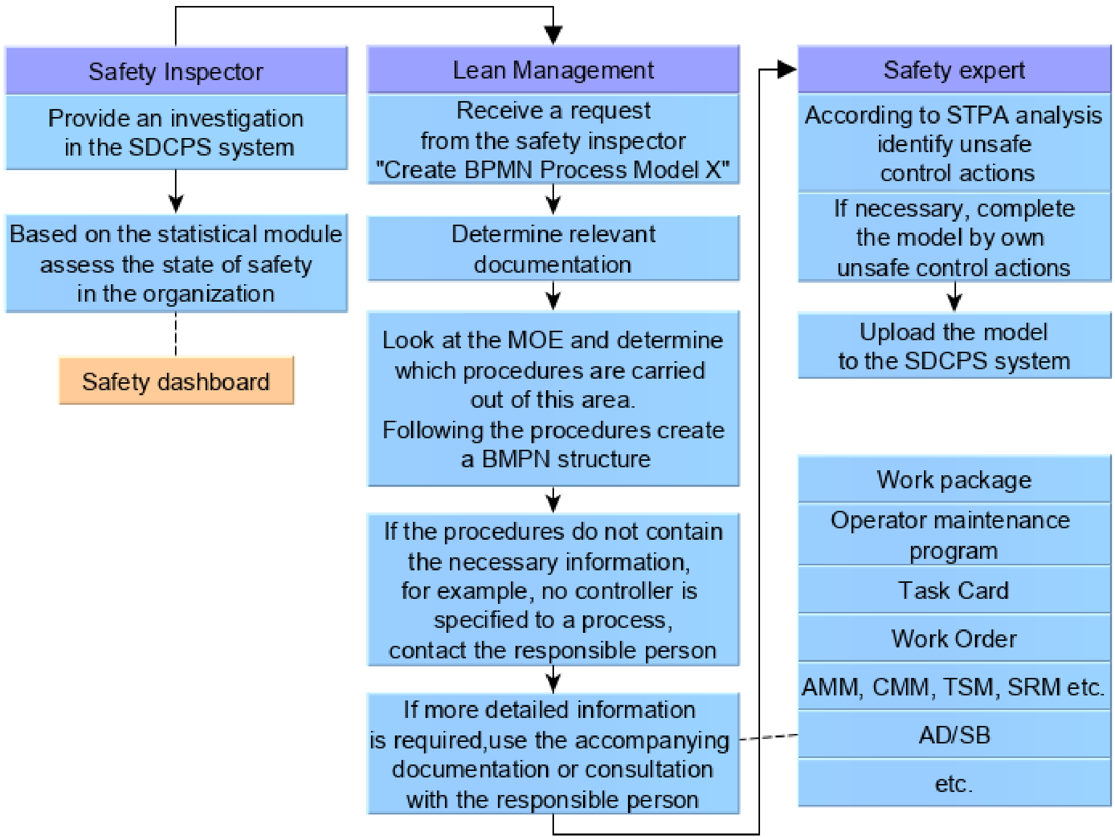

Figure 22 “Algorithms of investigation using SDCPS based on STAMP” [Author’s figure]

One of the main factors, which caused that accident were maintenance failures. An aircraft was destroyed, and two people died. Description of the accident is provided below. I highlighted parts from NTSB analysis description, which I modelled in figures bellow (figure 23 and figure 24) [31]

"The proto-type experimental light jet airplane was departing on a local maintenance test flight. Witnesses reported that the airplane entered a right roll almost immediately after liftoff. The roll continued to about 90 degrees right wing down at which point the right wingtip impacted the ground. During examination of the wreckage, ***the aileron control system was found connected such that the airplane rolled in the opposite direction to that commanded in the cockpit****. The maintenance performed on the airplane before the accident flight included* ***removal of the main landing gear (MLG)*** *in order to stiffen the MLG struts. Interviews with the mechanics who performed the maintenance revealed that during re - installation and system testing of the MLG, it was* ***discovered that the changes to the MLG struts impacted the V- bracket holding the aileron control system's upper torque tube****. The V-bracket was removed and a redesigned V-bracket was installed in its place. This work required the* ***disconnection of a portion of the aileron control system****, including the* ***removal of the aft upper torque tube bell crank from the torque tube****.* ***The mechanic*** *who reinstalled the aft upper torque tube bell crank* ***was under the incorrect assumption that there was only one way to install the bell crank on the torque tube****. However,* ***there are actually two positions in which the bell crank could be installed****. The incorrect installation is accomplished by rotating the bell crank 180° about the axis of the torque tube and flipping it front to back, and this is the way the bell crank was found installed.* ***With the bell crank installed incorrectly*** *and the rest of the system installed as designed, there is binding in the system. This binding was noticed on the accident airplane during the inspection after initial installation. However,* ***the mechanic did not recognize that the bell crank was improperly installed on the torque tube****. Instead of fixing the problem by removing and correctly reinstalling the bell crank,* ***he fixed the problem by disconnecting the necessary tie rods and rotating the upper torque tube*** *so that the arm of the bell crank pointed up and to the left. This action reversed the movement of the ailerons. According to all of the personnel interviewed,* ***there was no maintenance documentation to instruct mechanics how to perform the work*** *since this was a proof-of-concept airplane.* ***None of the mechanics who performed the work could recall if the position of the ailerons***

in relation to the position of the control stick was checked. *Such a position check, if it had been performed by either the mechanics after the maintenance or by the flight crew during the preflight checks, would assuredly have indicated that the system was installed incorrectly."*

NTSB defined following probable cause and findings:

- **Incorrect installation by company maintenance personnel** of the aft upper torque tube bell crank resulting in roll control that was opposite to that commanded in the cockpit.
  Contributing factors:
    - **The lack of maintenance documentation** detailing the installation of the bell crank
    - The installing **mechanic's incorrect assumption** that the bell crank could only be installed in one position
    - **The failure of maintenance personnel** and the flight crew **to check the position of the control stick** relative to the ailerons after the maintenance and during the preflight checks.

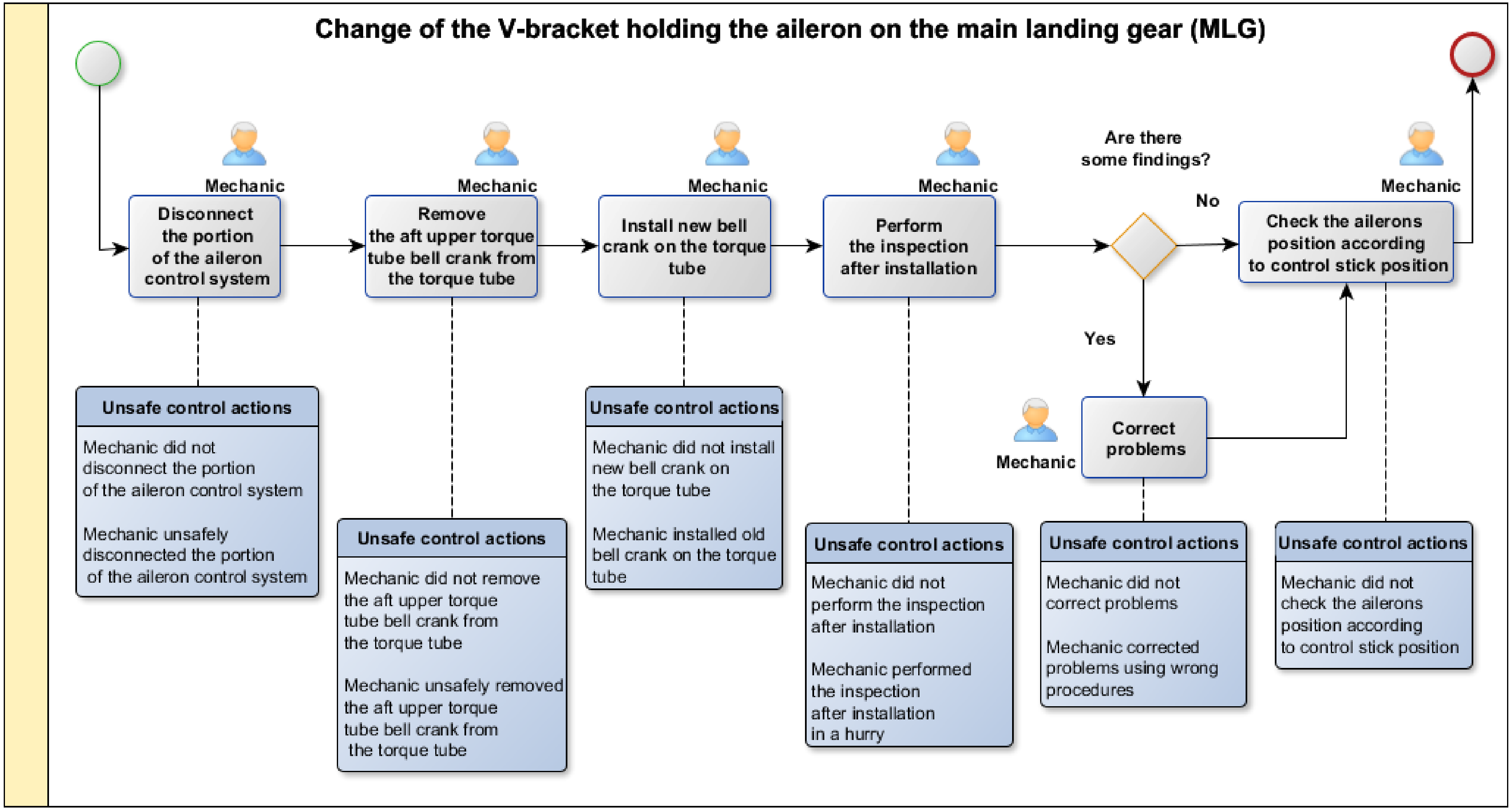

Figure 23 "Model of an accident in a BMPN 2.0 language" [Author's figure]

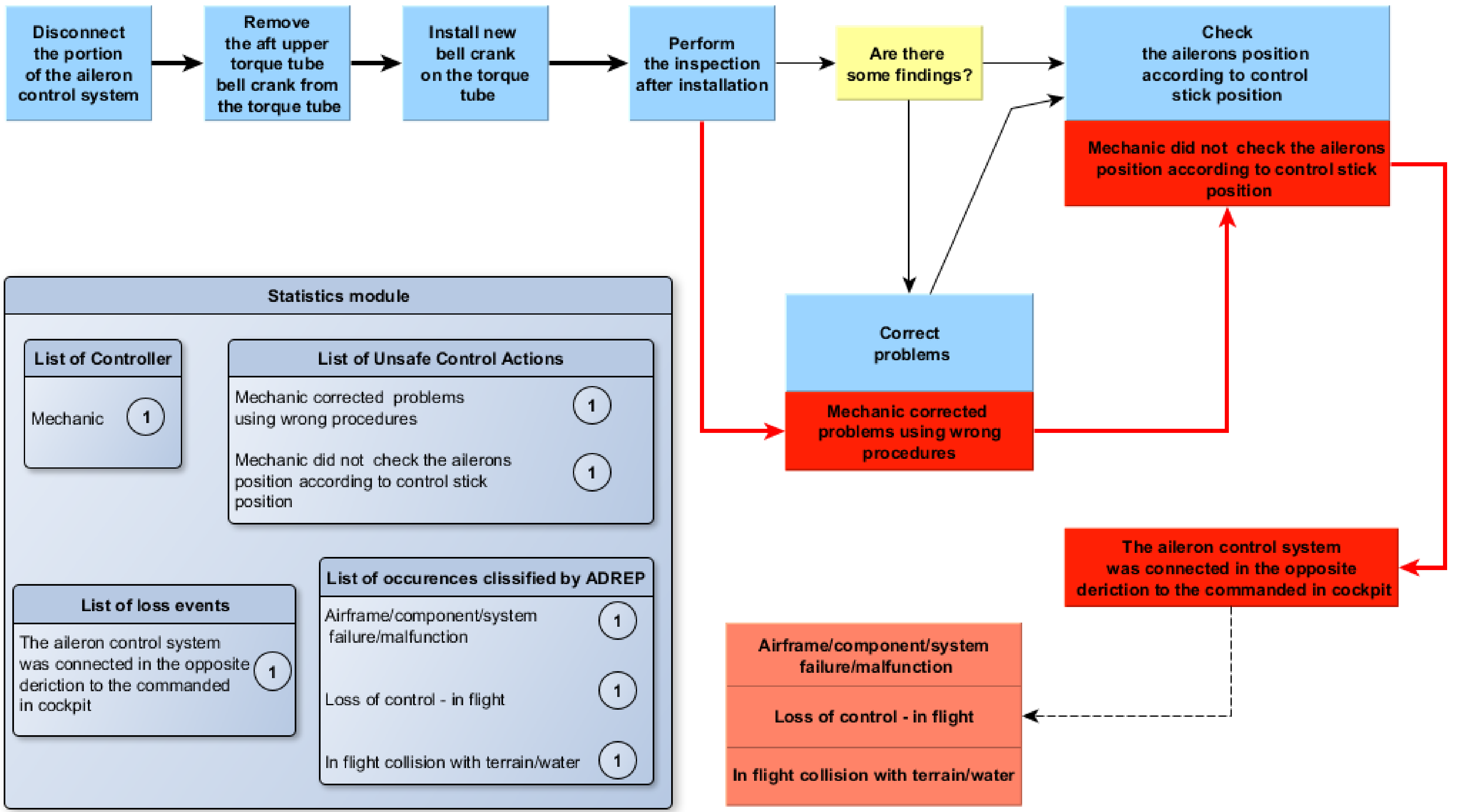

Figure 24 “Investigation with the proposed SDCPS system” [Author’s figure]

As you can see, in figure 23 I modelled using BMPN language basic model with some unsafe control actions. All NTSB findings were identified as STAMP unsafe control actions. NTSB contributing factors *The failure of maintenance personnel to check the position of the control stick*, *The lack of maintenance documentation* and *Mechanic's incorrect assumption* were defined by STPA. Regarding the factor *Incorrect installation by company maintenance personnel*, this unsafe control action would be identified during STPA analysis of an upper process *Change of the V-bracket*. That unsafe control action could be named "Change of the V-bracket did not provided" or "Change of the V-bracket provided incorrectly".

In figure 24, there is a representation, how that investigation could be processed in an SDCPS system. Safety expert would get a maintenance process, choose which unsafe control actions happened and, in result, get statistics from occurrences with that situation. The statistic module can automatically show frequencies from all reports, that would show how many times an unsafe control actions happened with particular mechanic and in particular context. Also, there are a possibility to classify the occurrence according with ADREP taxonomy and get overall statistics, although at more general level.

6. Validation of the proposed solution

Validation of the proposed solution was performed during my assistance in the project No TJ01000377, in three steps. The first one was to check BPMN models for syntax in Bizagi, for completeness and correctness with CSAT. The second one was modelling of safety data based on BPMN artefacts and comparison with current SDCPS and statistical module at CSAT. The third validation was discussions with experts about the usefulness, meaning and benefits of the newly proposed SDCPS.

6.1 Validation of the BPMN model

BPMN model verification was provided in three steps:

1. After a model creation, I prepared a list of questions, which referred to procedures content. After that, I attended meetings with specialists, who execute these procedures. It was an informal conversation, where I asked procedure's performers to describe what they are usually doing during these processes. It was better to let them speak continuously without interruption, because they reproduced their activities flow automatically, without thinking about rules from procedures. If there was not an information I needed, I asked them relevant questions from my list. That verification gave me information about BPMN model content. It would show, if there had been necessary information missed.
2. The second way was comparing my models with existing CSAT BPMN models. These models did not contain all procedures that I needed, but there were some parts from them. It gave me a possibility for partly checking the models. Also, I asked experts from CSAT to check if my models contain all relevant information.
3. Bizagi Modeller software can check if model BPMN notation was followed. I used that tool to check semantics of my models. Also, there is a module, where you can simulate processes. I used this simulation to check if all activities are provided step by step. Simulation module can show different scenarios too. I used it to check if all that scenarios could happened in real life situation.

6.2 Comparison of the proposed MRO's SDCPS with current SDCPS at CSAT

There are some internal confidential ways how CSAT collects its safety data. I studied those particular rules and tried to collect their safety data from MSRs by myself.

After that, I used 20 internal CSAT incidents to model them using the new SDCPS approach. Modelling was carried with Protégé[12] tool. Protégé allows conceptual (ontology) modelling of future software systems.

As said in chapter 5.1, my part in a project was to test the STAMP ontology. This ontology I was testing through incidents modelling. During the modelling, I distinguished particular data from investigation, which can be processed in the SDCPS. Next I modelled them using existing ontology. After that I checked the Protégé output which data it shows to me and in which form.

According to that testing, first of all I helped to revise mistakes in the ontology. Secondly, speaking about validation goals, I checked if this new SDCPS will collect and process the particular safety data what I wanted.

6.3 Discussions with experts about proposed SDCPS

Last, but not least, verification of the proposed SDCPS was provided during discussions with safety experts. I showed the main ideas to safety and quality department in CSAT and they gave me their opinions.

They found that there are some advantages and disadvantages in the new approach to SDCPS system. First of all, they appreciated the possibility to collect and to analyse new types of data. They found it useful for soft data processing. Also, that approach can help them to control different maintenance documentation procedures. During the modelling, there is a possibility to find gaps in information. Also, in that approach, they found bridges how to connect existing maintenance software to collect more data from maintenance operations for safety performance goals.

However, they found one serious disadvantage in that approach. Procedure models have to be checked and improved all the time because of procedure changes. That

[12] Protégé was developed by the Stanford Center for Biomedical Informatics Research at the Stanford University School of Medicine. (https://protege.stanford.edu/products.php)

type of work needs a special expert, who will be able to work with BMPN, understand maintenance operations and safety.

6.4 Summary

There is my comparison conclusion in table 3:

Table 3 “Comparison of the nowadays and proposed SDCPS approach” [Author’s table]

Old SDCPS MROs approach	Proposed SDCPS MROs approach
Hard data collection, processing and analysing shows all relevant information for safety performance indication	Stay same
Soft data is collected only like a narrative text	Soft data is collected using STAMP-based classifiers. Now it is not just a text, it is a box with data distributed to different particular boxes (Soft data database is used)
Factors classification is provided using common worldwide taxonomies. That taxonomy does not fulfil MROs needs.	Factors classification is provided by specific internal data description, based on BPMN models
Statistical module contains only hard data or generalised factor classification trends.	Statistical module additionally contains specific soft safety data. There is information about particular processes, controllers, sensors and actuators. Statistic module contains and analyses data from incident description.
Component-based approach to safety	Systemic approach to safety
Maintenance documentation is used only as an administrative resource.	Possibility to revise maintenance documentation procedures. Possible process gaps can be identified.
Factor’s classification taxonomy has to be checked and updated all the time.	Procedure models have to be checked and improved all the time
Do not need extra specialists	Needs a special expert, who will be able to work with BMPN, understand maintenance operations and safety

6. Evaluation of the proposed solution

In this chapter I would like to discuss the new SDCPS system approach. SDPCS system has to do three main things: data collection, data analysis and data exchange.

Speaking about data collection evaluation, I found one main advantage. It gives a possibility to collect and process new types of safety data. Existing SDCPS systems can collect soft data like a narrative text or use common safety taxonomies. However, they cannot be used well in statistics. That systems today cannot convert data from narrative text to a structured form for statistical module.

Nowadays approach to collecting and processing data is aimed to work with hard data, as a result of historical thinking about safety. This approach leaded safety experts to pay more attention to hard safety data. For example, safety managers were focused on a death counting or on money loss evaluation. That approach lead safety experts to blame mechanic failures for the most occurrences.

The new approach proposed in this thesis leads safety experts to collect specific safety data, which describe occurrences in different aspects. That approach guides through the whole situation and forces to think about not only blaming, but also about what in particular situation happened and why. During an occurrence investigation, safety expert can intuitively find if there was a problem with mechanics and the way they work, or the process was designed incorrectly.

The new SDCPS system based on the proposal in this thesis works with systemic approach to collecting data. It means that safety department will collect and process complex soft data from internal processes. There will be an information about what is necessary to perform during the processes, and which kind of unsafe control actions can happen and already happened. The new SDCPS will collect detailed information about process' controllers with their attributes.

Nowadays, safety experts have such data in a narrative text. However, it takes a lot of time to study that information. Also, after an investigation, that soft data can be lost in time and cannot influence future organization safety. The present situation is that the only influence from the soft data on safety performance is providing safety recommendations that are exclusively based on expert assessment.

The new approach to data collection and processing can resolve that problem. If safety data will be collected according to that approach, they will be saved in a computer database form. That database can be used in everyday safety work. Additionally, that data will be influencing safety performance for a long time.

In future, soft safety data collection can be performed not only by using BMPN models. New maintenance planning software have modules, which contain information about maintenance activities, performers and other necessary information which can affect aviation safety. That gives a possibility to connect SDCPS with external software.

Speaking about safety analysis, collecting new safety data gives an opportunity to use new safety models. Proposed SDCPS uses only STAMP model, but there is a possibility to build a connection to other systemic safety models and methods. Systemic approach to safety is new and can be used in future. Some of well-known institutions like a MIT, NASA, Eurocontrol and etc are interested in Safety-II safety approach. There are some researches about Safety-II systemic approach and, for instance, in NASA STAMP was applied for several use-cases in safety analysis. [23] That is a reason to start and implement STAMP based SDCPS, because it is likely that a new systemic safety approach can become standard in the future, including the aviation.

Of course, obligation is not the main reason to use the new approach to SDCPS. That approach shows us how to work with specific internal data. In statistics module, safety experts will have additional trends. For example, which process is the most problematic, or which controller does most of unsafe control actions. Also, there is a possibility to audit, how safety recommendations and process changes affect safety situation inside an organization. All that analysis will be provided automatically by SDCPS.

By discussing safety data exchange, MROs could share more detailed information about safety. That data will be specific for particular kind of repairs or maintenance processes. It gives an opportunity to warn MROs community about safety problems in more detailed way. It can help to judge from conventional safety data classification, for example, how much damages to an aircraft was due to mechanic failure. And start to talk about, for instance, which part of the particular aircraft was damaged due to specific unsafe control actions.

There are also some aspects, which will affect start of using the new SDCPS MROs approach. The first one is a suitability of using that approach. Today it looks almost impossible to build such system in an organisation. Mainly, it is caused by necessity of translating organisation procedures to BMPN language. However, first of all, most of the big corporations have Lean managements departments, that are processing procedures and processes by BPMN software. That step is necessary not only because of safety, but to maintain process efficiency. Also, for a safety investigation goals, there is no need to translate all processes. Occurrences usually happen more frequently with particular processes, and not with all of them.

Also, if an organisation only starts with process modelling, this approach gives good background to what information they have to model and can show what information they are lacking in their procedures.

One important thing that can affect using a new SDCPS system, is cost-efficiency. Such system requires a specialist, who will be responsible for a data quality. That person has to work with BMPN language, have knowledge about maintenance processes and, also, understand systemic safety approach. Because of the complexity of that work, such person may not be able to do another activity in safety department except for assurance of data quality in SDCPS system. So, safety department will increase in costs with his or her work. Although, the assumption is that the gain from limiting occurrences and contingencies should significantly outweigh increased costs of safety management.

This thesis considered variability of different maintenance documents and procedures. However, according to the thesis goal, all of them was not modelled. For the purpose to propose MRO's SDPCS, modelling of MOE procedures was sufficient.

Speaking about safety audits, which are used to maintain safety, there is a possibility to extend the new SDCPS by an audit module. However, in line with the thesis goal, the audit module was not proposed, but the potential extension gives an opportunity to improve new SDCPS by internal and external audits.

Conclusion

The goal of this thesis was to propose safety data collection and processing system based on STAMP for maintenance, repair, and overhaul organizations. Before starting proposal activities, I studied the information about SDCPS systems. It made me identify a gap in the soft data collection and processing in nowadays SDCPS systems. This gap I resolved by developing the architecture and workflow of the new safety data collection and processing, that can be used in a new SDCPS system.

During studying existing approaches to how to work with soft safety data today, I identified existing aviation safety taxonomies. Besides the possibility to classify some data using the taxonomies (ECCAIRS/ADREP), the statistical module in today's SDCPS cannot analyse all the data from occurrence reports. It is caused by the form of these data; they are collected in narrative text. Also, speaking about MROs, the existing taxonomies do not contain sufficient detail of event classification to describe all maintenance occurrences.

After that, I studied the issue of maintenance organisations and their documentation to understand, which data MRO's SDCPS will work with. According to that, I understood, that MRO organisation is a sociotechnical system, which needs to work with soft and hard data as a whole.

There are three safety systemic models, which can be used for analysis of such data. According to the thesis goal, the STAMP safety model was chosen.

I modelled MROs processes in BPMN 2.0 language and defined procedures how to improve these processes' models with STAMP based artefacts. In the result, I designed a proposal, how to collect and process soft safety data using STAMP as the basis.

The new approach in collecting and processing was validated in three steps:

- BPMN models were checked for syntax in Bizagi Modeller. Their completeness and correctness were provided in contact with CSAT experts.
- Safety data based on BPMN artefacts were modelled and compared with current SDCPS and statistical module at CSAT.
- I discussed with experts about the proposed solution.

After evaluation of the proposed solution, I found three main advantages of this solution:

- The new approach to soft safety data collection and processing gives a possibility to do a safety performance using unique safety data. That data classify in detail a safety situation inside particular organisation.
- The safety data are described by a systemic safety analysis. It means, that the new SDCPS can use new safety technologies and gives an opportunity to develop SDCPS system to include other systemic models and methods from the domain of Safety-II. Also, this approach collects and processes a control structure data, analysing such data like processes, activities, controllers and their attributes.
- Statistical module will work with internal soft safety data. In this way, safety expert has more information needed to evaluate current level of safety. There are more indicators in statistical module to control a safety situation.

However, there are also some limitations of the proposed solution:

- Implementation of the solution is a time-consuming task. It needs some time to model all processes, which are needed for a safety investigation.
- Models have to be continually checked if they contain current process situation. That model has to be like a life organism (the real system), which is changing all the time.
- It needs a new safety expert, which will support the new SDCPS system. That person has to have knowledge from BPMN modelling, maintenance and safety.

On the other hand, those limitations give ideas in which ways the proposed solution can be developed. First of all, after the situation, when all process will be modelled, or, when that solution will be common in SDCPS systems, there can be developed an extension to other Safety-II models. Future safety data collection and processes can be improved by FRAM or RAG ideas and perspectives.

Furthermore, my thesis was based on resolving maintenance safety occurrence reporting. I suppose that the proposed solution can be extended to a safety audit data collection and processes using the same process modelling approach.

References

1. INTERNATION CIVIL AVIATION ORGANISATION (ICAO). Airworthiness Manual. 3rd edition. Montreal, Quebec: International Civil Aviation Organization, 2014. ISBN 978-92-9249-454-4
2. COMMISSION REGULATION (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks. In: Official Journal of the European Union, Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1589820167562&uri=CELEX:32014R1321
3. INTERNATION CIVIL AVIATION ORGANISATION (ICAO). Safety Management Manual (SMM). 4th edition. Montreal, Quebec: International Civil Aviation Organization, 2018. ISBN 978-92-9258-552-5
4. What is Lean Management. CIO information, news and tips – SearcgCIO [online]. [25.04.2020] https://searchcio.techtarget.com/definition/lean-management
5. AAGESEN, Gustav & KROGSTIE, John. (2015). BPMN 2.0 for Modelling Business Processes. Handbook on Business Process Management 1: Introduction, Methods, and Information Systems. 219-250. 10.1007/978-3-642-45100-3_10.
6. Bizagi Modeler and Modeler Service documentation. [online] [16.04.2020] Available from: https://help.bizagi.com/process-modeler/en/
7. No. 49/1997 Coll. ACT of 6 March 1997 on Civil Aviation and on amendment of Act No. 455/1991 Coll., Trade Licensing Code, as amended. In: Low Gazette, Available from: https://www.zakonyprolidi.cz/cs/1997-49
8. INTERNATION CIVIL AVIATION ORGANISATION (ICAO). Operations of Aircraft. 9th edition. Montreal, Quebec: International Civil Aviation Organization, 2010. ISBN 978-92-9231-536-8
9. INTERNATION CIVIL AVIATION ORGANISATION (ICAO). Airworthiness of Aircraft. 11th edition. Montreal, Quebec: International Civil Aviation Organization, 2010. ISBN 978-92-9231-518-4
10. INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). Annex 19 – Safety Management. 2nd edition. Montreal, Quebec: International Civil Aviation Organization, 2016. ISBN 978-92-9249-965-5

11. European Aviation Safety Agency (EASA) | Mobility and Transport. European Commission [online]. Raimond Spekking [26.04.2020]. Available from: https://ec.europa.eu/transport/modes/air/safety/easa_en
12. REGULATION (EU) 2018/1139 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91. In: Official Journal of the European Union, Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1139
13. What are the areas of responsibility for the Agency? | EASA. EASA | European Union Aviation Safety Agency [online]. easa.europa.eu 2020 [26.04.2020]. Available from: https://www.easa.europa.eu/faq/19233
14. COMMISSION REGULATION (EU) No 1321/2014 of 26 November 2014 on the continuing airworthiness of aircraft and aeronautical products, parts and appliances, and on the approval of organisations and personnel involved in these tasks. In: Official Journal of the European Union, Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32014R1321
15. COMMISSION IMPLEMENTING REGULATION (EU) 2019/1383 of 8 July 2019 amending and correcting Regulation (EU) No 1321/2014 as regards safety management systems in continuing airworthiness management organisations and alleviations for general aviation aircraft concerning maintenance and continuing airworthiness management. In: Official Journal of the European Union, Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1383
16. COMMISSION IMPLEMENTING REGULATION (EU) 2019/1384 of 24 July 2019 amending Regulations (EU) No 965/2012 and (EU) No 1321/2014 as regards the use of aircraft listed on an air operator certificate for non-commercial operations and specialised operations, the establishment of operational requirements for the conduct of maintenance check flights, the establishment of rules on non-commercial operations with reduced cabin crew on board and introducing editorial updates concerning air operations

requirements. In: Official Journal of the European Union, Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019R1384

17. GUIDE FOR TRANSITION TO PART-CAO and PART-CAMO (Revision January 2020). [online] [10.05.2020] Available from: https://www.easa.europa.eu/sites/default/files/dfu/Guide%20for%20transition%20to%20Part-CA%28M%29O%20-%20revision%20Jan%202020.pdf
18. Maintenance Programme - SKYbrary Aviation Safety. [online]. [01.05.2020] Available from: https://www.skybrary.aero/index.php/Maintenance_Programme
19. IBM Knowledge Center. [online]. IBM Corp. 2017 [01.05.2020]. Available from: https://www.ibm.com/support/knowledgecenter/SS5RRF_7.6.1/com.ibm.mavm.doc/welcome.html
20. EUROCONTROL | Supporting European Aviation | EUROCONTROL [online]. Ig [04.05.2020]. Available from: https://www.eurocontrol.int/sites/default/files/2019-07/white-paper-resilience-2009.pdf
21. HOLLNAGEL E., WEARS R.L. AND BRAITHWAITE J. From Safety-I to Safety-II: A White Paper. (2015) The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark, University of Florida, USA, and Macquarie University, Australia. ISBN TBA
22. LEVESON, Nancy G. a John P. THOMAS. STPA handbook [online], (2018) [8.04.20] Available from: https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf
23. LEVESON, Nancy G. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, (2011). Engineering systems. ISBN 978-0-262-01662-9.
24. HANÁKOVÁ L., LALIŠ A., STOJIĆ S., AHMAD J., KOSTOV B., KAFKOVÁ M., SZENTKERESZTIOVÁ K., METHODOLOGY for improving analysis and management of risk with the utilization of conceptual modelling. CTU in Prague (2019) Available from: https://uld.fd.cvut.cz/en/science-and-research/scientific-outputs/
25. HOLLNAGEL, E. (2011). RAG – The resilience analysis grid. In: E. Hollnagel, J. Pariès, D. D. Woods & J. Wreathall (Eds). Resilience Engineering in Practice. A Guidebook. Farnham, UK: Ashgate.

26. HOLLNAGEL, E. (2012). FRAM. The Functional resonance Analysis Method for modelling complex sociotechnical systems. Farnham, UK: Ashgate.
27. Bizagi Modeler - BPM Software - Free Download. Bizagi - Intelligent Process Automation Leader [online]. (2003) [10.05.2020]. Available from: https://www.bizagi.com/platform/modeler
28. LEVESON, Nancy G. CAST HANDBOOK: How to Learn More from Incidents and Accidents. [online] (2019) [11.05.2020] Available from: http://sunnyday.mit.edu/CAST-Handbook.pdf
29. INTERNATIONAL CIVIL AVIATION ORGANISATION (ICAO). Action plan for the establishment and implementation of safety data collection and processing systems (SDCPS). Available from: https://www.icao.int/SAM/Documents/2018-SSP7/Action%20Plan_SDCPS.pdf
30. NASA. ASRS Maintenance safety report form. [online] [01.05.2020] Available from: https://akama.arc.nasa.gov/asrs_ers/maintenance.html
31. NTSB Accident Final Report [online] [10.05.2020] https://reports.aviation-safety.net/2006/20060725-0_SP33_N322LA.pdf
32. EASA (2011). IP44: Evolution / Optimization Guidelines. International Procedure, European Aviation Safety Association. [online] [11.05.2020] Available from: https://www.easa.europa.eu/download/imrbpb/IP%2044%20Evolution-Optimization%20Guidelines%20%20issue%203.pdf
33. INBAS. [online] [15.05.2020]. Available from: https://www.inbas.cz/welcome
34. EU Aviation Safety Reporting [online]. [15.05.2020] Available from: https://www.aviationreporting.eu/AviationReporting/
35. Aviation Safety Management System Database Software by Four Pillars. Web Based Aviation Safety Management System Software for Airlines Airports Maintenance [online] [15.05.2020] Available from: https://www.asms-pro.com/SMS.aspx
36. GUSKOVA, Natalia. Conceptualization of Selected Parts of STAMP Safety Model Prague, 2018 Bachelor thesis, CTU in Prague, Faculty of Transportation science. Ing. Andrej Lališ, Ph.D.
37. OMG | Object Management Group [online]. [15.05.2020]. Available from: https://www.omg.org/spec/BPMN/2.0/PDF/

38. EUROPEAN AVIATION SAFETY AGENCY (EASA). Internal occurrence reporting system (2017) Available from: https://www.easa.europa.eu/sites/default/files/dfu/214626__EASA__IORS__BROCHURE.PDF

Figures

Tables

Appendix 1 "Maintenance safety report" [30]

D

DO NOT REPORT AIRCRAFT ACCIDENTS AND CRIMINAL ACTIVITIES ON THIS FORM.
ACCIDENTS AND CRIMINAL ACTIVITIES ARE NOT INCLUDED IN THE ASRS PROGRAM AND SHOULD NOT BE SUBMITTED TO NASA.
ALL IDENTITIES CONTAINED IN THIS REPORT WILL BE REMOVED TO ASSURE COMPLETE REPORTER ANONYMITY.

(SPACE BELOW RESERVED FOR ASRS DATE/TIME STAMP)

DENTIFICATION STRIP: *Please fill in all blanks to ensure return of ID strip to you.*
NO RECORD WILL BE KEPT OF YOUR IDENTITY. This section will be returned to you.

TELEPHONE NUMBERS where we may reach you for further details of this occurrence:

HOME Area _______ No. ______________________ Hours ________________

WORK Area _______ No. ______________________ Hours ________________

NAME ____

ADDRESS/PO BOX ____

____

CITY _________________________ **STATE** _____ **ZIP** ___________

TYPE OF EVENT/SITUATION

____

____

DATE OF OCCURRENCE (MM/DD/YYYY) __________________

LOCAL TIME (24 hr. clock) (HH:MM) ________________

PLEASE FILL IN APPROPRIATE SPACES AND CHECK ALL ITEMS WHICH APPLY TO THIS EVENT OR SITUATION.

EXPERIENCE

Describe your qualifications	☐ A ☐ P ☐ NDT ☐ repairman ☐ inspection authority ☐ avionics ☐ other______________
What is your technician/maintenance experience in years?	lead technician _________ technician _________ repairman _________ avionics __________ inspector _________ other ___________________________________

FACTORS

Location	____
Was training a factor?	○ Yes ○ No **Reset** ☐ I was instructing ☐ I was receiving training
What other factors may have contributed?	☐ lighting ☐ weather ☐ work cards ☐ manuals ☐ briefing ☐ other ___________________
Check items which were involved in the event	inspection ○ Yes ○ No testing ○ Yes ○ No repair ○ Yes ○ No logbook entry ○ Yes ○ No fault isolation ○ Yes ○ No installation ○ Yes ○ No scheduled maintenance ○ Yes ○ No MEL ○ Yes ○ No *other ______________ *(*Describe in the Describe Event/Situation sector)* **Reset**
Component/System/Sub-system involved: ______________________________	
Was maintenance deferred? ○ Yes ○ No **Reset**	When was problem detected? ☐ routine inspection ☐ in-flight ☐ taxi ☐ while aircraft was in service at gate ☐ pre-flight ☐ other______________

CONSEQUENCES/OUTCOME

☐ flight delay ☐ flight cancellation	☐ gate return ☐ air turn back	☐ improper service ☐ rework	☐ in-flight shut down ☐ aircraft/engine damage ☐ other______________

AIRCRAFT/AIRWORTHINESS STATUS	MISSION	REPORTER ORGANIZATION (Check all that apply)
☐ aircraft released for service ☐ aircraft records completed ☐ aircraft required documents aboard ☐ not released for service ☐ unknown	☐ passenger ☐ personal ☐ cargo/freight ☐ training ☐ ferry ☐ other_______________	☐ air carrier ☐ air taxi ☐ contracted service ☐ corporate ☐ fractional ☐ FBO ☐ government ☐ military ☐ personal ☐ other____________

TYPE OF AIRCRAFT (MAKE/MODEL) AND ENGINE TYPE

type of aircraft ______________	series ______________	ATA Code ______________
aircraft zone ______________	engine model ______________	other ______________

NASA ARC 277D (May 2009) **MAINTENANCE** OMB No. 2700-0172 Exp 7/31/2022

NATIONAL AERONAUTICS AND SPACE ADMINISTRATION

NASA has established an Aviation Safety Reporting System (ASRS) to identify issues in the aviation system which need to be addressed. The program of which this system is a part is described in detail in FAA Advisory Circular 00-46E. Your assistance in informing us about such issues is essential to the success of the program. Please fill out this form as completely as possible, enclose in an sealed envelope, affix proper postage, and and send it directly to us.

The information you provide on the identity strip will be used only if NASA determines that it is necessary to contact you for further information. THIS IDENTITY STRIP WILL BE RETURNED DIRECTLY TO YOU. The return of the identity strip assures your anonymity.

AVIATION SAFETY REPORTING SYSTEM

Section 91.25 of the Federal Aviation Regulations (14 CFR 91.25) prohibits reports filed with NASA from being used for FAA enforcement purposes. This report will not be made available to the FAA for civil penalty or certificate actions for violations of the Federal Air Regulations. Your identity strip, stamped by NASA, is proof that you have submitted a report to the Aviation Safety Reporting System. We can only return the strip to you, however, if you have provided a mailing address. Equally important, we can often obtain additional useful information if our safety analysts can talk with you directly by telephone. For this reason, we have requested telephone numbers where we may reach you.

Thank you for your contribution to aviation safety.

NOTE: AIRCRAFT ACCIDENTS SHOULD NOT BE REPORTED ON THIS FORM. SUCH EVENTS SHOULD BE FILED WITH THE NATIONAL TRANSPORTATION SAFETY BOARD AS REQUIRED BY NTSB Regulation 830.5 (49CFR830.5).

Paperwork Reduction Act Statement - This information collection meets the requirements of 44 U.S.C. § 3507, as amended by section 2 of the Paperwork Reduction Act of 1995. You do not need to answer these questions unless we display a valid Office of Management and Budget control number. The OMB control number for this information collection is 2700-0172 and it expires on 7/31/2022. We estimate that it will take about 30 minutes to read the instructions, gather the facts, and answer the questions. You may send comments on our time estimate above to: P.O. Box 189 Moffett Field, CA 94035-0189. Send only comments relating to our time estimate to this address.

If you want to mail this form, please fold pages, enclose in a sealed, stamped envelope, and mail to:

NASA AVIATION SAFETY REPORTING SYSTEM
POST OFFICE BOX 189
MOFFETT FIELD, CA 94035-0189

Keeping in mind the topics shown below, discuss those which you feel are relevant and anything else you think is important. Include what you believe really caused the problem, and what can be done to prevent a recurrence, or correct the situation. (USE ADDITIONAL PAPER IF NEEDED)

Page 2 of 3

CHAIN OF EVENTS

- How the problem arose
- How it was discovered
- Contributing factors
- Corrective actions

HUMAN PERFORMANCE CONSIDERATIONS

- Perceptions, judgments, decisions
- Actions or inactions
- Factors affecting the quality of human performance

NASA ARC 277D (May 2009)

DESCRIBE EVENT/SITUATION (continued)

CHAIN OF EVENTS	Page 3 of 3	HUMAN PERFORMANCE CONSIDERATIONS
- How the problem arose - Contributing factors - How it was discovered - Corrective actions		- Perceptions, judgments, decisions - Actions or inactions - Factors affecting the quality of human performance

NASA ARC 277D (May 2009)