METHODOLOGY

for improving analysis and management of risk
with the utilization of conceptual modeling

Research project TA CR Zéta No. TJ01000377

Department of Air Transport Faculty of Transportation Sciences CTU in Prague	Department of Cybernetics Faculty of Electrical Engineering CTU in Prague	Prague Airport, Ltd.	Czech Airlines Technics, Ltd.
Hanáková Lenka, Ing. Lališ Andrej Ing., Ph.D. Stojić Slobodan Ing., Ph.D.	Ahmad Jana, Ing. Kostov Bogdan, Ing.	Kafková Markéta, Ing.	Szentkeresztiová Katarína, Ing.

T A Č R

Technology Agency of the Czech Republic

Program Zéta

Methodology for improving analysis and management of risk with the utilization of conceptual modeling

Contents

Introduction 2
1. Goal of the methodology 3
2. Dedication 3
3. Methodology description 3
3.1 Theory of STAMP 3
3.2 STAMP ontology 7
3.3 Application of STAMP ontology 13
3.3.1 Basic information about application 13
3.3.2 Ontology application on the CAST methodology 14
3.3.3 Practical recommendations 19
3.4 Utilization of process documentation and its tools 20
3.4.1 Documentation of a control loop 21
3.4.2 Library of controllers 22
4.1 Comparison with CAST methodology 23
4.2 Comparison with aviation industrial standards 24
5. Application of the methodology 24
6. Economic aspects 25
References 26
List of publications preceding the methodology 27
Appendix 1 28

Introduction

Safety data collection, processing and analysis belongs to basic and essential functionalities of every safety management system [1,2]. In complex socio-technical systems, such as the aviation, it is rather impractical if not completely impossible that operational records of aviation organizations are stored in simple software tools developed e.g. using MS Excel or MS Access environment and, simultaneously, achieving data quality as required by current needs of operations and management, especially in the context of performance-oriented processes of safety management. In fact, even more advanced systems for safety data collection and processing often possess numerous inherent deficiencies and it is the very complexity of aviation operations, which practically disables complete and correct description of a controlled system or specific event. This leads to the safety analyst and his or her conceptualization influencing the content and form of safety records, so as the process of their creation and further management [3]. While there are efforts spent on standardization of procedures and content of safety data by means of legislation, various industrial standards or by development of aviation safety taxonomies, these are largely based on long-term experience with aviation operations and widely accepted models of safety such as SHELL or Reason's model [6], also known as the Swiss cheese model. Undoubtedly, all this verified experience allowed for current high level of aviation safety, but the theory of safety is being developed further and today there is already concrete vision for further progress in the domain [7].

The need for further improvement may seem not significant given the current aviation safety records, however, it is important to realize that the industry is also developing further and one of the aspects of the development is ever increasing complexity and interconnectedness of operations, which is manifested in our limited ability to predict aviation accidents and incidents. Further, is it possible to observe increasing pace of technology modification and innovation, often without opportunity to earn sufficient experience with particular system as the technology is modified or replaced earlier that such experience can be earned [8]. Finally yet importantly, there are new hazards emerging such as unmanned aerial vehicles or new types and modes of aircraft automation, all contributing to new relations among the flight operation participants. They can resonate across the entire industry and so contribute to new types of aircraft accidents and incidents. Under such conditions, it can hardly be claimed that current level of aviation safety is stable and also sustainable in the future with the utilization of current tools.

At present, there is opportunity for further development by utilizing available theory of safety, which is oriented to systemic approach to safety management and which attempts to grasp system-level phenomena of complexity, resonance and emergence [3,8,9]. This methodology builds upon one of the first systemic models of safety - model STAMP (System-Theoretic Accident Model and Processes) [8], developed at the MIT in the U.S. This model was carefully selected due to proximity of its focus and content to current state of safety management in the aviation and because it offers new possibilities for progress with no fundamental changes to understanding of safety issues. The methodology focuses on utilizing systems theory and STAMP with safety data collection and processing systems in the aviation. To achieve necessary practical applicability, the methodology uses modern technology of ontology engineering [10], which allows creation of technologically advanced systems for safety data collection and processing. This technology also allows creation and management of quality data and owing to its conceptualization grounding, it reduces the impact of individual interpretation of a safety analyst on the data quality.

1. Goal of the methodology

The methodology aims to disseminate the results of executed research project No. TJ01000377 by the Czech Technical University in Prague, in cooperation with Prague Airport and Czech Airlines Technics, funded by the Technology Agency of the Czech Republic. The methodology is a summary of knowledge resulting from project execution and it contains key procedures for introducing new functionalities for support of analysis and management of risks in the context of safety data collection and processing. The document aims to further improve the level of safety in the aviation, with some overlap regarding other high-risk industries.

2. Dedication

The methodology is primarily dedicated to middle-size and larger organizations in the aviation industry, which plan to implement or already possess a safety data collection and processing system, typically within their safety management system, and which want to extend it with the newest knowledge from safety theory. The methodology can be also applied in other high-risk industries such as nuclear power installations, chemical industry or in the military, as a support for detailed hazard identification and consequent increase of effectiveness and efficiency of analysis and management of risk, with the use of systemic approach to safety management. Even though the procedure described in this methodology is general, in case of application in other industrial branches, the methodology does not guarantee full correspondence to the specifications of these domains and possible modification should be considered.

3. Methodology description

This section contains core description of key procedures of the new safety data collection and analysis framework. The methodology provides for new technical means of how to realize safety data collection and processing systems compatible with other systems and technologies used in the aviation industry, and as such is primarily intended to be used by technical and engineering personnel supporting development and implementation of the systems. Because the methodology is based on theory of STAMP and its formal representation by means of developed STAMP ontology, the first subsection describes relevant theory and the ontology. Next subsection follows with detailed description of the procedure and principles of the new framework for safety data collection and processing.

3.1 Theory of STAMP [8]

STAMP (System-Theoretic Accident Model and Processes) is predictive model of safety. It is one of the first systemic models of safety, explaining safety as a control problem. The model works with basic assumption that each safety occurrence (accident or incident) bears some failure of the safety control structure in place, i.e. hierarchically organized socio-technical system in which people are organized into operational and managerial positions in interaction with various types of technology and which is proposed as active barrier preventing failure of risk systems, i.e. as a barrier preventing accidents and incidents. Apart from the very organization, work distribution, obligations and responsibilities, there is systemic aspect, i.e.

the need for managing interactions across the entire system. In such a system, the key is information distribution, first of all the feedback from controlled processes to safety control structure. Due to that, STAMP works with feedback control theory-based representation [11] of a socio-technical system and guides the safety analyst to depict relevant parts of a system of interest in line with the theory. The advantage of STAMP-based analyses is utilization of systemic approach to explain safety occurrences, which is in contrast to conventional explanation based on linear factor chain modeling, barrier modeling or descriptive statistics for identification of base trends in monitored occurrence types (i.e. safety performance indicators) [4]. Systemic view of processes guides the analyst to use schemas depicting system parts of interest to explain safety occurrences from the system-level, i.e. analyze why the system failed as a whole. By this, the theory of STAMP established foundation for preventive measures at the system level and not only at the level of individual contributory factors or events.

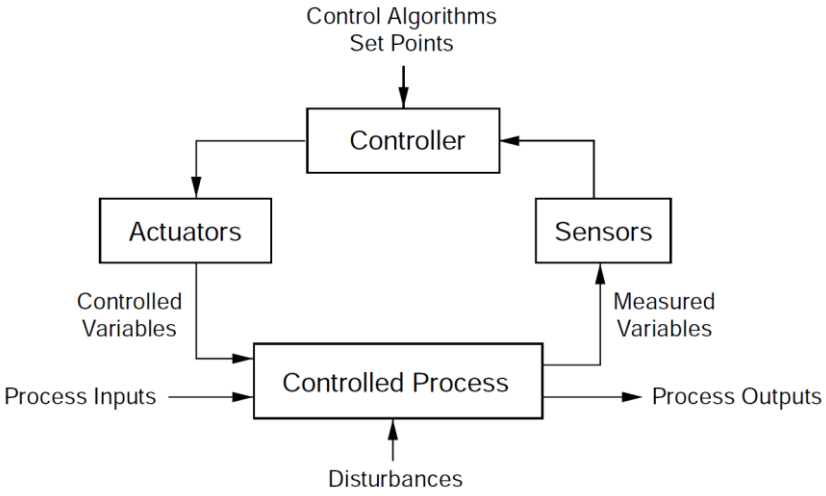


Fig. 1 Control loop based on feedback control theory [8]

As already mentioned, the core for executing STAMP-based analysis is description of system's part of interest in form of diagrams compatible with feedback control theory. The basic building block of such diagrams is a control loop depicted in Fig. 1. The figure shows all elements of a control loop - controlled process, sensors, controller and actuators. Controller can be human or automated. To enable controller to control a process, it is necessary that it has up-to-date information about the current state of the controlled process by means of sensors measuring state variables and also that there are actuators in the system, by means of which the controller controls the process, or more precisely influences specific state variables in the controlled process. The diagram in Fig. 1 can be extended or specified according to given context to progressively establish the entire socio-technical system representation. An example of socio-technical system with focus on safety-relevant processes is depicted in Fig. 2. The figure represents simplified hierarchy of feedback control loops without detailed description of actuators and sensors. As it is apparent from Fig. 2, the system description according to theory of STAMP is an object-based diagram.

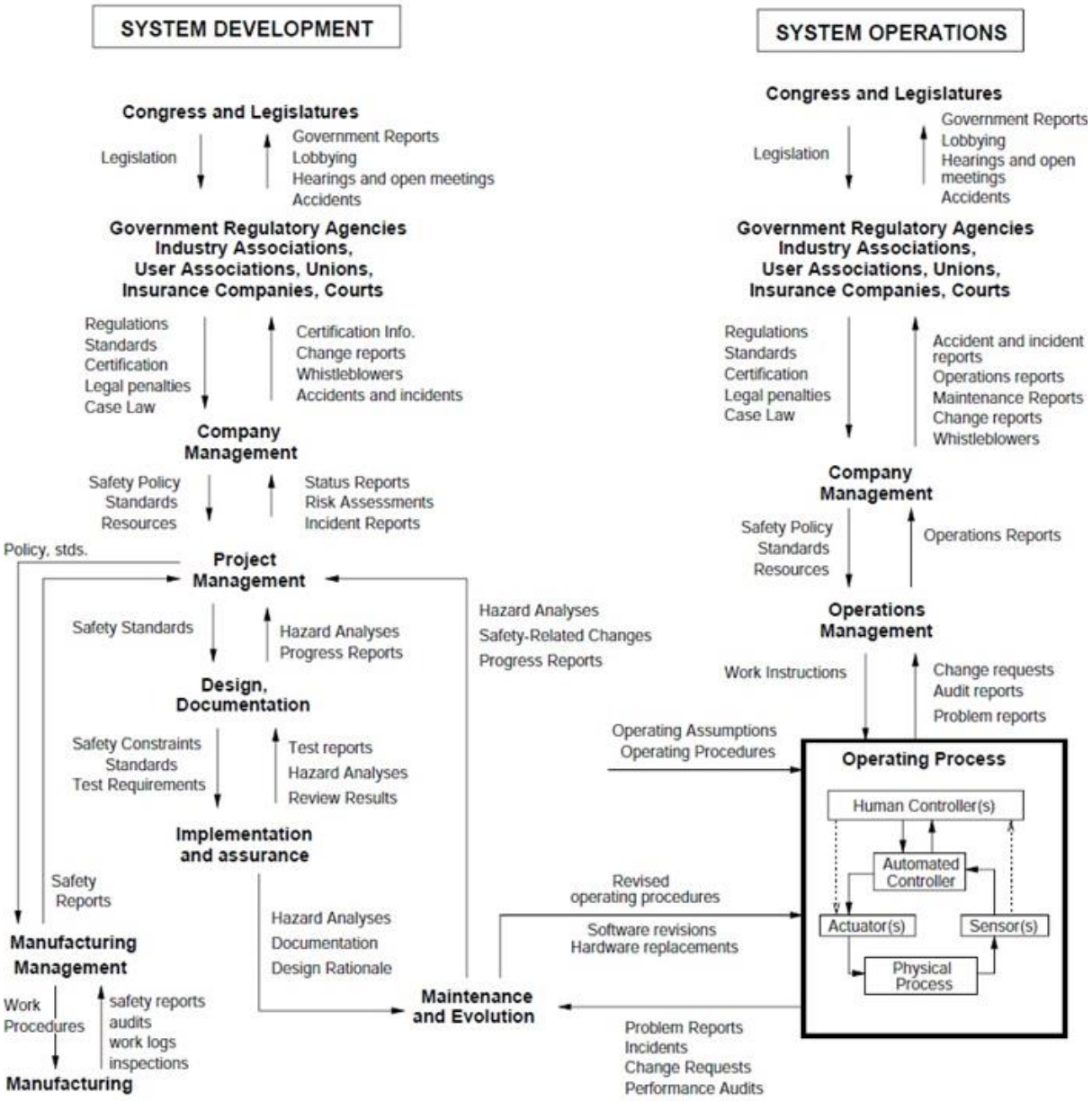


Fig. 2 Generic schema of a socio-technical system [8]

As a support to achieve completeness of safety analyses, the theory of STAMP offers generic taxonomy of all possible safety issues at the level of a control loop, according to Fig. 1. The taxonomy is depicted in Fig. 3 and for safety analyst it serves as a support tool for identification of contributory factors with respective safety occurrence report, or audit findings during typical process of safety data collection and processing. The taxonomy serves also identification of the complete list of hazards in the assessed system, however, this use case in out of the scope of this document.

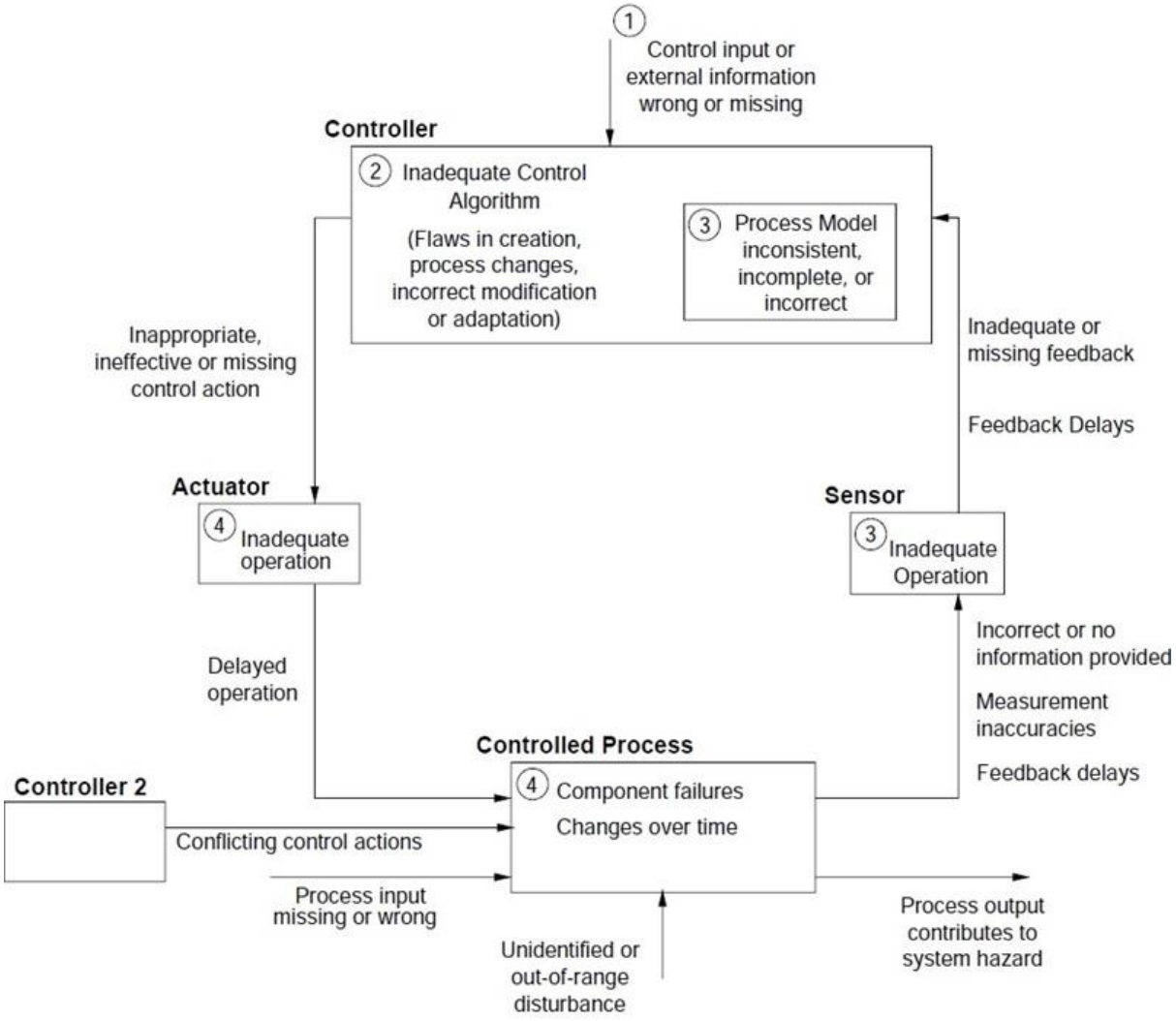


Fig. 3 Basic schema for identification of hazards and taxonomy of safety issues according to the theory of STAMP [8]

From the perspective of data collection and processing, the theory of STAMP offers support in form of CAST (Causal Analysis based on STAMP) methodology. This methodology is primarily dedicated to accident and incident investigation, its content however corresponds to key steps of usual data collection and processing in aviation, both from the perspective of data collection and processing about accidents and incidents, so as from the perspective of usual safety occurrence reporting with no significant impact on safety. The methodology consists of the following steps [8]:

1. Identification of the system(s) and hazard(s) involved in the loss
2. Identification of the system safety constraints and system requirements associated with the hazard
3. Documentation of the safety control structure in place to control the hazard and enforce safety constraint (diagram of feedback control loops)
4. Determination of proximate events leading to the loss
5. Analysis of the loss at the physical system level
6. Determination of how and why each successive higher level allowed or contributed to the inadequate control at the current level

7. Examination of the overall coordination and communication contributors to the loss
8. Determination of the dynamics and changes in the system and the safety control structure
9. Generation of recommendations

From the very steps of the CAST methodology it follows that the base is the documentation of object-based diagram (step 3) describing relevant part of the safety control structure, as per the example in Fig 2. The base for the documentation are steps 1 and 2 which help to narrow the selection of system parts of interest, which take part in the loss. From practical point of view, it is desirable that such a diagram contains only relevant parts of the evaluated system, because complete documentation of the entire system is usually impossible or greatly impractical.

The next steps of the CAST methodology (steps 4 and 5) are typical steps from the domain of accident and incident investigation. In case where safety data collection and processing pertains this type of occurrences, steps 4 and 5 can be executed with no change. If the situation involves an initial report, it may contain only general information which will be complemented during later stages of an investigation. In case where the subject of data collection and processing are data from regular occurrences from operation, which do not classify as accident or incident according to ICAO (International Civil Aviation Organization) standards [12], the steps 4 and 5 can be executed in simplified form, i.e. with no detailed identification of overall chain of events of the reported occurrence.

Steps 6, 7 and 8 of the CAST methodology are steps of systemic analysis, where the safety analyst is tasked to consider the evaluated system with respect to the processed safety data. These steps are innovative analytic steps based on STAMP, since in currently utilized safety data collection and processing systems in the aviation there is no need for correlation of safety data with documentation of a system, which generated the data; basic analysis by means of descriptive statistics to estimate trends and correlations suffice. In the CAST analysis, by contrast, such analysis is absent since analysis and interpretation of data with no system documentation provides insufficient support to propose targeted preventive measures. Correlation of safety data with system documentation, on the other hand, generates guidelines how the controlled system can be modified to be acceptably safe. It also offers base for better risk comprehension and subsequent prioritization of safety issues.

Step 9 concludes CAST methodology and it is typically step of any accident and incident investigation process. In case where the scope of interest are normal everyday occurrences from the operation, recommendations may not necessarily be drawn.

3.2 STAMP ontology

The key parts and aspects of the developed ontology are closely described in this section. The STAMP ontology was designed with two high-level requirements; first, to allow formally specifying statements about STAMP concepts and the relations among them, such as specifying statements about the control structure and the investigated loss as described in the CAST methodology. Second, the ontology was designed to support data integration with other information systems and methodologies.

The STAMP ontology is formalized using the OWL 2 language and aligned with the Unified Foundational Ontology (UFO). The ontology is available online[1].

Fig. 4 shows a fragment of UFO which represents a causal network using its object-event model. Events are characterized by their triggering situation and the situation that they bring about. *Actions* are a special kind of events which are *performed* by *Agents*, i.e. objects with a mental/internal state. *Situations* represent the state of objects and relations among them, e.g. the speed of the vehicle and the structural strength of the aircraft. *Situations* describe the state of affairs before and after the events occur. Apart from that, *situations* can *activate dispositions* of objects such as the structural strength of the aircraft fuselage. The activation of a disposition is manifested as an *event* which brings about a new *situation*. Note, that it is not necessary to describe every aspect of the UFO model in order to create a network. However, specifying additional information allows for automated reasoning according to UFOs formalization of events. For example, when describing causal networks, one can use the *causes* relation between events and the *performs* relation between agents and action events and omit/postpone the description of situations, dispositions and moments of objects.

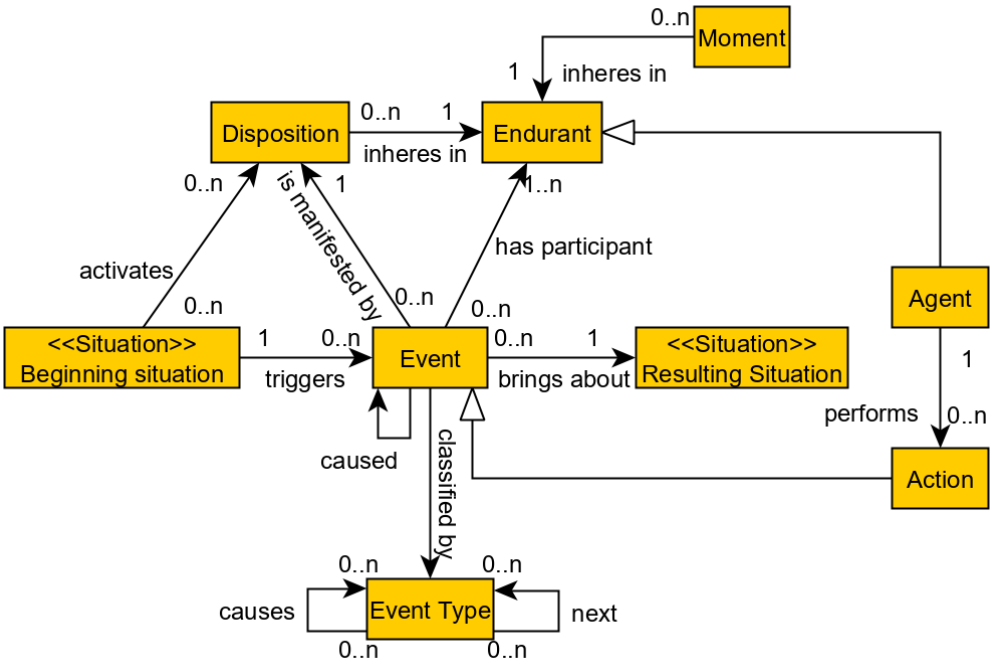


Fig. 4 Basic causal network of objects and events in UFO.

STAMP is based on several widely used conceptual models. The main model used in STAMP is the feedback control model. This model is used to specify the control structure. Apart from that STAMP refers to an object-event model, a causality model, a constraint model and a business process model. The object-event model is used to describe actual events, e.g. loss events in CAST and hypothetical loss event scenarios in STPA (Systems-Theoretic Process Analysis) methodology, even though STPA is out of the scope of this document. The causality models are used to represent the findings of the investigations of loss scenarios (both actual and hypothetical). A causality model typically captures a causal network of events, states and

[1] http://onto.fel.cvut.cz/ontologies/stamp/

object dispositions. In safety, this network leads to a loss event. Finally, business process models are used to represent behavioral patterns and constraints needed to avoid and or minimize losses.

We propose the use of a generic structure which allows to represent both the control structure and the structure of the controlled process, see Fig. 5a. A *Structure* is composed of several parts, here *Structure Elements*, specified using the “has-structure-element-part” relation in the ontology. There are two main types of Structure Elements, namely the *Structure Component* and relational element named *N-ary Structure Connection*. The *ufo:mediate*s relation specifies the components of which the connection is composed. The *Structure Connection* is a binary connection, a specialization of the N-ary connection, with two mediation relations, *from-structure-component* and *to-structure-component*. Fig. 5b shows the types of structures used in STAMP, i.e. the *Control Structure* and the *Process Structure*. Additionally, the ontology allows to specify the structure of structure elements. This allows describing elements in more detail, if necessary. As a result, this model is capable of capturing different views of the control structure where some control components are viewed in detail while others are not. Finally, Fig. 5c shows the different kinds of components (on the left) and connections (on the right) used to represent the control and the process structures.

STAMP specifies five key kinds of *Control Structure Components*, namely *Controller*, *Process Model*, *Algorithm (part of the Controller)*, *Sensor*, and *Actuator* but the list might be extended if necessary. Furthermore, STAMP specifies three types of connections, represented in the STAMP ontology as *Action Control Connection* (representing control by means of actuators), *Feedback Control Connection* (representing feedback connection with sensors) and *Information Control Connection (r*epresenting coordination and information links between *Controllers)*. A process structure is described in terms of the *Process* components, which can be connected with *Next Connection* (i.e. organized in a flow).

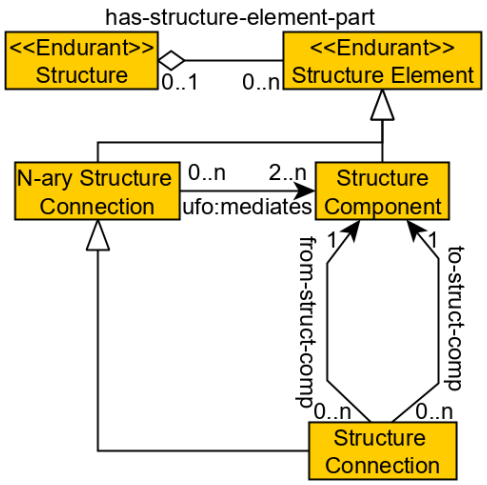


Fig. 5a STAMP Structure Model

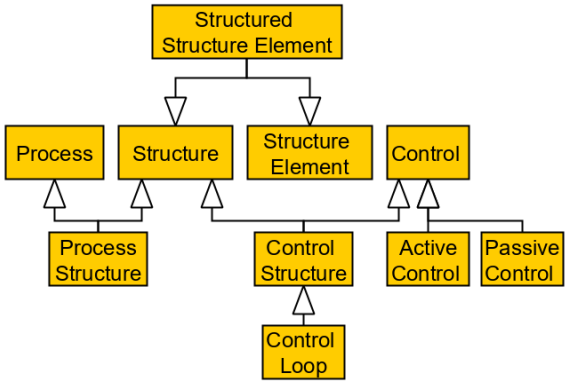


Fig. 5b STAMP Structure Taxonomy

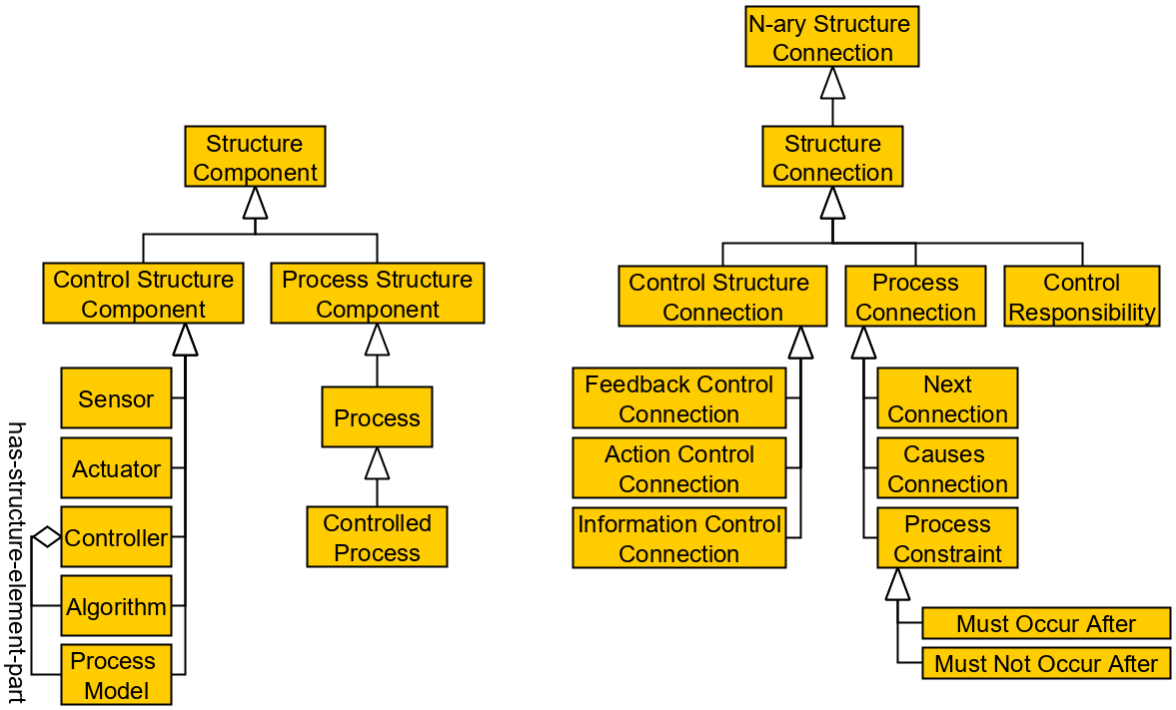


Fig. 5c Structure element taxonomy

The core of the ontology is visually depicted in Fig. 6. The central concept is *Controlled Process*, which usually consists of a task sequence and is described in typical operational documentation. In the context of a UFO ontology, this process is modeled as *Event Type*, where various objects and agents can *participate in*. The objects and agents are commonly modeled by means of *Substantial* concept (orange in Fig. 6). Further, the participant in the *Controlled Process* is a *Control*, which is modeled as specialization of the *Substantial* concept. *Control* is responsible to control certain *Variables* and it is an aggregate of objects and agents as per the theory of STAMP (i.e. organized controllers, sensors, actuators) which may change in time, but retain their identity. *Hazard* is considered as a capability or a property of objects and agents as well as their abilities or functions. However, STAMP defines the term hazard as a state. In the proposed ontology we use the term *Hazardous State* instead for such states to avoid terminology confusion. Hazards in the ontology are modeled as *Dispositions* which *inhere in Endurants* and are *manifested in Unwanted Events*, *violating* existing Safety *Constraints* as per the STAMP theory. Safety constraints are modeled as *Substantials* and their goal is to *mitigate* manifestation of *Hazards* in *Unwanted Events*. This is done by *constraining Variables*, which *describe* different aspects of the *Controlled Process.* Furthermore, *Variables* can be defined in terms of objects and events (not shown in the figure). For example, the variable “distance between the aircraft and a vehicle” can be modeled as a UFO formal relation between objects “aircraft” and “vehicle”. This and other similar ontology patterns aim at better definition of control and grasping quantifiable aspects of controlled processes, which in the context of STAMP theory are utilized as variables in the controlled process and which can be manipulated or measured. *Enforcing* of safety *constraints* is realized by the concept *Control*.

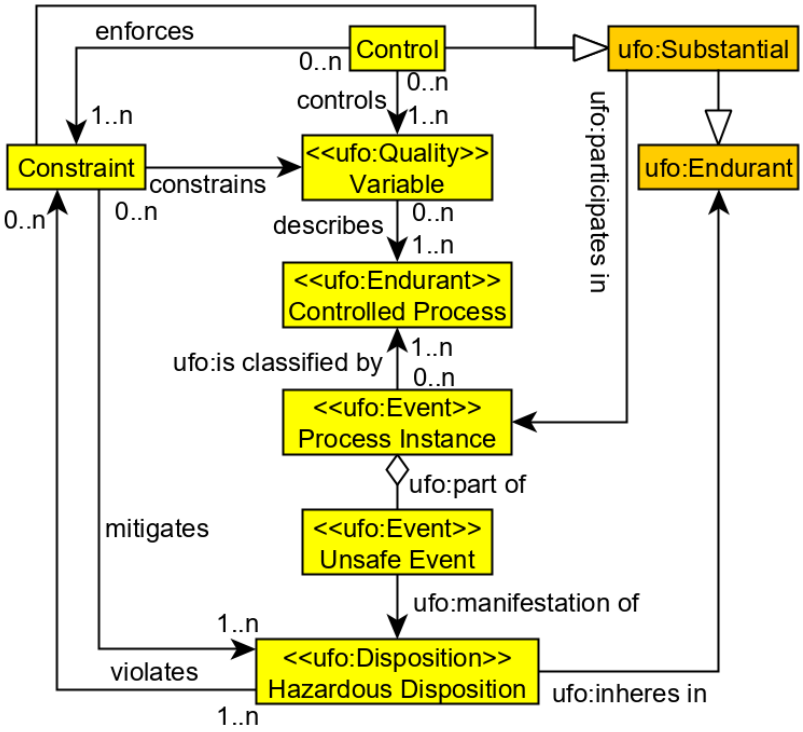


Fig. 6 The core of developed STAMP ontology

The next key part of the published ontology is description of events associated with the *Control Structure Components* from Fig. 5 and the *Controlled Process*, see Fig. 7. For example, a *Control* can be composed of a *Controller* and several *Sensors* and *Actuators*. Furthermore, the *Controlled Process* is modeled as consisting of several parts (events) which are the focus of interest in STAMP theory (hence the class *STAMP Event*) and which can be divided into events related to communication (*Communication Event*), control (*Control Action*), actuation (*Actuating Event*) and measurement (*Sensing Event*). The participants in these events are specified by means of *participates in* relation and also by relation *performs*, which ties the *Controller* with *Control Action*. For illustration and intelligibility, Appendix 1 to this document includes several specific examples about ontology application in the aviation industry.

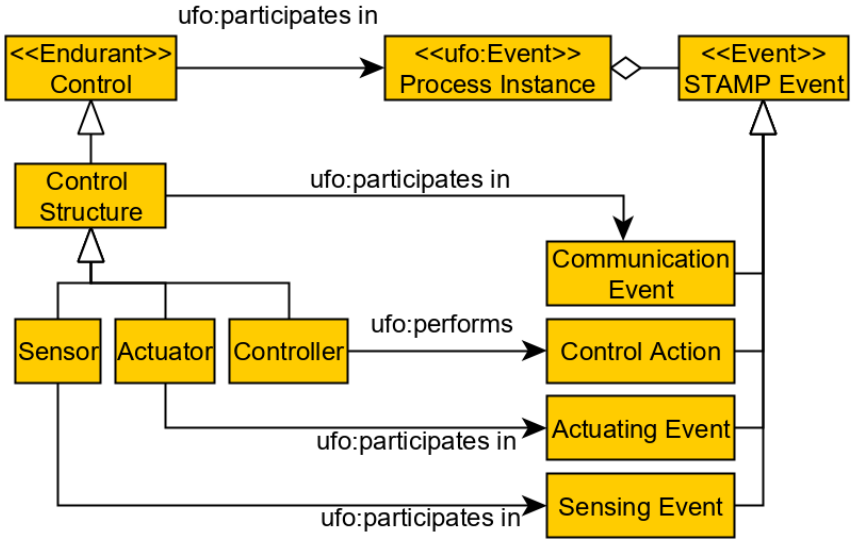


Fig. 7 Key concepts related to control as per the STAMP ontology

The STAMP model describes *Control Actions* and other control structure events such as controller's decision or sensors' operations. The STAMP ontology models this in terms of *Capabilities* (a specialization of the concept *Disposition*). Fig. 8 depicts the schema pattern to associate *Capabilities* with the *Control Structure Elements,* in this case the *Capabilities* of the *Control Connections.* The property used to represent this association is *has capability.* Fig. 9 shows how to specify a particular unsafe capability, the *Unsafe Action Capability* (unsafe control action in STAMP terminology). The schema allows to describe a capability from which the unsafe capability is derived, e.g. "unsafe brake capability" is derived from the "break capability". Also, the schema allows to specify the particular type of the *Unsafe Action Capability* according to STAMP, e.g. action "not provided" and action executed "too early" Furthermore, the schema allows to specify the hazardous state (*Hazardous State Type*) to which the capability potentially leads, the source, i.e. the *Control Component Controller* (e.g. the *Controller* who performed the action) and the *Context* (e.g. the process or activity during which the capability is unsafe).

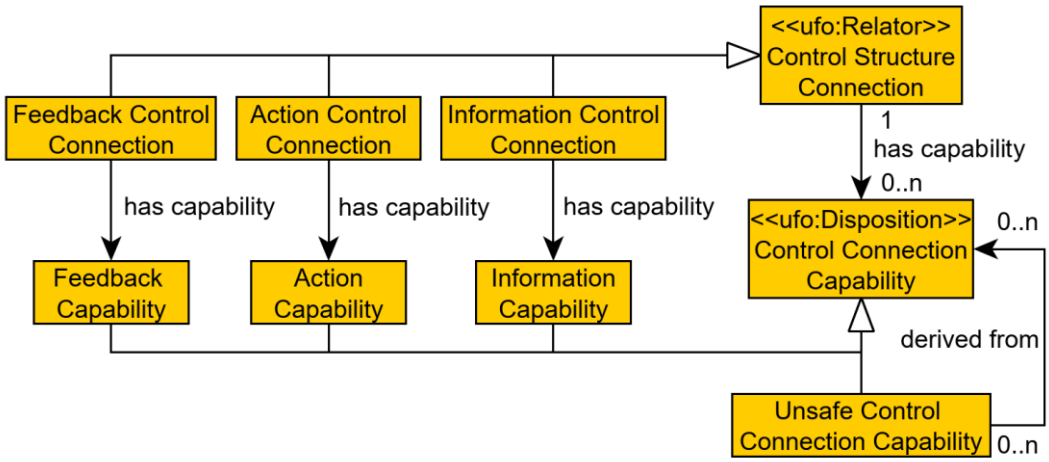


Fig. 8 Specifying *Capabilities* of a *Control Structure*

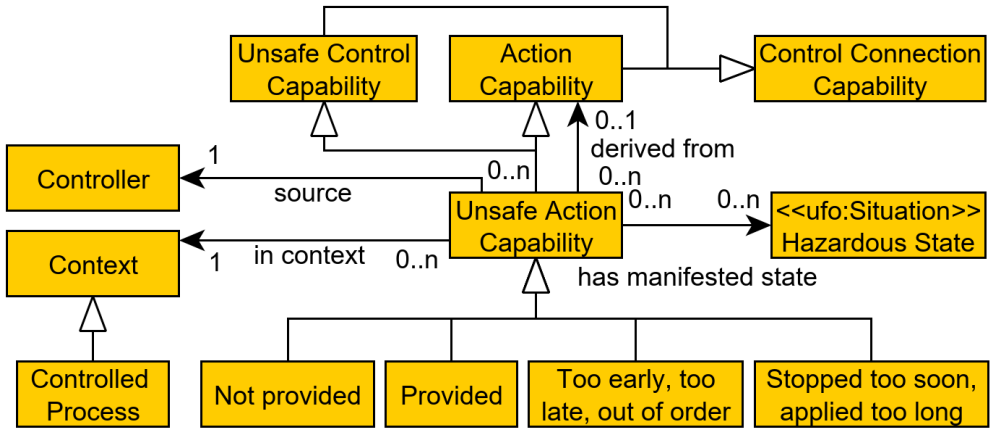


Fig. 9 Schema of *Unsafe Action Capability*

Finally STAMP requires to specify *Control Responsibility*, see Fig. 10. A *Controller* is associated with a *Control Responsibility* via the *has responsibility* relation. The responsibility *has goal* a *State Constraint* and is related to a *Process* by the *has plan* relation. This part explains that a controller is designed to take pre-defined measures with certain conditions

emerging to avoid unwanted events that could lead to a hazard, i.e. the *Controller enforces* the *State Constraint*. *State Constraint* and *Hazard State* reflect the safety constraints and hazards as used with the theory of STAMP.

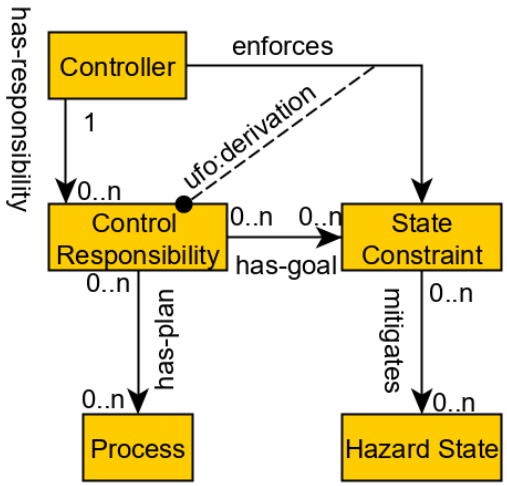


Fig. 10 Schema of *Control Responsibility*

3.3 Application of STAMP ontology

This part of the methodology describes utilization of the developed STAMP ontology in the context of safety data collection and processing.

3.3.1 Basic information about application

The process of ontology application is compatible with the theory of STAMP so as the CAST methodology, however, it brings new technical capabilities for storing data so as how to execute specific steps of the CAST methodology. The basic difference is ontological definition of STAMP theory concepts. This mostly influences the execution of step 3, i.e. documenting the safety control structure in place, which is now limited by the ontology according to its patterns. Because the ontology is machine-readable artefact, it does not require the documentation by means of object-oriented diagrams similar to the one in Fig. 2, even though such representation may be useful in some cases. The ontology allows mainly machine-readable documentation, which is normally stored in RDF (Resource Description Framework) format in a triple store (subject, predicate, object) such as RDF4J.

Realization of the machine-readable documentation of a safety control structure can be performed either directly with the utilization of the published ontology artefact (e.g. in Protégé[2] tool) or by implementation of the ontology into existing software environment used to support safety or documentation management in respective organization. Especially in the latter case there is the opportunity to implement it into an integrated management system, which usually includes several information necessary for STAMP-based analyses and which can be utilized for multiple purposes within a single system. It is especially convenient to use standard

[2] https://protege.stanford.edu

process documentation, if there is one available, because it includes a basic description of processes, their participants so as distribution of responsibility. In case the process documentation is not available electronically, a solution is to utilize available business process modeling tools with the use of BPMN language (such as free open-source tool Modelio[3] or commercially available Adonis[4] or Bizagi Modeler[5] and similar). The created system description is then necessary to complement with additional information according to the published ontology, which produces documentation of safety control structure as per step 3 of CAST methodology and, at the same time, operationally exploitable artefact for normal business management. The only difference is that such safety control structure would be complete and not filtered to the particular accident or safety occurrence. On the other hand, by application of the methodology in combination with business process modeling, a synergy effect is achieved and so a unique opportunity to maintain complete and up-to-date description of a system, compatible with STAMP theory. This way it is possible to significantly simplify and expedite the process of safety data collection and processing based on STAMP. Step 3 of CAST methodology is eventually reduced to simple filtration of existing system description according to the scope of respective safety data processing, i.e. according to the output from steps 1 and 2 of the CAST methodology. Execution of initial steps (1 and 2) of CAST methodology then depends on the way of carrying step 3. If the step 3 is carried in form of integrated solution, then the filtration of existing documentation is performed in all three initial steps. If the STAMP ontology is applied as a stand-alone solution (e.g. with Protégé), then the documentation of safety control structure shall be performed each time safety data are collected and processed, as is usual with STAMP-based methodologies. Due to the mentioned reasons, it is therefore more advantageous to use the first option, i.e. filtration of an already existing artefact.

3.3.2 Ontology application on the CAST methodology

Documentation of the safety control structure as per step 3 of CAST methodology requires definition of control loops, control structure, controlled processes, constraints and all objects and relations, which are mutually connected and relevant to particular accident or safety occurrence. The base of STAMP is a control loop and Fig. 11 depicts an example of single control loop definition in line with the developed STAMP ontology. Specifically, the figure shows a *controller* - driver of conveyor belt vehicle for loading baggage into an aircraft, which controls the process of parking for baggage loading with a *sensor* measuring distance between the vehicle and aircraft. Apart from basic elements of the loop, in the ontology there is also support for definition of *variables*, which are controlled by the *controller* in the *controlled process*, here the distance and orientation between aircraft and vehicle (see Fig. 12). Figs. 13, 14 and 15 provide detailed description of parts of the control loop from Fig. 11 in terms of representing details of connection, objects and events relevant to the loop. Fig. 11 (so as all other figures in this section) are only an attempt to visualize result of data collection and processing by means of UML language, even though recording the data in RDF does not require any visualization. Stereotypes (names of classes in parentheses) correspond to types of objects according to the STAMP ontology.

[3] https://www.modelio.org
[4] https://www.adonis-community.com
[5] https://www.bizagi.com/products/bpm-suite/modeler

After definition and modeling of control loops, it is necessary to determine distribution of control loops with respect to the controlled processes and safety constraints. The distribution is graphically represented in Fig. 16 where *control loops* are tied to specific *controlled processes* (with control-feedback relations) according to the process documentation and their task is to *enforce* specified safety *constraints*. The STAMP ontology provides that each safety *constraint* must be *enforced* by some *control loop*. Example is safety constraint - 1 from Fig. 16 which requires that the parking process of the conveyor belt cannot be initiated without parking coordinator and which is part of baggage loading process, specifically part of control loop CL12-CSP of parking coordinator. Certainly, it is possible and in practice rather usual, that one *control loop enforces* several safety *constraints* and also that one safety *constraint* can be enforced by several *control loops*. From the perspective of safety, however, it is unacceptable if some safety *constraint* is not enforced by any *control loop*.

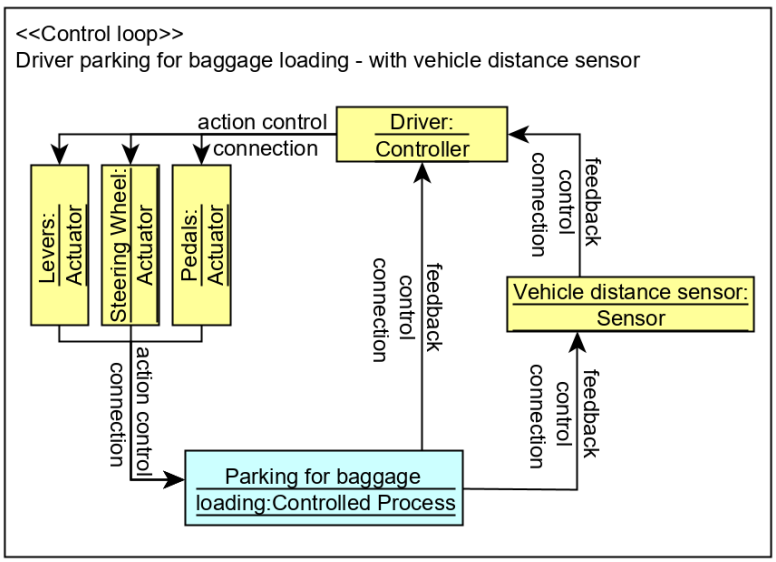


Fig. 11 Example of control loop modeling by means of STAMP ontology

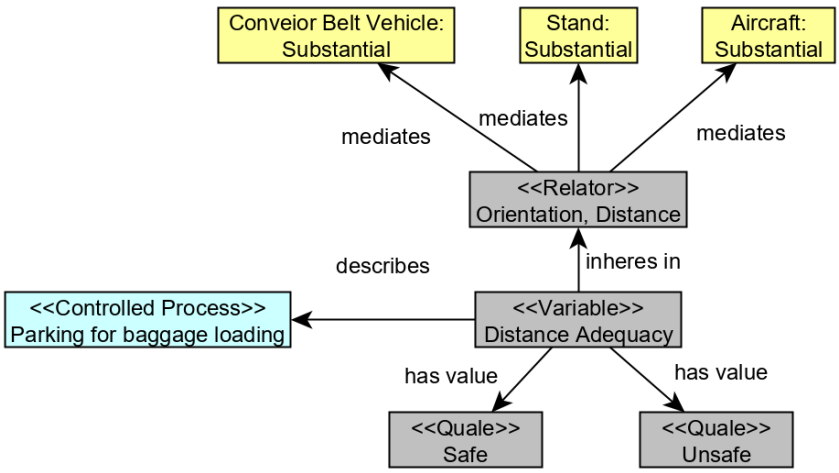


Fig. 12 Specification of control variables used to control the controlled process

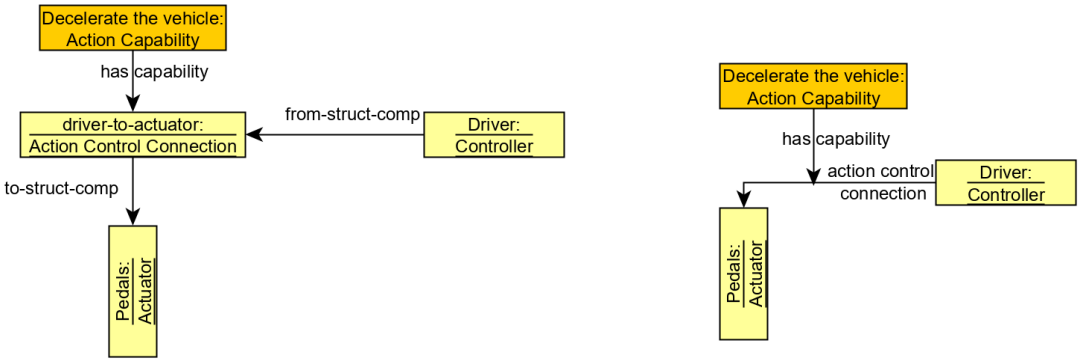


Fig.13 Notation used to represent of connections in the diagrams

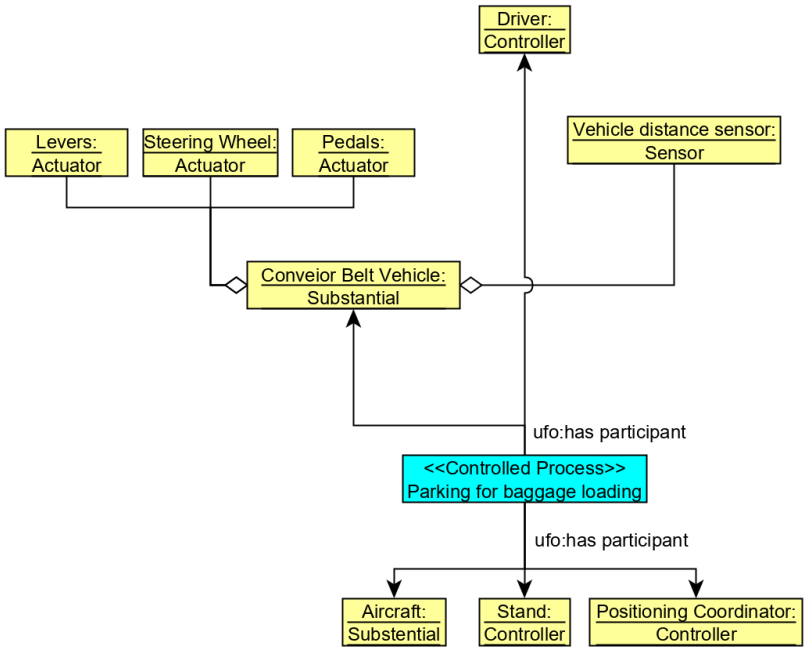


Fig. 14 Detailed specification of the objects referenced in the control loop

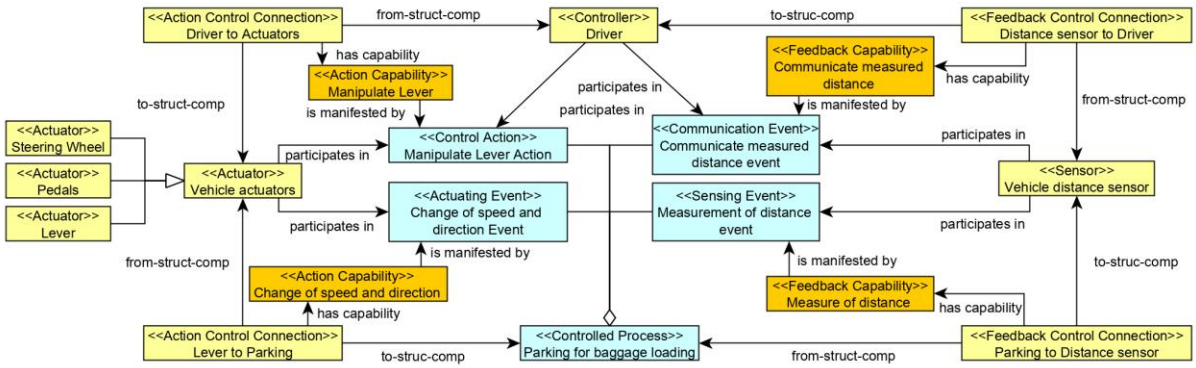


Fig. 15 Detailed specification of the events related to the control loop

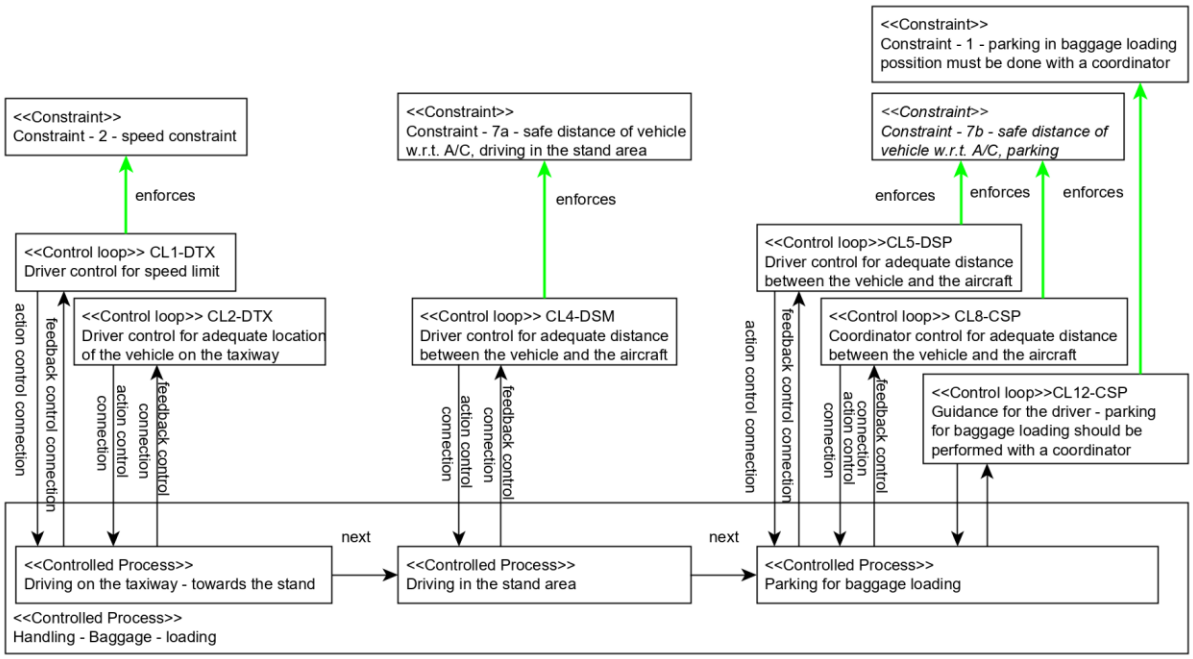


Fig. 16 Modeling of operational processes and their relations with safety constraint by means of STAMP ontology

Steps 4 and 5 of CAST methodology are supported by STAMP ontology in similar way as it is with steps 1, 2 and 3. Here, it is necessary not only to set a chain of events, as it is common with every investigation, but also to map this chain to the established documentation of safety control structure from step 3, i.e. in the context of schemas from Figs. 11-16. Fig. 17 in this respect shows an example of fictional occurrence where a collision occurred between the conveyor belt vehicle for baggage loading and an aircraft. The collision occurred during vehicle parking into position, from which it is possible to load baggage into an aircraft, by means of the conveyor belt. The vehicle driver wrongly estimated relative distance and position of the vehicle with respect to the aircraft and crashed with the conveyor belt into the aircraft fuselage, causing a damage. Contributing factors of this event were approach started without positioning coordinator, no feedback from positioning coordinator, driver's belief about situation not matching reality and inadequate vehicle movement. The event chain is depicted in magenta, documentation of safety control structure in yellow (objects), blue (events) and orange (capabilities), and the accident in red. Relations among magenta/red and orange elements shows mapping of the chain to the system description (documentation of the safety control structure).

After finishing the basic event description according to the example in Fig. 17, it is then necessary to define how and why each individual parts of a system contributed to inadequate control during the event, i.e. to execute step 6 of CAST methodology. In this respect, there are two types of information important and definition of which is required by STAMP ontology: which safety constraints were violated and how these constraints map to the model of processes, i.e. to the safety control structure documented in step 3 of CAST methodology. Fig. 18 shows specification of violated safety constraints according to the STAMP ontology. It is possible to infer mapping of the constraints to the control loops from the already created

documentation, specifically from schema in Fig. 16. When implementing the ontology into software environment, this can be inferred automatically.

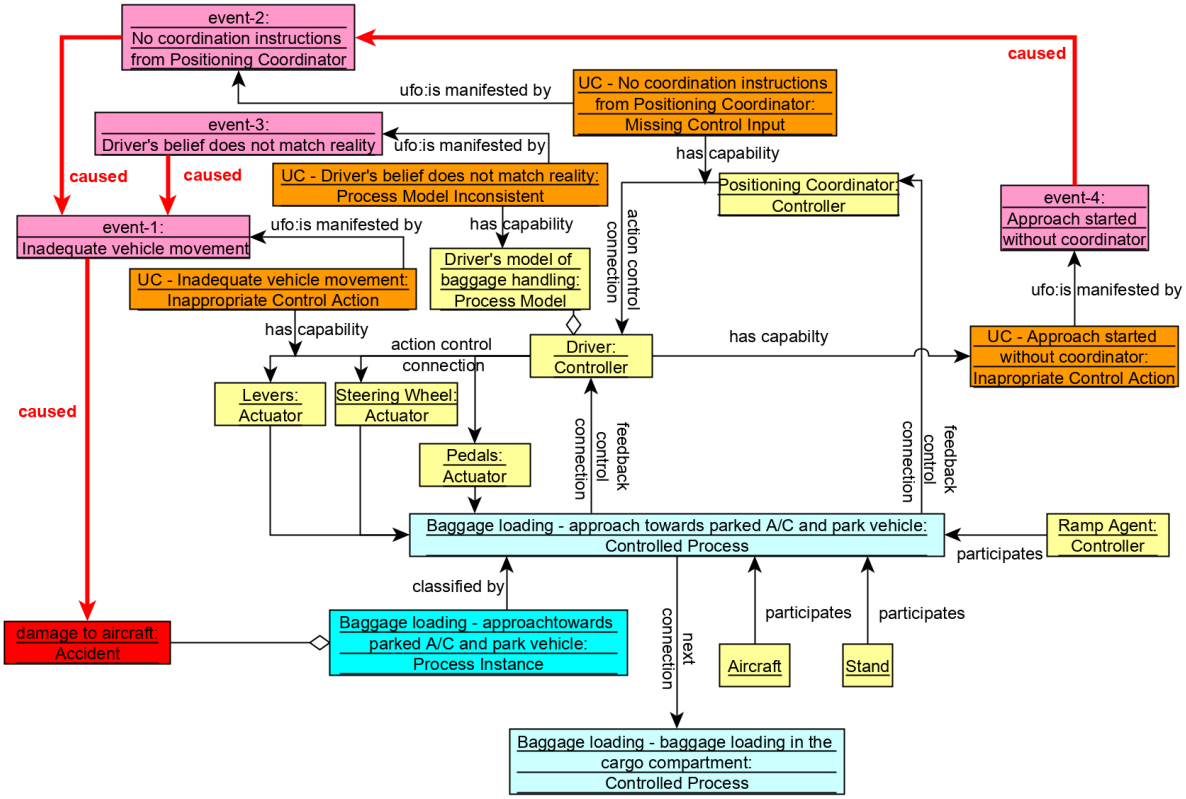


Fig. 17 Modeling of fictional event of aircraft damage during process of vehicle parking by means of STAMP ontology

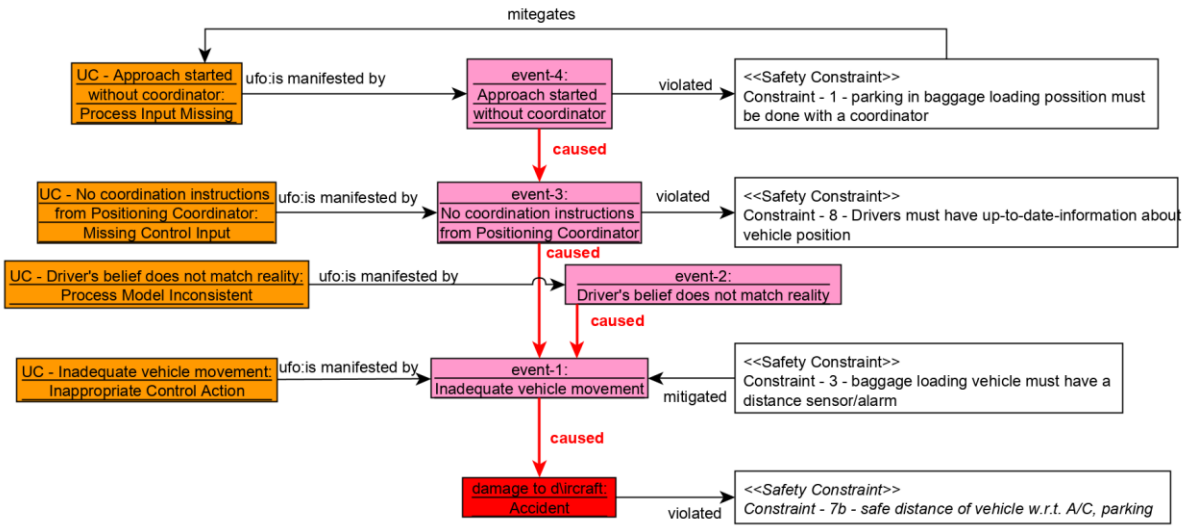


Fig. 18 Modeling of fictional occurrence of damage to aircraft and its mapping to safety constraints by means of STAMP ontology

As is apparent from Fig. 18, STAMP ontology specified the process of data collection and processing. The ontology requires here definition of violation relations between contributory factors of an occurrence and safety constraints. The mentioned example of safety constraint -1 from Fig. 16 is in Fig. 18 violated by specific contributory factor - approach started without coordinator. Even though the example used in this chapter is rather simple and regards only two control loops, the same procedure applies when multi-level hierarchy of control loops would be considered.

3.3.3 Practical recommendations

Performing safety data collection and processing with the utilization of the developed STAMP ontology brings several possibilities for how to facilitate, expedite but simultaneously maintain the advantages of ontology application with respect to supporting the execution of some of the steps of CAST methodology based on STAMP.

First of the possibilities for facilitation is introduction of libraries covering object types, employee roles and similar. Ontology inherently works with types and it is not necessary to specify all the instances. In some cases it may be beneficial to work with instances (e.g. define personal details of individual employees, who are playing different roles in the processes or define identifiers of individual vehicles which are being used in different processes), however, STAMP aims at systemic point of view and so it aims rather at mutual relations, links and arrangement of objects, control loops and similar entities appearing in the processes at more generic (functional rather than particular object-dependent) description. With respect to this, definition of roles and types suffice (e.g. conveyor belt driver, or aircraft, or even fleet etc.) and by establishing a library of all such types, manageable sets of objects are created from which a safety analyst can pick relevant objects during both process definition in the process documentation so as during mapping of events to the documentation.

Another from practical recommendations pertains modeling of complex control, when a higher level of detail is necessary for an analysis. Theory of STAMP admits existence of overlapping control loops but it is rather limited in providing the ways of how to depict details of such control in real conditions. Example of such a situation is depicted in Fig. 19. The example includes the already described control loop of conveyor belt driver from Fig. 11 and, in addition, also detailed description of a control loop of parking coordinator (highlighted in magenta) with the relations among the two control loops. Similarly as for the previous figures, Fig. 19 is an attempt to visualize the situation, even though the main goal would be definition of its content by means of classes and relations in RDF format. In this way, by means of the STAMP ontology, it is possible to document an accurate description of a complex control in desired level of detail, which may not be easily visualizable, and the documentation can be conveniently used for safety data collection and processing.

The last recommendation relates to the possibility of utilizing STAMP taxonomy depicted in Fig. 3. The taxonomy is general and applicable for safety data classification. In the context of STAMP ontology application, this taxonomy can be used in its general form to classify safety occurrences and contributory factors (as used in Fig. 18 in orange boxes). Because the general STAMP taxonomy is mapped to specific objects of a control loop (e.g. inadequate process model maps to controller), by modeling the general taxonomy by means of the

STAMP ontology there is an opportunity to filter the taxonomy per object of interest and so to enable practical pre-defined lists for event classification.

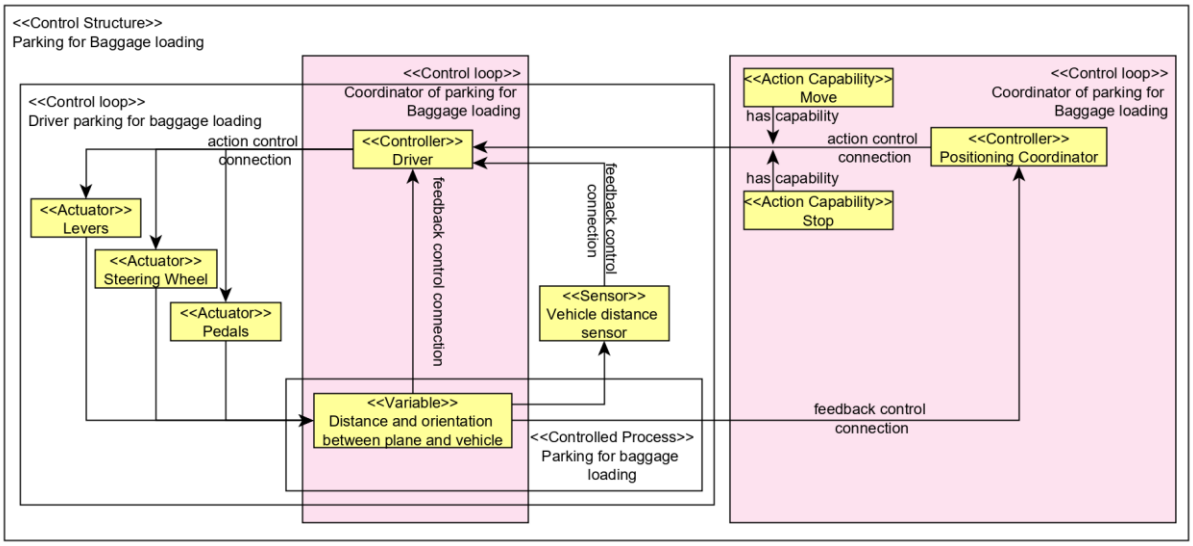


Fig. 19 Modeling of detailed relations between two control loops by means of the STAMP ontology

3.4 Utilization of process documentation and its tools

Process documentation lays down principles and procedures for execution and management of processes and activities in respective organization with the aim to achieve unified and effective control. The documentation is issued in common form and single system and there are rules and responsibilities specified for its creation and management. It specifies binding rules needed for correct functioning of company processes, it describes them, their sequence or connections, including authority and responsibility. Following that, it can be noted that the process documentation is suitable foundation for establishing documentation of a system of interest.

Graphical representation of business processes by means of process diagrams, which is suitable and valid tool for documenting a system, is governed by rules and principles of BPMN. Process diagram is a set of single or multiple interconnected procedures or activities carried in given order. Other external conditions can be also included. The tools available for modeling with BPMN allow integration of all principles described in the previous chapters in a way introduced in this chapter.

Processes of an organization or a company can be divided into three basic groups: main, supporting and control processes. A model of such division provides an overview of a system for analyst. The groups can be further elaborated and detailed to a higher level of resolution because every activity in a process may represent a whole other process at the higher level or resolution. Eventually, every single action within an activity can be described, even though

such resolution is typically not needed. It is very important, however, to record the work as done rather than work as imagined when documenting the processes.

The following figure (Fig. 20) shows a diagram of a basic process. Its elements are start, i.e. beginning of the process activity, individual activities arranged into required structure and interconnected with relations, and finally an end where process activity finishes. The figure shows a process of vehicle parking used in examples from the previous chapters. It specifies two parallel activities as per the responsible person, here the vehicle driver and a positioning coordinator.

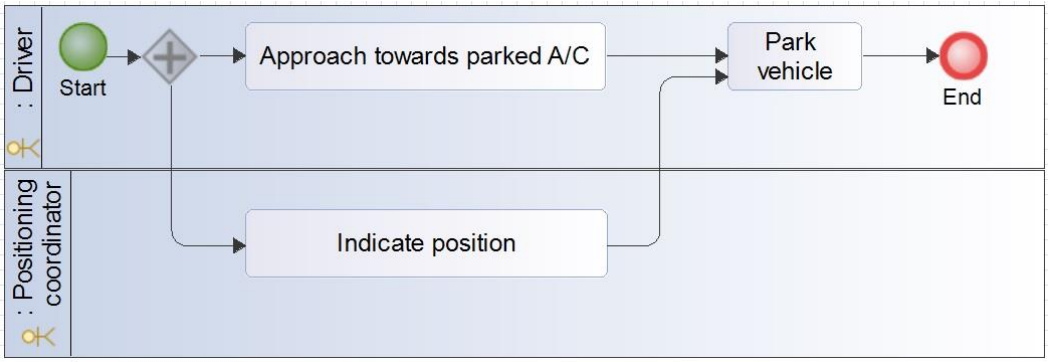


Fig. 20 Example of process diagram according to the BPMN notation produced with Modelio

As can be seen from Fig. 20, the process diagram provides functional documentation of a system, i.e. a documentation of what the system does rather than what it is (from the object-based perspective). This is very useful when applied in the context of CAST methodology execution since it can guide safety analyst to avoid extremely detailed description of a system that could eventually be limited to analysis of failure modes of individual components rather than systemic issues.

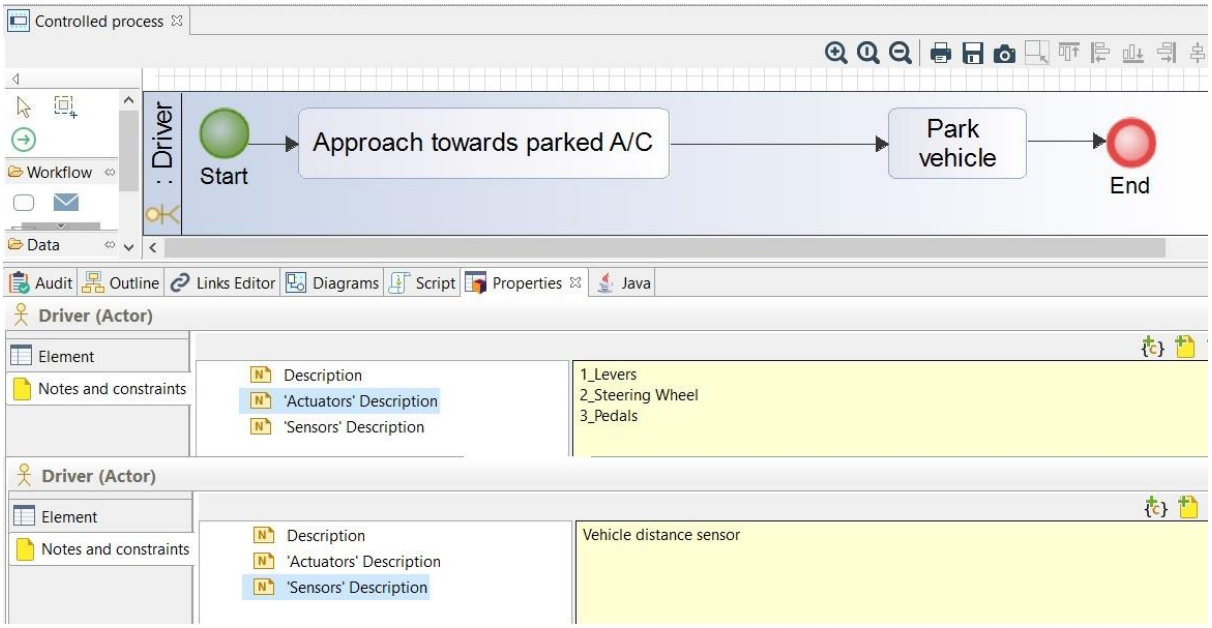
Available tools for process modelling can be used for documentation of a system (safety control structure), as discussed in chapter 3.3.1, since they allow for storing all necessary information to be used with the ontology application. Following subchapters provide some details about how to use the tools for this purpose.

3.4.1 Documentation of a control loop

Control loop according to the feedback control theory and as used by STAMP consists of four basic elements: controller, actuators, sensors and controlled process. In BPMN, a controlled process is every activity arranged in a process diagram. Every activity must have precisely one responsible role assigned as responsible for its execution. From the perspective of STAMP, such role is the controller. The list of actuators and sensors used with the role can be added using attributes of the role. Example of implementation of a control loop description according to feedback control with BPMN is shown in Fig. 21. The figure shows specification of available actuators (‘Actuators’ Description) and sensors (‘Sensors’ Description), namely “1_Levers”, “2_Steering Wheel”, “3_Pedals” as actuators and “Vehicle distance sensor” as sensor. This way it is possible to add part of the information needed for STAMP analysis directly into a process documentation of an aviation organization.

3.4.2 Library of controllers

Roles of the employees who are responsible for individual processes can be displayed in a library of responsible roles. For the purpose of the described methodology, roles are defined by actuators and sensors available to a controller in respective activity. Example of a preview of a library of controllers is shown in Fig. 22. The library shows two roles - namely the vehicle *driver* and *positioning coordinator*. As already mentioned in chapter 3.3.3, establishing a library facilitates process documentation management with regard to provision of the information required by STAMP analysis. It is sufficient to establish library of controllers by means of standard available tools for process modelling, nevertheless depending on the specifics of respective tool it may be useful to consider establishing other libraries, which may facilitate process documentation management in respective cases. Establishing such libraries then follows the same principles as for library of controllers.



Obr. 21 Example of a control loop description with BPMN produced with Modelio

4. Novelty of the methodology

The novelty of the methodology can be defined in two contexts: (a) in comparison with CAST methodology based on the theory of STAMP and (b) in comparison with current industrial standards of aviation safety data collection and processing. The following subsections provide the highlights from both contexts.

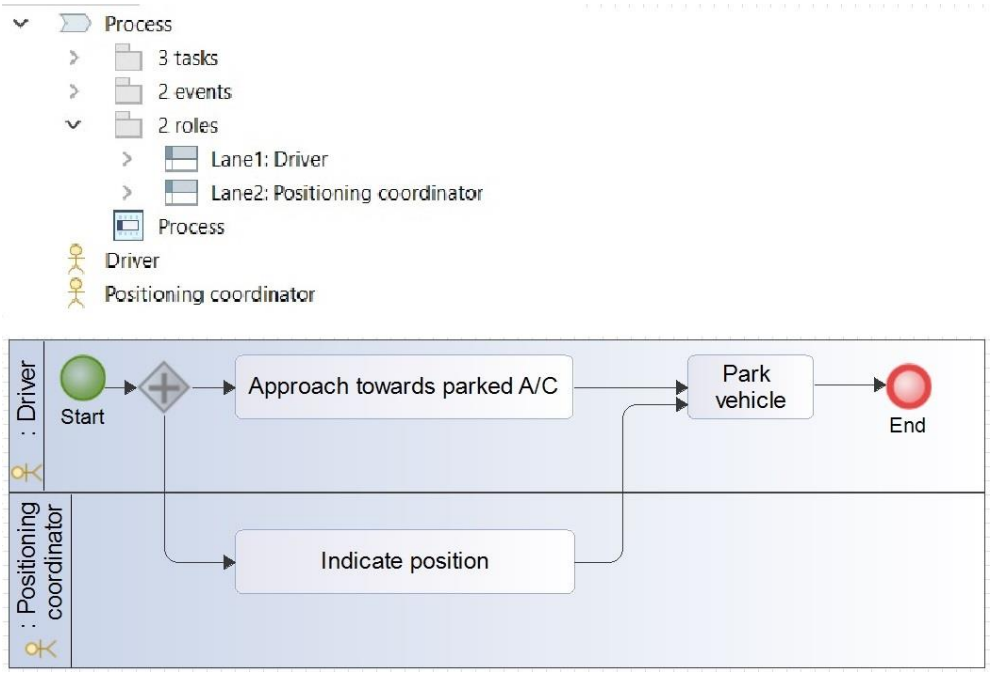


Fig. 22 Example of utilization of library of controllers according to the BPMN notation produced with Modelio

4.1 Comparison with CAST methodology

The methodology already includes direct comparison with CAST methodology based on the theory of STAMP. CAST is founded on the theory of STAMP so is the developed ontology in this methodology. Both methodologies are compatible, however, this document describes new technical possibilities for how to support specific steps of CAST by the developed ontology and how to achieve practically exploitable results in the aviation industry, especially in the context of current safety management standards in the industry. In addition, the application of ontology brings new possibilities for integration of the safety data collection and processing with company and industrial processes, which is out of the scope of CAST. The developed ontology allows for utilization of standard process documentation as a source of necessary information for carrying out safety data collection and processing and, vice versa, it allows for storing data in the context of the very same documentation. Apart from the benefits of the integration, this brings also few other possibilities: (1) CAST methodology can be executed with complete and up-to-date documentation of a system, which produced the data and not only with ad-hoc representation (snapshot) of a safety control structure of interest, which is necessary to be established with every safety analysis; (2) storing safety data in the context of process documentation allows for better and more effective support for identification of problematic parts of a system so as preventive measures, which have the potential to mitigate the problems; (3) in case the ontology modeling technology is applied in other then safety domains, it enables partly automated identification of correlations between safety data and data about quality, reliability, cost-efficiency and similar and consequently the possibility to propose system-level measures in the context of standard process documentation.

4.2 Comparison with aviation industrial standards

In the context of current standards for safety data collection in the aviation industry, the main novelty regards application of the theory of STAMP in the aviation industry and support for carrying out CAST methodology which is now (owing to proposed technical solution) more accessible from the perspective of the systems already in use for safety data collection and processing.

Current industrial standards for these systems are defined by ICAO Doc. 9859 Safety Management Manual, issued by the International Civil Aviation Organization, now in edition 4 from 2018. This document requires aviation organizations and states to establish a system for safety data collection and processing and it lays down principles for which data and how to collect and process. These principles are until today based on SHELL and Reason's model, i.e. based on identification of accidents and incidents with linearly ordered contributory factors, in line with the core ideas of the models. The industry focuses of event classification according to current safety taxonomies available, in the aviation especially the ICAO ADREP taxonomy and in Europe the ECCAIRS taxonomy, or its filtered version known as RIT (Reduced Interface Taxonomy). Safety data collected and processed according to the taxonomies are subjected to analysis by means of safety performance indicators, which are analyzed for trends or correlations with other safety performance indicators. Other processes defined by ICAO with respect to the safety data collection and processing regard data completeness or security and they are not innovated by this methodology.

The novelty with respect to the mentioned industrial standards in the aviation regards the shift in safety model used to explain safety occurrences and safety issues. This methodology uses STAMP prediction model of safety, which aims at system-level assessment of safety and for identification of safety issues at the level of a system as a whole, by means of feedback control theory. This methodology brings key innovations and technical possibilities owing to which it is possible to close the gap between the theory and industrial processes of data collection and processing and so it facilitates application of STAMP in the aviation industry. The methodology guides the user to create safety occurrence records mapped to the documentation of a system, which generated the data, and so it allows for the system-level safety analysis. The goal is not to monitor pre-defined set of safety performance indicators over some time periods, as is the current practice in aviation, but to monitor the behavior of individual parts of a system with analysis focused on which parts of the system or which safety measures are correlated, eventually providing for the understanding of how to effectively manage safety from the perspective of the whole system. In this respect, the methodology with its technical solution based on ontology engineering creates new functionalities, which allow for faster, simpler and more accurate analysis and management of risk in the context of current safety management systems in the aviation.

5. Application of the methodology

This methodology describes the possibility for increasing efficiency and effectiveness of analysis and management of risks by means of conceptual modeling, i.e. by means of the developed STAMP ontology, and based on customized safety data collection and processing. It is dedicated to aviation organizations, which can implement its content into their safety

management systems, and for which it offers technical and methodological solution for integration of standard process documentation activities with safety management. It is possible to apply the methodology in several contexts detailed in the following paragraphs. Even though the methodology is based on innovative solutions, which are not required by any current law of aviation standard in force, it offers potential for improvement in areas where the law and standards aim to govern industrial practice and its application eventually supports meeting the goals of applicable law and standards.

The methodology can be applied in the context Czech aviation standard L19 and ICAO Annex 19 provisions, so as in the context of specific provisions of ICAO Doc. 9859 Safety Management Manual regarding the establishment and management of Safety Data Collection and Processing System - SDCPS.

The methodology can be applied in the context of European legislation regarding the aviation safety data collection and processing, especially in the context of Commission Regulations No. 996/2010, No. 376/2014 and No. 2015/1018.

The methodology can be applied also in the context of EUROCONTROL Safety Regulatory Requirement ESARR2 about safety occurrence reporting by the European Organisation for the Safety of Air Navigation.

6. Economic aspects

Application of the methodology induces several implementation costs. If the methodology is implemented into own custom software solution, then the costs are induced for such implementation. Further, there are costs regarding the training of relevant personnel and update of respective processes in a company. In some cases, it may be needed to increase the number of employees of a safety management unit of respective company, nevertheless such measure is not considered necessary for the methodology implementation. If the methodology is implemented independently from existing software solutions in respective company, especially by means of free available tools, then the implementation costs are reduced but, on the other hand, an opportunity of integrated solution is lost.

Potential economic benefits cannot be precisely quantified, but these are primarily related to the improvement of safety management processes, namely with increased effectiveness and efficiency of the safety management system. Effective safety management brings improvement in financial health of a company, because it leads to less safety occurrences in the operations and the occurrences can be better anticipated, i.e. adequate resources can be planned for potential remedy in advance [14]. Standalone economic opportunity is the realization of integrated solution, which offers the potential for limitation of the workload of safety management employees in the context of safety data collection and processing. It also improves the capability of identifying system-level opportunities for improvement of respective company operations and so to increase the capability of a company to adequately allocate resources to priority issues from the perspective of maintaining its safe and efficient operations.

References

[1] Gabbar, H. A. *The design of a practical enterprise safety management system*. Dordrecht: Kluwer Academic Publishers, 2004. ISBN 9781402029493.

[2] Stolzer, A. J. and Goglia, J. J. *Safety management systems in aviation*. Second edition. Burlington, VT: Ashgate, 2015. ISBN 978-1472431783.

[3] Dekker, S. *Drift into failure: from hunting broken components to understanding complex systems*. Burlington, VT: Ashgate Pub., 2011. ISBN 978-1409422211.

[4] International Civil Aviation Organization (ICAO). Safety Management Manual (SMM): Doc 9859 AN/474. Fourth Edition. Montréal, 2018. ISBN 978-92-9249-214-4.

[5] Regulation (EU) No 376/2014 of the European Parliament and of the Council on the reporting, analysis and follow-up of occurrences in civil aviation. Brussels: Official Journal of the European Union, 2014, L122/18.

[6] Reason, J. T. *Managing the risks of organizational accidents*. Brookfield, Vt., USA: Ashgate, 1997. ISBN 978-1840141054.

[7] Grant, E., Salomon, P. M., Stevens, N.J., Goode, N. and Read, G.J. Back to the future: What do accident causation models tell us about accident prediction?. *Safety Science*. 2018, 104, 99-109. DOI: 10.1016/j.ssci.2017.12.018. ISSN 09257535.

[8] Leveson, N. Engineering a safer world: systems thinking applied to safety. Cambridge, Mass.: MIT Press, 2011. Engineering systems. ISBN 978-0-262-01662-9.

[9] Hollnagel, E. *FRAM, the functional resonance analysis method: modelling complex socio-technical systems*. Burlington, VT: Ashgate, 2012. ISBN 978-1409445517.

[10] Hitzler, P., Gangemi, A., Janowicz, K., Krisnadhi, A. and Presutti, V. *Ontology engineering with ontology design patterns: foundations and applications*. Amsterdam, Netherlands: IOS Press. Studies on the Semantic Web, v. 025. ISBN 978-1614996750.

[11] Doyle, J. C., Francis, B.A. and Tannenbaum, A. *Feedback control theory*. Mineola, N.Y.: Dover, 2009. ISBN 978-0486469331.

[12] International Civil Aviation Organization (ICAO). Annex 13 to the Convention on International Civil Aviation. Eleventh Edition. Montréal, 2016. ISBN 978-92-9249-968-6.

[13] Guizzardi, G. and Wagner, G. Using the Unified Foundational Ontology (UFO) as a Foundation for General Conceptual Modeling Languages. Poli, R., Healy, M. a Kameas, A. ed. *Theory and Applications of Ontology: Computer Applications*. Dordrecht: Springer Netherlands, 2010, 2010-8-12, s. 175-196. DOI: 10.1007/978-90-481-8847-5_8. ISBN 978-90-481-8846-8.

[14] Lališ, A., Červená, V., Stojić, S. and Kraus J. Methodology for Justification of Aviation Safety Investments. In: *2018 XIII International Scientific Conference - New Trends in Aviation Development (NTAD)*. IEEE, 2018, 2018, s. 87-90. DOI: 10.1109/NTAD.2018.8551627. ISBN 978-1-5386-7918-0.

List of publications preceding the methodology

Kostov, B., Ahmad, J. and Křemen P. Towards Ontology-Based Safety Information Management in the Aviation Industry. Ciuciu, I., Debruyne Ch., Panetto, Weichhart, H. G., Bollen, P., Fensel, A. and Vidal, M.-E., ed. *On the Move to Meaningful Internet Systems: OTM 2016 Workshops*. Cham: Springer International Publishing, 2017, 2017-03-29, s. 242-251. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-55961-2_25. ISBN 978-3-319-55960-5.

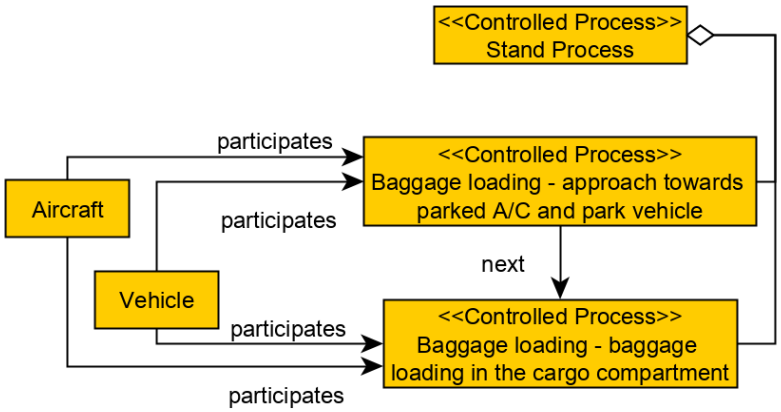
Křemen, P., Kostov, B., Blaško, M., Ahmad J., Plos, V., Lališ, A., Stojić, S. and Vittek P. Ontological Foundations of European Coordination Centre for Accident and Incident Reporting Systems. *Journal of Aerospace Information Systems*. 2017, 14(5), 279-292. DOI: 10.2514/1.I010441. ISSN 2327-3097.

Ledvinka, M., Lališ, A. and Křemen, P. Toward Data-Driven Safety: An Ontology-Based Information System. *Journal of Aerospace Information Systems*. 2019, 16(1), 22-36. DOI: 10.2514/1.I010622. ISSN 2327-3097.

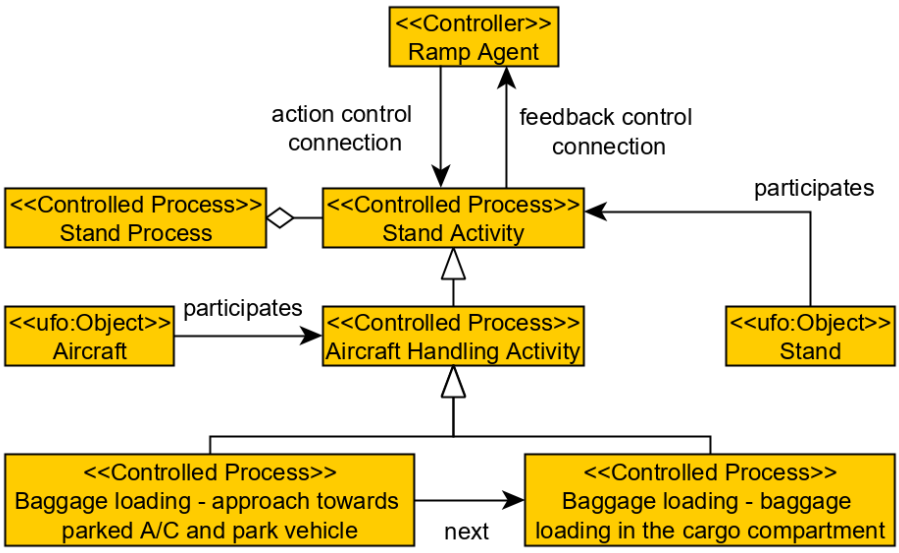
Saeeda, L. Iterative Approach for Information Extraction and Ontology Learning from Textual Aviation Safety Reports. Blomqvist, E., Maynard, D., Gangemi, A., Hoekstra, R., Hitzler, P. a Hartig, O. ed. *The Semantic Web*. Cham: Springer International Publishing, 2017, 2017-05-07, s. 236-245. Lecture Notes in Computer Science. DOI: 10.1007/978-3-319-58451-5_18. ISBN 978-3-319-58450-8.

Underwood, P., Waterson, P. and Braithwaite, G. 'Accident investigation in the wild' – A small-scale, field-based evaluation of the STAMP method for accident analysis. *Safety Science*. 2016, 82, 129-143. DOI: 10.1016/j.ssci.2015.08.014. ISSN 09257535.

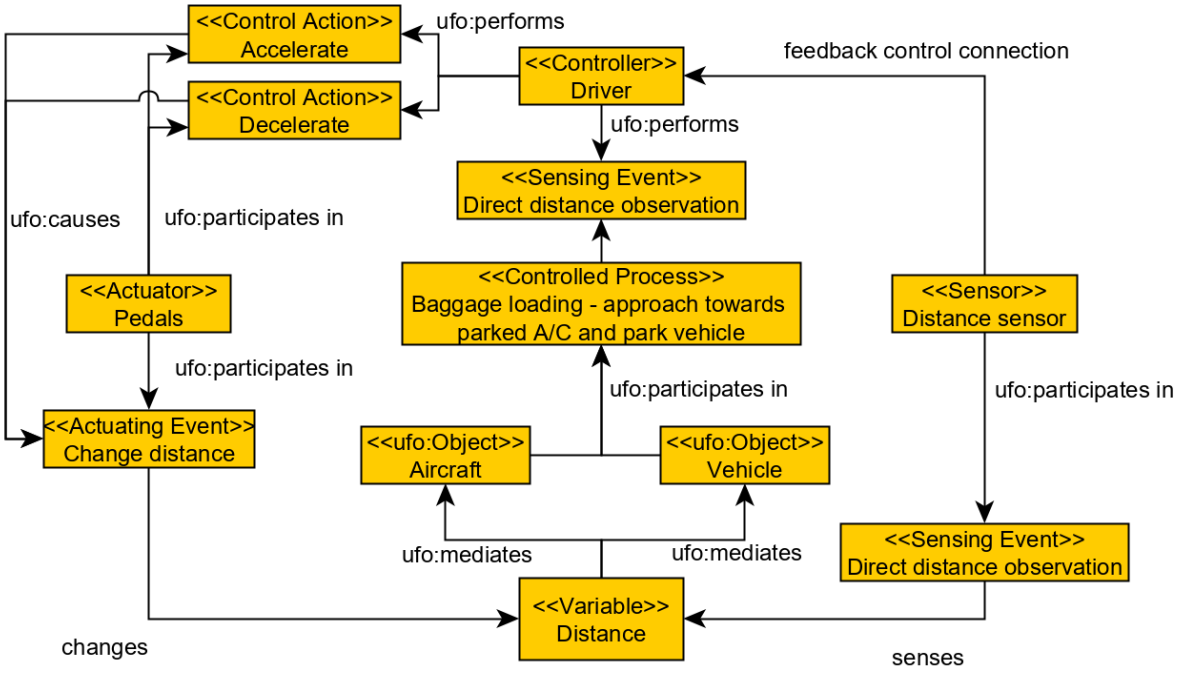
Appendix 1: Examples of STAMP ontology application on industrial situations from the domain of airports



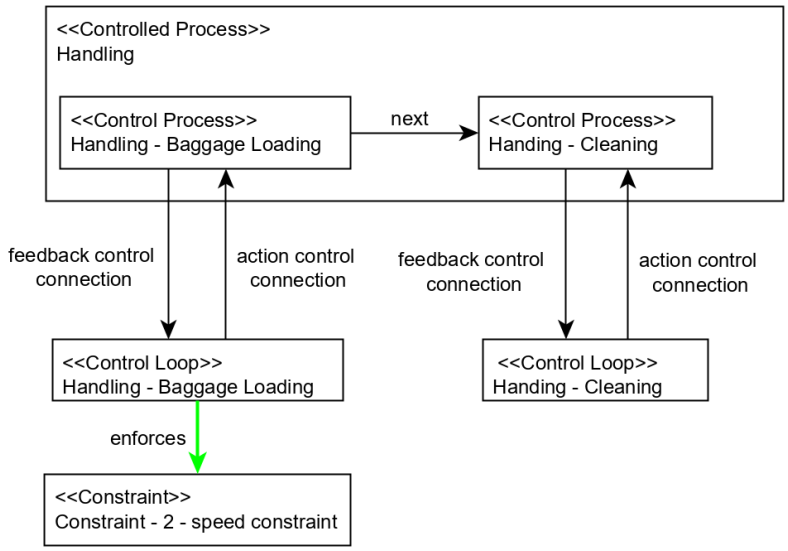
P1: Description of a baggage loading process during ground handling of an aircraft



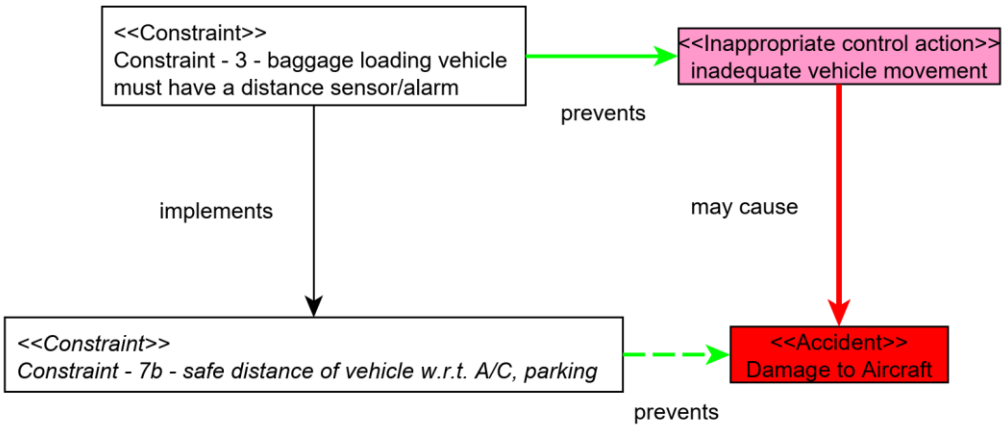
P2: Specification of participants and relations of feedback/control in the context of describing aircraft baggage loading process



P3: Modeling of control and events related to the conveyor belt driver



P4: Modeling of relations between safety controlled process, safety control structure and safety constraints in the context of aircraft ground handling



P5: Modeling the relations between safety constraints in the context of unwanted events they are designed to prevent