MATEC Web of Conferences **273**, 02011 (2019) https://doi.org/10.1051/matecconf/201927302011
*ICSC-ESWC 2018*

# Challenges in Future Mathematical Modelling of Hierarchical Functional Safety Control Structures within STAMP Safety Model

**Liran Bar Or[1,3,*], Shai Arogeti[2] and Daniel Hartmann[1]**
[1] Management & Safety Engineering Unit, Engineering Faculty, Ben-Gurion University, Israel
[2] Department of Mechanical Engineering, Engineering Faculty, Ben-Gurion University, Israel
[3] NRC-Negev, Israel

## ABSTRACT

In the STAMP model, based on control theory, the control relationships between various system elements enforced by the closed Control Loops (CLs) are logical and functional. A literature survey emphasized the fact that for the moment STAMP and its main tools STPA and CAST are not associated with any numerical tools. The main rationale of our work is to understand whether STAMP matches to be a quantitative model. Furthermore, in a case that we find that numerical tools can be used in STAMP, we intend to bridge the gap between the logical-functional approach in STAMP and any of the suitable quantitative approaches applied in Engineering Control Theory (ECT). As a first step, a literature comparison was performed between the basic control parameters existing explicitly at the moment in the STAMP model, and those well known in the literature of ECT. The results reveal that there are many similar terms, especially related to conceptual and general definitions. However, we have observed that there are also basic quantitative parameters from ECT which are not yet referred to in STAMP as quantitative safety evaluation parameters. Another main finding is an inherent difference in various ECT related parameters and the CLs at the various hierarchical levels. ECT was originally developed to deal with physical systems. Thus, any machine related internal control loops within the lower-physical level of a Sociotechnical System (STS) can be directly addressed with quantitative methods from ECT. However, most of the human-machine interactions in the lower levels and the human and societal controls in the higher levels are at the moment not suitable for those methods. We assume these ECT parameters may have an important role in designing and examining systems safety and hence we suggest, should be integrated into STAMP model, in purpose to be able to enhance systems safety.

**Keywords:** Engineering Control Theory; Closed-loop Control; Mathematical Modelling; Control Theory Parameters.

## 1. INTRODUCTION

The System-Theoretic Accident Model and Processes (STAMP), being a systems safety model, is dealing with the entire system responsible for providing safety, namely a Sociotechnical System (STS). According to STAMP (Leveson, 2004, 2012), the architecture of a STS describes the most important functional characteristics of the elements and the structure of the relationship among the elements. Basic fundamentals of STAMP model for the safety of STSs are Hierarchical Functional Safety Control Structure (HFSCS) and Safety Constraints (Leveson, 2004, 2012). According to the STAMP model, loss events and accidents occur when safety constraints are not enforced successfully in the control structure, leading to Unsafe Control Actions (UCAs). From an

* Corresponding author: lbaror@yahoo.com

engineering point of view, those safety constraints can vary from physical and tangible ones such as physical safety barriers in a machine or personal protective equipment; up to abstract and intangible constraints as legislation and regulations ("risky actions performances are prohibited") and decision making. STAMP refers to the enforcement control action within the entire system as the cause of the emerged systems safety and not to the actual performance action.

In the STAMP model, based on control theory, the control relationships between various system elements are logical and functional. According to Leveson (2004, 2012) real systems and STSs, are not static and have a dynamic nature and tendency to drift and change over time. This dynamic behaviour of the systems and its controllability in the time domain can lead to several engineering challenges about the proper way to cope theoretically and practically with the mentioned changes (linear and nonlinear). At the moment, the behaviour of the Control Loops (CLs) in STAMP model is logic and therefore the safety level of the system cannot be dealt with advanced engineering tools, and cannot be simulated and evaluated by quantitative means at a specific systems state, let alone about changing systems.

### 1.1. Problem Statement

STAMP has been developed to achieve systems safety within existing and operating systems or in systems undergoing initiation or development. The System-Theoretic Process Analysis (STPA), a theoretical hazard management tool, has been developed to establish detailed verbal safety requirements for those systems by looking at theoretical accidents and unsafe control actions (Leveson, 2012); and in addition, the Causal Analysis using Systems Theory (CAST), an accident investigation tool, was developed to deal verbally with actual loss events (Leveson, 2012). We find that there is a gap between the present qualitative STAMP model and its logical and verbal tools STPA and CAST, and the quantitative approaches, theories, and practices in the engineering domain. As others have already done (Abdulkhaleq & Wagner, 2013; Abdulkhaleq et al., 2015; Chatzimichailidou at el., 2016; Dulac et al., 2005; Li et al., 2017; Rejzek et al., 2018), we continue the search for integrating into STAMP and its methods a quantitative approach, related to control engineering.

### 1.2. Research Objectives

The main objective of this research is threefold. First, we aim to understand the above-mentioned gap by comparing the explicit and implicit statements in the vast STAMP literature regarding control engineering and their variables and parameters embedded in STPA and CAST. Second, we study those control engineering parameters that were not integrated until now in the model and its tools and examine their applicability for systems safety. The final stage would be to understand which of the quantitative approaches in control engineering and which methods best suit to be integrated into STAMP and its methods. It is necessary to clarify our view of "quantitative approaches". Our intention is to use numerical tools applied in Engineering Control Theory (ECT) to simulate and evaluate the safety control loops mathematically. Be it on a narrower level (just one subsystem and its control loops), or on a broader level of the entire HFSCS. Our approach is not in any way an attempt to transfer STAMP into a numerical probabilistic safety tool.

### 1.3. Contribution

We suggest using a broader control engineering approach to enhance the already highly developed STPA logical and verbal tools (Leveson and Thomas, 2018). We present some of the main findings of the above-mentioned phase one and two at the system level, as well as at the various main hierarchical levels. We show that it is critical that the already embedded control variables in STAMP should be treated differently at any given hierarchical level. In addition, we present some new control variables that are not yet used by STAMP and STPA and have potential, when used, to increase our understanding of systems safety and can help create more system safety

requirements. The last phase of examining the quantitative control engineering tools is still under investigation and will probably demand more interactions with STAMP community.

## 2. BACKGROUND

### 2.1. STAMP and Engineering Control Theory (ECT)

STAMP, following control theory, implies that the minimal safety unit in a STS or any other system must include at least two elements: a performing element where a hazardous process takes place and an enforcement element to keep it in a safe state. It also implies that the enforcement element must be aware of the performing element actions and their quality and to have the ability to change them dynamically, if necessary. In ECT terms (Dorf & Bishop, 2011; Ogata, 2010), the structure of a control loop in closed form emerges, resulting in that the enforcement element gets feedback on the hazardous process state and conditions.

Leveson (2004), further, by integrating the ECT concept of CLs in closed form, introduced in STAMP a new safety paradigm that top-down, every hierarchy level must impose safety constraints on the activity of the level beneath it to control its systems safety-related behaviour (Leveson, 2004, 2012). These features suit the enforcement – performing interactions, as described above. The hierarchical control structure must enforce top-down throughout the entire system the function "provide safety" and thus in STAMP we refer to safety as systems emergent property (Leveson, 2012). Later on, this view of the system was named by Sgueglia (2015) as a Hierarchical Functional Safety Control Structure (HFSCS). A scheme of a minimal basic structure of a safety control loop and its interactions is shown in Figure 1. It can be seen that any higher enforcement level, named N+1 level, imposes top-down safety goals, policies, constraints, and commands on the level beneath it containing the potential hazardous processes (N level) and receives a feedback which consists of various measurable parameters from the N level operational experience, results, measurements and reports.

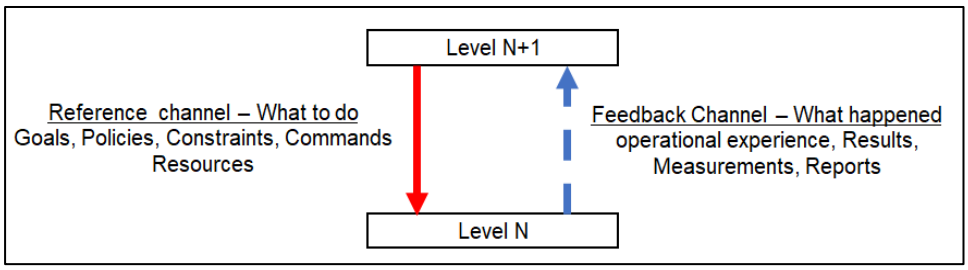


Figure 1: Interactions between enforcement and performing bodies (after Leveson, 2004, 2012)

In the STAMP model safety is an emergent property of the system. It means, on abstract terms, that the theoretical system's safety can only be assumed, a priori, if the method STPA is implied from the concept and early design stages, or a posteriori, if an operating system is analysed with STPA or in a case of an accident, with the CAST method, and then with STPA. At the moment only in a case that systems safety, related to the entire HFSCS, is being analysed with appropriate methods, namely STPA or CAST, the emergent property can be qualitatively assumed. Thus, for the moment, only implying the verbal and logical method of STPA seemingly guaranty theoretical systems safety, if performed in a perfect way. However, from the field of critical safety systems (e.g., aviation, space, nuclear power, car industry, pharma, and medical treatment) it is well accepted that even after a thorough theoretical hazard and risk management phase starting at concept, early design and prototype built, some severe phases of physical and simulation testing is needed to expose various unsafe control actions hidden in the concept, design or in the performance of the target system (Delsart, 2016; Thomas & Vidal, 2017 and Bradley, 2006). Since STAMP paradigms are based on ECT and system's architecture of HFSCS, it seems that it would be most suitable to

suggest numerical analysis tools used in ECT to analyse, simulate and examine the performance of the CLs. ECT is a well-established knowledge field which contributed for decades to the design, manufacturing, and operation of almost every modern machine which are physical-technical systems, from water kettle and microwave oven to smartphones and satellites in space. Its main purpose is to bring a system (be it mechanical, electromechanical or hardware-software integrated systems) from an initial state to the desired state in required time and to keep its desired state even when certain unplanned events occur. Since those principles correlate with STAMP safety paradigm, it is obvious that if tools from ECT will be implemented within the STAMP model, system safety can be determined less ambiguously in quantitative terms. Moreover, system safety can be examined quantitatively with different hypothetical scenarios, and the results can be useful to regulators, management and design decision making.

### 2.2. Basic Control Principles in ECT

Control System (CS) is a kind of a dynamic system which uses system model, algorithms, resources and feedbacks to govern the actual system behaviour by sensing its state, comparison to the desired state, calculating the error and needed improvement action, and performing it according to a predefined algorithm. Figure 2 shows a basic generic structure of CS with its sub-elements and the relation between them. A basic and generic STAMP safety control structure is based on it (Leveson, 2004, 2012) and has similar components as a controller, an actuator, a process, and sensors. We argue that at the moment, one of the fundamental differences between ECT and STAMP is the absence in STAMP of a quantitative variable called error, a variable in a CL that constantly measures the gap between the actual and the desired states of the controlled process to the desired state (the circle shape component in Figure 2). In ECT, according to a predetermined gap value by design, related to the error variable, the controller is acting correspondingly to bring back the controlled system to its desired state. For the moment, STAMP recognizes theoretically only two systems states, namely safe or not safe. In addition, it should be noted that it is accepted in ECT that in most real cases, measurement output is not identical to actual output, although both are located on the feedback channel. This happens because sensor measurement changes the output due to various types of measurements noises, and the controller must take the quality of the signal into account while deciding the desired response.

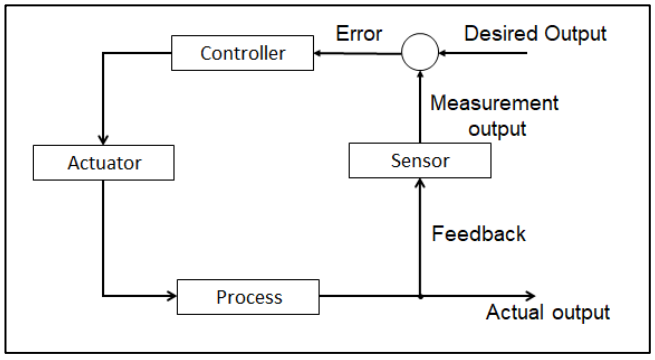


Figure 2: Basic structure of a control system (after Dorf & Bishop, 2011)

In the ECT theoretical and practical fields, the algorithms which control the controlled process are mathematical (e.g., mathematical functions with a state variable). This variable is the controlled input and the mathematical function describes its quantitative behaviour upon different states and conditions, which can be defined by several parameters, and its main purpose is to ensure that the system stays between defined quantitative boundaries.

In engineering, dealing with a physical system (e.g., hydraulic, chemical, mechanical and electrical systems) the use of mathematical functions to study the dynamics of a system in a quantitative way is expected. Hence in engineering, these tools are commonly used for optimization

of various systems parameters at the lower, machine-based level of HFSCS (i.e. the physical level). However, for the higher STS's levels, encompassing human-machine and human-human controls, Vinciarelli et al. (2015) state "However, modelling, analysis, and synthesis of human behaviour are far from being solved problems". Thus, mathematical description, due to inherent problematics, is much less used on human-machine or human-societal systems, which constitute the main levels in STSs, including management, organization, regulation, and legislation levels. Probably because societal systems are complex and have many not yet well-quantified parameters that define the controlled input state. Since control algorithms in ECT must use mathematical functions, we address the research question and ask whether it is possible to use mathematical modelling in STAMP for every control loop in an HFSCS. In case there are differences in the ability to describe the various control loops mathematically in the various hierarchical levels, the limitations for the user should be clearly identified. One of our research goals is to search for the suitable and necessary mathematical approach or hybrid approaches to connect between ECT and STAMP model. Preliminary suggestions for mathematical methods that appear to be suitable for this challenge were found and should be examined in this manner in future research.

## 3. RELATED WORK

Several past research tried enhancing STAMP, STPA and CAST by using qualitative and quantitative methods related to ECT. Abdulkhaleq & Wagner (2013) and Abdulkhaleq et al. (2015) examined the integration of Finite State Machine (FSM) while performing STPA Step 1 in purpose to represent the relation between the process model variables, control actions, and hazards. The concept in FSM is that the system is assembled from well-defined and discrete states and it is a tool which describes the behaviour of a system while passing between those states. FSM is widely used in the field of engineering discrete control since it allows analysing the system with quantitative means. However, in the mentioned research FSM was used to perform a hazard analysis process without any mathematical implementation (Abdulkhaleq & Wagner, 2013; and Abdulkhaleq et al., 2015).

Li et al. (2017) noted that the FSM method does not suit systems with multiple controllers and suggest to extended STPA model while using Hybrid Dynamic Theory (HDT). In this field, systems are analysed as a combination of finite state machines where every state has a time-dependent behaviour function. Their extension enables to understand changes over time. Although HDT has the ability to investigate safety upon system structure, the method was used as well just to enhance the STPA step 1 process qualitatively (Li et al., 2017).

Chatzimichailidou at el. (2016) developed a methodology called RiskSOAP which examines the safety state of a system. The methodology is based on a comparison between desired safety state to current state, which are being represented by binary vectors, and according to them, the gap between those states can determine the systems safety state. Although this methodology can produce quantitative results, it does not investigate the systems architecture and its influence on system safety and its reactions upon different scenarios.

Dulac et al. (2005) and Leveson (2012) examined the behaviour of a complex engineering system within STSs by using System Dynamics (SD) models. SD has three basic control loops: reinforcing loop, balancing loop and delay loop and various interactions of those control loops can describe almost any dynamic system. Hence it seems to be suitable for STAMP. Dulac et al. (2005) used SD to understand factors involved in the Columbia space shuttle accident and also performed a risk analysis of a new working group in NASA. Hypothetical scenarios were examined with SD, and the system behaviour was monitored upon those scenarios. Although SD enables to understand system behaviour, especially organizational behaviour, it does not yet directly connect to HFSCS, and it is impossible to conclude about the systems architecture from the results. Another research to examined HFSCS was performed by Rejzek et al. (2018). HFSCSs with multiple levels of abstractions were investigated, and their results showed the importance of parent-child relations in the feedback channel.

We conclude at this stage, according to reviewing past published research, that STAMP as an engineering model and its tools STPA and CAST lacks at the moment a quantitative methodology that defines the STS safety level from its HFSCS. Hence, the main goal of this research is to identify and develop such an approach and tool, which can improve the quantitative safety of systems.

## 4. COMPARISON BETWEEN ECT AND STAMP

The first and preliminary step to achieve our goal was a comparison between the basic implicit and explicit control parameters at the moment in the STAMP model, and those not mentioned yet, however well-known and successfully used in the ECT literature. As mentioned above, the first step in the research is to understand whether STAMP matches to be a quantitative model. Hence, a literature comparison was made between the basic control definitions and parameters which are well known in the literature of ECT to those existing now in the STAMP model. The comparison was done by characterizing and understanding ECT basic parameters and concepts, taken from control engineering textbooks (Astrom & Murray, 2010; Dorf & Bishop, 2011; Haugen, 2010; Ogata, 2010), and finding any references about those parameters and concepts in the STAMP model literature (mainly Leveson, 2012 and Leveson and Thomas, 2018). The main purpose of this process is to locate similar parameters or to find parameters which are currently not mentioned in STAMP literature and represent knowledge gaps between ECT and STAMP. Practically, the comparison was performed in two stages. The first stage compared between basic definitions and general concepts, with the desire to understand whether STAMP control variables are similar to those existing in ECT.

Upon finding similar terminology and concepts in both models, the next stage was to perform a second comparison which compared possible evaluative parameters. The parameters were chosen as they represent a) basic concepts that may be applicable for any control system, b) concepts which are important to safety and c) can be modelled mathematically. The results of the first stage comparison are presented in Tables 1 and 2 representing the findings of the second stage.

Table 1 Comparison between basic definitions and concepts of ECT and STAMP

| Basic definitions and concepts | ECT | STAMP | Similar/ Different |
|---|---|---|---|
| System | "A system is a combination of components that act together and perform a certain objective" (Ogata, 2010) | Interrelated components that are kept in a state of dynamic equilibrium (Leveson, 2012) | Similar |
| Controlled Variable | "The quantity or condition that is measured and controlled" (Ogata, 2010) | Variables which are being manipulated in order to keep the process within predefined limits (Leveson, 2012) | Similar |
| Control | "The ability to correcting the system behavior so that specifications for this behavior are satisfied" (Haugen, 2010) | Knowledge of process state and adequate response (Implicitly in (Leveson, 2012)) | Similar |
| Disturbances | "A signal that tends to adversely affect the value of the output of a system" (Ogata, 2010) | An external event which influences upon the system and may cause accidents (Leveson, 2012) | Similar |
| Feedback Control | "An operation that, in the presence of disturbances, tends to reduce the difference between the output of a system and some reference input and does so | An action which tends to reduce the gap between an actual state to a desired state (Implicitly in (Leveson, 2012)) | Similar |

| Basic definitions and concepts | ECT | STAMP | Similar/ Different |
|---|---|---|---|
| | on the basis of this difference" (Ogata, 2010) | | |
| Closed Loop Control | A system with a measurement of the output signal and a comparison with the desired output to generate an error signal that is applied to the actuator uncertainty (Ogata, 2010) | An open system which contains Interrelated components that are kept in a state of dynamic equilibrium by feedback loops (Leveson, 2012) | Similar |
| Basic Components | Controller, Process, Sensor, Filter (Haugen, 2010) | Controller, Actuator, Controlled Process, Sensor (Leveson, 2012) | Similar |
| Top Level Purpose | Diminish Uncertainties in the system (not only safety) in order to achieve robustness | Diminish uncertainties in the system in order to achieve safety (Implicitly in Leveson, 2012) | Partially similar |
| Open Loop Control | "The output has no effect on the control action" (Ogata, 2010). An open loop system is highly sensitive to uncertainty (not only safety ) | Not mentioned since feedback is crucial property in the model. An open loop system is being considered as an inherently non safe system. | Partially similar |
| Feed Forward | "The control variable adjustment is not error-based. Instead it is based on knowledge about the process in the form of a mathematical model of the process and knowledge about or measurements of the process disturbances" (Haugen, 2010) | Not mentioned since these could be instructions and constraints transferred to lower hierarchy, that is not based on feedback but on a priori knowledge. | Different |
| Examination Tools of feedback system | 1. Stability<br>2. Time domain performances<br>3. Frequency domain performances<br>4. Structural properties | 1. Executing STPA Process<br>2. Comparison with other risk analysis models | Different |

Table 2 Evaluative control parameters

| Parameter | ECT | STAMP | Similar/ Different |
|---|---|---|---|
| Time Constant | "The (quantitative) time interval necessary for a system to change from one state to another by a specified percentage" (Dorf & Bishop, 2011) | Delays in qualitative responding to manipulated variables (Leveson, 2012) | Partially similar |
| Time Delay | "A (quantitative) time delay, T, so that events occurring at time t at one point in the system occur at another | Control loop qualitative respond time (Leveson, 2012) | Partially similar |

| Parameter | ECT | STAMP | Similar/ Different |
|---|---|---|---|
| | point in the system at a later time t + T" (Dorf & Bishop, 2011) | | |
| Stability | "A dynamic system with a bounded response to a bounded input" (Dorf & Bishop, 2011) | Not mentioned explicitly as a system control parameter. However, system stability is related to qualitative system safety | Partially similar |
| Instability | "The tendency of the system to depart from the equilibrium condition when initially displaced" (Dorf & Bishop, 2011) | Not mentioned explicitly as a system control parameter. However, the non-stable system tends to accidents, hence related to qualitative system safety. | Partially similar |
| Error | "The difference between the desired output and the actual output" (Dorf & Bishop, 2011) | RiskSOAP (Chatzimichailidou at el, 2016) calculates the difference between the desired state and the actual state | The concept is similar, the implementation is limited |
| Robustness | "Exhibits the desired performance despite the presence of significant process uncertainty" (Dorf & Bishop, 2011) | Mentioned as an undefined qualitative parameter for communication channel (Leveson, 2012). Not related to the whole control system | Different |
| Sensitivity | "The ratio of the change in the system function to the change of a process or a parameter for a small change" (Dorf & Bishop, 2011) | Not mentioned as a system control parameter | Different |
| Overshoot | The maximum peak value of the response from the desired response of the system (Ogata, 1987) | Not mentioned as a system control parameter | Different |
| Noises | Sensor measurements uncertainty (Astrom & Murray, 2010) | Not mentioned as a system control parameter | Different |
| Hysteresis | "The effect that a system not only depends on its current state but also on its past. That is because of the character of the relation between input and output" (Boersma, 2012) | Not mentioned as a system control parameter | Different |

It can be seen from Table 1 that although there are several different definitions between the two models, many general definitions and concepts are similar. The meaning of the results is that on its basic level STAMP matches well with the variables suitable for the quantitative approach as used in ECT. Table 2 shows that there are control parameters from ECT which are not explicitly referred in STAMP as safety evaluation parameters and those which are referred to have only qualitative significance.

## 5. PARAMETERS IN STAMP WHICH CAN BE IMPLEMENTED WITH ECT TOOLS

We claim that several added values can be achieved by integrating and using ECT principles and its quantitative tools in the STAMP model and are worth mentioning. Error, as described above (Figure 2, and Table 2), is one of the basic quantitative parameters from ECT field which is not mentioned explicitly as such in the STAMP model. It is obvious that the ability to determine numerically exactly to the extent possible the gap or error (with respect within a system or its control loops to the desired state) is necessary for expressing quantitative safety state, and can enhance the logical descriptive power of STAMP model. Stability is another basic parameter in ECT and describes a linear system that its natural response decreases to zero in infinite time. The significance of this parameter is that a stable system can recover fast from external disturbance and can continue functioning without significant damage. Such a parameter would be most important for those systems that are obliged or want to perform business continuity plans (Olson, & Anderson, 2016). Foreknowledge about system stability, especially when supported by numerical values can prevent event loss, particularly in open-loop non-stable processes systems.

The detectability parameter, which refers to the ability to detect system state from the measured output, is also important to systems safety and can point upon areas in the system where the sensors do not function as expected or there exist potential conflicts between sensors outputs. Another important parameter is robustness, which refers to the ability of a system to achieve its required state under uncertainties of input values. These are examples of several basic parameters in ECT that may play a significant role in achieving systems safety by using the STAMP model. We claim that many HFSCS safety-related properties can be determined not only logically and qualitatively, but by numerical analysis upon them and produce quantitative information suitable for decision makers, managers and systems designers.

Another part of the study was to identify parameters in the STAMP model which have a crucial role in systems safety and can be treated further by ECT tools. These parameters were recognized while developing the model as open issues that should be considered in system design and operation (Leveson, 2012), but practical tools were not added yet. As part of the STAMP model, those parameters are for the moment logical and do not have any quantitative expression. Since they are important to safety, it is obvious that numerical methods to evaluate those parameters and their influence on the control structure will enhance systems safety.

Our view is that the main control parameters in the model are four folded: communication channels, time lags, time delays, and timing. Communication channels are the actual means where the data and information transfer between components within a control loop. Those channels are presented schematically in figure 1. The flow of information includes algorithms such as instructions and guidance from a higher level to lower level and feedback to a higher level. It should be noticed that there is a great difference between those parameters in control loops within a system that is just a machine, to those in a human-machine system and to those in a pure human or societal system.
To implement adaptive control to achieve a safe system, effective communication channels are required. The main question is how to define and measure and quantify their effectiveness. Johnson (2017) examined coordination between decision units, which is an aspect of communication channels. The research method was using STPA and CAST performing on chosen test cases and comparison of the logical, verbal outcomes to official qualitative reports related to the same cases. His research strengthened the importance of effective coordination within an HFSCS but did not use any mathematical functions nor quantitative results to evaluate the effectiveness of the communication channels. We suggest that ECT parameters, especially detectably, can be a suitable quantitative solution for this issue. Time lags are also a major challenge in evaluating safety control loops. They are being caused since action times are different within and between different hierarchical levels and can vary between many decades at upper levels, to Nano or microseconds depending on the specific control loop at the machine level. It means that inherently in STSs most of the time data and information flow to higher levels does not suit the actual state in the lower and physical levels or even within one level.

Therefore, it is crucial to distinguish between inherent or ordinary time lags and time mismatch, to unsafe control actions resulting in various timing problems. Time lags can appear between and within low levels control loops (Leveson, 2012) and also in relation to legislation, regulation and higher-level decisions making as well. Inherent time lags can lead to time delays, which is the inherent system response time. Sometimes, especially at upper systems levels, STSs have a significant difference in time delays between its internal levels, which cause the appearance as being an open control loop system behaviour, although in reality and at the right inherent long-time domain possess a closed-loop structure. Obviously, such a complex control structure appears inherently less safe compared to the safety of a less complex system as any machine, or a special machine as an aeroplane operated by a highly qualified person. As shown in Table 2, a time delay is an actual and crucial parameter in ECT; hence there are quantitative means to control it. Time lags are not direct references in Table 1, but as a preliminary conclusion from these studies, it seems that this issue can be treated while using Hybrid system control tools (a similar approach to the one mentioned in Li et al., 2017).

The timing of control actions is, however, a critical issue in the STAMP model, especially in STPA. Basic action in STPA Step 1 is to examine qualitatively and verbally the timing of a control action within a control loop, e.g. executed “too soon” or “too late” (Leveson & Thomas, 2018). This relative verbal analysis might be suitable while performing theoretical hazard analysis for a specific control loop. We suggest that the examination of the timing of the numerous control loops related to different hierarchical levels within the entire STS requires a different engineering approach. While low hierarchy levels control loops work in relatively fast time constants (Nano- to milliseconds, seconds up to minutes and hours), high hierarchy levels control loops operate in much slower time constants (days, years, decades and centuries). For example, control loops of computer act in milliseconds and even faster, while legislation and regulation control loops can receive their feedback many years after the command action. Leveson (2012) referred to this difference within control loops as time lags and focused on the technological mismatch coordination between the different levels. From our point of view, the technological mismatch between hierarchical levels results from the inherent difference in timings and working times of each control loop. This differentiation is an inherent STSs property that should be considered while modelling it. Basically, any lower hierarchy that is much faster than the higher hierarchy can be model as a FSM within the hybrid model of the higher hierarchy. In this way, the steady stats of the fast dynamics are being considered, while the quick change is neglected. However, a deeper examination of these topics should be done in the future.

## 6. DISCUSSION, CONCLUSIONS AND FUTURE WORK

Basic elements of the STAMP model for the safety of STSs are safety constraints and HFSCS. According to the model, loss events and accidents occur when safety constraints are not enforced successfully within all CLs of the HFSCS. In STAMP model the control relationships between various system elements are logical and functional and are expressed verbally. Thus, from an engineering point of view and for the moment, any numerical quality of the entire HFSCS and the safety level of a system analysed by STAMP and its tool STPA, cannot be evaluated by quantitative means at a specific systems state.

The paper suggests adopting, developing and implementing quantitative analysis tools from ECT field. ECT is a well-established knowledge field which contributed to the design, manufacturing, and operation of almost every modern physical-technical and hardware-software system. The first step is to understand whether STAMP matches to be a quantitative model. Hence, a literature comparison was made between the basic control parameters existing now in the STAMP model, and those well known in the literature of ECT. Our research results clearly show that there are many similar terms, especially related to conceptual and general definitions. However, we have observed that there are also many basic parameters from ECT which are not yet referred to in STAMP as safety evaluation parameters. It can be concluded from the results that although on its basic level the control structure in STAMP has similar outlines as an ECT control structure, it doesn’t have at

the moment practical quantitative parameters which can perform in a numerical evaluation process of the safety control structure. We suggest that the main reason for this gap is the difficulty and the complexity of numerical modelling of the HFSCS in STSs which contains not only the physical machine level but also human-machine and human-human interactions levels and high levels as legislation and regulation. Efforts to bridge this gap have been put in recent years, as mentioned in the background chapter, and we believe that additional future research can bridge it, at least for several parameters.

The paper also suggests using quantitative ECT tools for qualitative parameters in STAMP model that were recognized while developing the model as open issues that should be considered in system design and operation and have a crucial role to safety. The parameters are communication channels, time lags, time delays, timing, and resources. Preliminary quantitative ECT methods as Finite State Machine and Hybrid Dynamic Theory were suggested to treat with these parameters. In general, it can be seen, even at this preliminary research stage, that ECT has tools to treat quantitatively many STAMP qualitative parameters and additional ECT tools can be turn out to be suitable in a deeper examination. It strengthens our suggestion that ECT approach is suitable for implementation in STAMP and STSs safety can be enhanced.

A mathematical description is hardly used on human-machine or human-societal systems, which constitute the main levels in STSs, including management, organization, regulation, and legislation levels. To bridge the gap between STAMP and ECT, the main challenge is to develop a mathematical description of human-machine and human-societal systems. Our approach for the next step of our future work is to define several simplified control loops which contain human-machine interactions, and the research goal will be to model them mathematically. Generally, in STSs, human-machine interactions are located on higher levels than the lower physical level. Achieving this goal may bring closer the ability for entire STS quantitative modelling.

## REFERENCES

Abdulkhaleq, A. & Wagner, S. (2013). Integrating State Machine Analysis with System-Theoretic Process Analysis. *Software Engineering (Workshop).*

Abdulkhaleq, A. Wagner, S. & Leveson N.G., (2015). A comprehensive safety engineering approach for software intensive systems based on STPA. *Procedia Engineering, 128*, 2–11. DOI: 10.1016/j.proeng.2015.11.498

Astrom, K.J. & Murray, R.M. (2010). *Feedback Systems*. 2nd edition. Princeton University, New Jersey, USA: Princeton University Press.

Boersma, J.H. (2012). *Controller Design of LTI Systems Subject to Hysteresis*. (Master's thesis, University of Twente, Netherland). Retrieved from https://www.utwente.nl

Bradley, P. (2006). The History of Simulation in Medical Education and Possible Future Directions. *Medical Education*,40(3), 254–262. DOI: 10.1111/j.1365-2929.2006.02394.x

Chatzimichailidou, M.M. Karanikas, N. & Dokas, I. (2016). Measuring Safety through the distance between System State with the RiskSOAP Indicator. *Journal of Safety Studies, 2(2).* DOI: 10.5296/jss.v2i2.10436

Delsart, D., Portemont, G., Waimer, M. (2016). Crash Testing of a CFRP Commercial Aircraft Subcargo Fuselage Section. Procedia Structural Integrity, 2, pp. 2198-2205. DOI: 10.1016/j.prostr.2016.06.275

Ding, S.X. (2008). *Model-based Fault Diagnosis Techniques*. Berlin, Germany: Springer

Dorf R.C & Bishop R.H. (2011). *Modern Control Systems*. 12th edition. New Jersey, USA: Pearson

Dulac, N. *Leveson, N.G. Zipkin, D. Friedenthal, S, Cutcher-Gershenfeld, J. Carrol, J. & Barrett, B.* (2005). *Using system dynamics for safety and risk management in complex engineering systems*. Proceedings of the 2005 winter simulation conference, Orlando, FL, USA. DOI: 10.1109/WSC.2005.1574392

Haugen, F. (2010). *Basic Dynamics and Control*. Retrieved from https://home.usn.no

Johnson, E. (2017). *Theoretic Safety Analyses Extended for Coordination*. (Doctoral dissertation ת MMassachusetts Institute of Technology). Retrieved from https://psas.scripts.mit.edu

Leveson, N.G. & Thomas, J. (2018). *STPA Handbook*. Retrieved from https://psas.scripts.mit.edu

Leveson, N.G. (2004). A New Accident Model for Engineering Safer Systems, *Safety Science, 42(4)*, 237-270. DOI: 10.1016/S0925-7535(03)00047-X

Leveson, N.G. (2012). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA, USA: MIT Press.

Li, Z. Zhong, D. Sun & R. Wang, H. (2017). *Extend STPA Method using Hybrid Dynamic Theory*. 4th International Conference on Dependable Systems and their Applications, Beijing, China. DOI: 10.1109/DSA.2017.30

Ogata, K. (1987). *Discrete-time control systems*. New Jersey, USA: Prentice-Hall.

Ogata, K. (2010), *Modern Control Engineering*. 5th edition. New Jersey, USA: Pearson.

Olson, A., & Anderson, J. (2016). Resiliency scoring for business continuity plans. *Journal of Business Continuity & Emergency Planning*, 10(1), pp. 31–43.

Rejzek, M. Bjornsdottir, S.H. & Krauss, S.S. (2018). Modelling multiple of abstraction in Hierarchical Control Structures. *International Journal of Safety Science*, 2(1), pp 94-103. DOI:10.24900/ijss/020194103.2018.0301

Sgueglia, J. (2015), *Managing Design Changes using Safety-Guided Design for a Safety Critical Automotive System* (Master's thesis). MIT, MA, USA

Thomas R.W. & Vidal J.M. (2017). *Toward detecting accidents with already available passive traffic information*. IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC), pp. 1–4. DOI:10.1109/CCWC.2017.7868428

Vinciarelli, A. Esposito, E. Andre, F. Bonin, M. Chetouani, J. F. Cohn, M. Cristani, F. Fuhrmann, E. Gilmartin, Z. Hammal et al. (2015) Open challenges in modelling, analysis and synthesis of human behaviour in human–human and human–machine interactions. *Cognitive Computation, 7(4)*, 397–413. DOI: 10.1007/s12559-015-9326-z