2021 MIT STAMP Workshop

Workshop Schedule

The workshop will be held virtually from 11am-1pm EDT each day on June 21-30, 2021.

All times below are Boston Time (EDT).

Legend
Tutorial
Interesting Uses Spotlight
Regular Presentation
Lightning Talk
Panel Session

Monday, June 21

11:00-11:20	**Welcome, Introduction, and New Developments**
11:20-12:40	**Tutorial: Identifying Leading Indicators** *Nancy Leveson (MIT)*
12:40-01:00	**Open Discussion**

Tuesday, June 22

11:00-11:05	**Workshop Overview**
11:05-11:10	**A Sensor Architecture View of the System Control Loop** *Kristin Nelson-Patel (Akamai Technologies)*
11:10-12:40	**Tutorial: Enhancing Human Factors Analysis** *John Thomas (MIT)*
12:40-12:55	**Security Policy** *William Young (US Air Force)*
12:55-01:00	**Open Discussion**

Wednesday, June 23

11:00-11:05	**Workshop Overview**
11:05-11:10	**Safety-Guided Design: Integrating STPA into the Systems Engineering Process for the Safety of Remote Health Workers**

	Ashley Brooks (Imperial College London), Prof. Washington Ochieng (Imperial College London)
11:10-11:30	**Introducing STAMP to a major health organisation** *Wallace Grimmett (MATER)* The aim of this presentation is to outline why a large health care organization chose a Safety 3 approach for a re-organization of Quality and safety Department. Partly it was serendipity; the state health department was issuing guidelines Clinical Incident Guidelines for directors and executive of private hospitals, while its own staff struggled with the practicalities of the same guidelines. Concurrently a major private health organisation was looking at revamping its quality and safety processes. Into this mix STAMP has obvious appeal. It has utility. It is easy communicate it's principles and much of the existing process can be preserved.
11:40-12:00	**Effectiveness of CAST, 5M and HFACS in Accident Investigation and Prevention** *KAEFER Guenter (Austrian Air Force), KOGLBAUER Ioana (Graz University of Technology, Austria)* A re-investigation of a helicopter accident, originally investigated after the 5M-model, shows the broader approach and better effectiveness of CAST compared to 5M. An additional HFACS overlay to the results of the 5M and CAST analysis clearly points out the narrow, "front-line-workers"-oriented approach of 5M an the systemic, management-oriented approach of CAST. Simplification and reductionism by 5M seems to be better suited for short-term, "in the field" risk assessments. For an accident investigation, a more open and holistic approach like CAST appears to be recommended.
12:10-12:30	**STPA at Google** *Tim Falzone (Google), John Thomas (MIT)* Google has applied STPA as part of Site Reliability Engineering to identify undesirable software interactions and prevent them during design.
12:40-01:00	**Open Discussion**

Thursday, June 24

11:00-11:05	**Workshop Review and Overview**
11:05-11:10	**An STPA on OpenAPS - a Linux medical device** *Milan Lakhani (Codethink)*
11:10-11:30	**Leveraging STPA to Create an Improved Risk Matrix** *Sam Yoo and Dro Gregorian (MIT)* - The risk matrix is a widespread assessment tool that measures probability/severity of a risk to help decision makers - STPA is applied to improve the risk matrix by introducing a measure of mitigation effectiveness as a proxy for probability. - A new STPA-Informed Risk Matrix (SRM) is introduced by using two separate methodologies: the scenario based approach and hazard based approach. - The SRM combines the strengths of STPA and traditional risk assessment to better equip decision makers, particularly with new complex systems.
11:40-12:00	**STPA Return on Investment – An Industry Perspective** *Marc Nance (Boeing Retired, STAMP Engineering Services), Mark Vernacchia (General Motors), Lori Smith (Boeing Retired, STAMP Engineering Services)*

"Foresight is not about predicting the future; it's about minimizing surprise". This quote from futurist Karl Schroeder is relevant to STPA's value. One of the first management questions asked when considering STPA is what Return On Investment does it provide? This can become a chicken-or-egg dilemma as business leaders rightfully ask what "returns" can be expected from the additional "investment" in performing STPA. This presentation will discuss both "returns" and "investment" for a variety of projects of different sizes and types across several large industry sectors. It will also touch on initial thoughts of how STPA works in a scaled agile framework environment

12:10-12:15 **Industrialization Panel Speaker**
Gus Larard (Air Hong Kong/Cathay Pacific)

12:15-12:20 **Industrialization Panel Speaker**
Viana Tavares (Embraer)
The following Embraer applications will be covered
1) STPA – Product Development
2) STPA-Sec – Product Development
3) CAST – Group Study that includes ANAC

12:20-12:25 **Industrialization Panel Speaker**
Mark A Vernacchia (General Motors)

12:25-01:00 **Panel Discussion**
The panelists above were in your shoes many years ago, faced with the task of proposing and implementing STPA/CAST in their organization. This is your chance to ask the panelists about the challenges they encountered and the solutions they found to successfully implement STPA/CAST in their organization!

Friday, June 25

11:00-11:10 **Workshop Review and Overview**

11:10-11:30 **Analyzing national responses to COVID-19 pandemic using STPA**
Shufeng Chen (WMG, University of Warwick)
This talk descries the application of STPA to analyse the national-level responses to the COVID-19 pandemic. The analysis treated various stakeholders as a part of the system, including W.H.O, relevant departments of the Governments, relevant organizations (i.e. Public Health Service, Vaccine Research, Police & Military, Essential and Non-essential Service Providing Companies, and Media Companies), and the General Public, and it analyses the interactions between these stakeholders. Two example UCAs (from the Public Health Service and Vaccine Research), together with their loss scenarios and proposed requirements, will be presented in this talk.

11:40-12:00 **STPA in Support of Next-Gen Automotive E/E Architecture Development**
Sandro Nüesch (Huawei Technologies Duesseldorf GmbH), Christoph Ainhauser (Huawei Technologies Duesseldorf GmbH), Gereon Hinz, Odysseas Papanikolaou, Diego Ortiz (STTech GmbH)
- To enable the vehicles of the future, the automotive industry requires a new generation of centralized, software-defined E/E architectures (EEA).
- STPA was applied on an assumed function (L3 Highway Pilot - HWP) to derive safety requirements for a proposed EEA.
- The HWP control loop from the STAMP control structure was mapped onto the EEA design. Detail of the EEA was used to identify loss scenarios on technical level and requirements

meaningful to EEA development.
- As future work it is envisioned to apply STPA on a large collection of functions. By mapping sets of functions onto the out-of-context EEA design, the corresponding safety assurance can be provided.

12:10-12:30 **STPA Applied Before the SolarWinds Attack**
Michael Bear (BAE), John Thomas (MIT)

12:40-01:00 **Open Discussion**

Monday, June 28

11:00-11:05 **Workshop Review and Overview**

11:05-11:10 **Calculating Safety Level in Real Time: An extension of STPA**
Apostolos Zeleskidis (Democritus University of Thrace), Ioannis M. Dokas (Democritus University of Thrace), Basil Papadopoulos (Democritus University of Thrace)

11:10-11:30 **Applying STPA in development of autonomous container handling machinery**
Eetu Heikkilä (VTT Technical Research Centre of Finland Ltd.)
This presentation describes application of STPA on an autonomous container handling system. As one of the first applications of STPA in the heavy mobile machinery sector, we evaluate the suitability of STPA in this context by comparing the method with HAZOP. This includes definition of evaluation criteria for the comparison. The study suggests that STPA is a useful method in identification of accident scenarios related to autonomy.

11:40-12:00 **Key Safety Indicators using STPA**
Stuart Williams (University of Strathclyde, Glasgow)
This presentation summarizes the research done by the author for his PhD at the Maritime Safety Research Centre in the Department of Naval Architecture at the University of Strathclyde.
- STPA was used to model the safety management approaches at a cruise ship and a ferry operator to develop a set of key safety indicators.
- As a result of this work the two ship operators have modified their sets of safety indicators and their tracking processes.
- This research fills a gap in the use of safety indicators in the maritime domain by developing a set of safety indicators to provide ship operator with better feedback on the state of their safety management approaches.

12:10-12:20 **Consideration of STPA in Civil Aviations**
Linh Le (Federal Aviation Administration), Eric M Peterson (Federal Aviation Administration)
In consideration of congressional mandates and safety recommendations resulting from the 737MAX events, and in conjunction with its overall objective to improve the system safety assessment process (independent of the MAX events), the FAA seeks commercial aviation industry's experience in using STPA (or other tools/methods) in their product development and system safety assessments. Providing such information to the FAA is voluntary. All information will be treated as confidential and will be de-identified if the FAA uses it in future guidance materials.

12:20-12:30 **Hazard Analysis of Teaming Systems**
Andrew Kopeikin (MIT)
Teaming systems include multiple controllers, human and/or autonomous, acting interdependently

to achieve a common goal. There is increasing interest in fielding teaming systems in both military and civilian applications. For example, future manned helicopters will team with multiple UAS systems to execute a mission, and human-autonomy teams are envisioned to enable Urban Air Mobility. A systematic and rigorous hazard analysis method is needed to enable safety driven design of such systems to enhance V&V and certification. This talk will discuss some of the properties associated with teaming systems, and explore how a Systems Theoretic framework can enable this analysis.

12:30-12:40 **Incorporating STPA into DoD Acquisition Program**
Drake Mailes (USAF)
A short review of the work involved in getting STPA written into the contract on an extensive DoD Acquisition program. This lightning-fast presentation will describe our approach, mindset, as well as the contract language the program office adopted. You should leave with an idea of incorporating STPA into your own contracts and avoiding some of the pitfalls we discovered.

12:40-01:00 **Open Discussion**

Tuesday, June 29

11:00-11:05 **Workshop Review and Overview**

11:05-11:10 **Are You Having Success with Machine Learning?**
Michael Schmid (MIT)

11:10-11:30 **Safety analysis of interoperability conformance profiles in Medical Information Exchange**
Jens Weber (University of Victoria)
- Experiences of using STPA for hazard analysis of an interoperability conformance profile for medical information systems
- STPA is used at the level of conformance requirements
- A real-world case study in British Columbia

11:40-12:00 **Safety Analysis of a Low-cost Insulin Infusion Pump using STPA: A Case Study with Brazilian Company**
Aldo Martinazzo (Federal University of São Paulo), Luiz Eduardo Martins (Federal University of São Paulo), Tatiana Cunha (Federal University of São Paulo), Sebastião Vagner Aredes (DeltaLife)
- The low-cost insulin infusion pump is under development in Brazil by the Federal University of São Paulo in cooperation with DeltaLife, a brazilin company of medical equipment
- The purpose of the safety analysis using STPA was to support the insulin pump architectural design from a safety perspective.
- The Control Structure Model allowed a better interaction with team members of heterogeneous specialties, including health care, software development, electronic design, and mechanical design.
- Requirements were generated to implement safeguards in architectural design and to define behavioral procedures for insulin pump user.

12:10-12:20 **STPA Results From Agility Prime (Flying Cars)**
William Young (US Air Force)

12:20-12:30 **Safety analysis for an in-wheel electric motor powertrain**
Joaquim Maria Castella Triginer (Virtual Vehicle), Helmut Martin (Virtual Vehicle)
The European project HiPERFORM addresses the challenge of reducing CO2 emissions with the

	introduction of advanced wide-bandgap semiconductor technologies. The powertrain (PT) use case conceives such capabilities increasing levels of power density and improving efficiency. This presentation provides the results of the PT safety analysis following the ISO 26262 standard of the Road vehicles – Functional safety on the concept phase level together with the STPA analysis support. The STPA analysis includes the study of the unsafe control actions applied to relevant loss scenarios of the PT in-wheel motors and the design and analysis of the process model for support validation activities.
12:30-12:40	**Using STPA to address challenges in achieving SOTIF** *Amardeep Sidhu* - ISO/PAS 21448 safety of the intended functionality (SOTIF) is an upcoming standard aimed at ensuring absence of unreasonable risk due to functional insufficiencies, performance limitations, and foreseeable misuse of intended functionality. - STPA is applied on a toy ADAS system to study the use of STPA as an aid to achieve SOTIF. - The systematic approach of STPA in identifying unsafe scenarios is shown to directly help in creating artifacts related to ISO/PAS 21448 Clauses 6, 7, and 8. - Observations and key takeaways from applying STPA to achieve SOTIF are elaborated.
12:40-01:00	**Learning from a Cargo Aircraft Incident** *Gus Larard (Air Hong Kong/Cathay Pacific)*
01:00-01:20	**Open Discussion**

Wednesday, June 30

11:00-11:10	**Workshop Review and Overview**
11:10-11:30	**STPA Evaluation of Potential Conflicts between Large Commercial Air Traffic and Small Uncrewed Aircraft Systems in the Terminal Airspace** *Paul Stanley (Boeing), Victor Arcos Barraquero (Boeing)* - The rapid increase in availability and use of Small Uncrewed Aircraft Systems (sUAS) presents a potential challenge to ensuring safe separation in the crowded terminal airspace. - The system for this analysis comprises several distinct entities and organizations, so an emphasis was placed on ease of communicating the conclusions to all stakeholders. - By allocating requirements to system entities to address each causal scenario, and evaluating the current state of validation and verification for each requirement, we are able to focus discussions with stakeholders on a manageable and prioritized requirement set. STPA allows consistent traceability between the requirements and hazards.
11:40-11:50	**Discussion on STPA validation, replicability and analyst bias** *Idoaldo Lima (RWTH Aachen)* STPA includes input from analyst's and topic-expert's perspective, possibly leading to bias and reducing replicability from a different group of analysts. In a validation and replicability study for our application "STPA applied for Safety, Security and Privacy Issues in Smart Airport Terminal New Concepts", we gave a student the same input parameters and standard STPA procedure to develop a separate application. We gained valuable intel on different ways to model and implied assumptions, while finding similar control actions and constraints, leading up to similar scenarios. In order to enhance reproducibility, associated assumptions are essential, besides STPA inputs, method and results.

11:50-12:00 **Cybersecurity Incident Analysis by CAST using the Report of Unauthorized Access to the Information System**

Tomoko Kaneko (National Institute of Informatics)

This was the first case study of cybersecurity incident analysis by CAST in Japan. Results of the experiment, CAST has proven to be crucially effective as it can be applied to the analysis of cybersecurity incidents about "Report of unauthorized access to the information system of National Institute of Advanced Industrial Science and Technology (AIST)". I am a leader of the Japanese STAMP community. I will introduce that CAST Handbook have translated into Japanese with JAXA members.

12:10-12:20 **Applying CAST to Human Error Related Manufacturing Mishaps Primary Contact for the Abstract**

Jess Reid (Boeing), Emily Howard, PhD (Boeing), Kyle Ryan (Boeing)

Traditionally, Boeing utilizes chain of event problem-solving to investigate manufacturing mishaps, which treats mishaps as isolated incidents that are the result of human error. To better address the complexities in large organizations, Boeing is exploring CAST to address process and organizational improvements. We conducted CAST investigations on five separate incidents and identified common factors among them. We mapped these common factors to different parts of the control structure model and gained insight on how these seemingly 'isolated incidents' were influenced by systemic cultural and organizational issues. Based on these results, Boeing is exploring CAST as an investigation technique to be used across the enterprise.

12:20-12:30 **Using STPA to identify conflicts in coal mining safety procedures**

Alicja Krzemien (GIG Research Institute), Stanislaw Prusek (GIG Research Institute)

- This presentation analyses control actions within underground coal mines related to methane and ventilation control measures.
- Methane is an odourless gas, which is explosive within a certain proportion in the air and can also lead to suffocation.
- Given the complexity of the operational control measures that should be adopted, unsafe control actions are possible.
- Critical unsafe actions appear when different system-level hazards occur simultaneously or very close to each other.
- After identifying these cases with STPA, the most restrictive control measure should be applied in the first place to eliminate unsafe control actions effectively.

12:30-12:40 **Open STPA with RAAML and Gaphor**

Dan Yeaw (Ford Motor Company), Kyle Post (Ford Motor Company)

Do you want the ability to easily apply STPA using modern engineering tools? What about using a common language so that you can easily share the information with stakeholders? Come learn about the STPA portions of the Risk Analysis & Assessment Modeling Language (RAAML) and the open source tool that has implemented STPA called Gaphor.

- RAAML is a standardized modeling language from the OMG that is out for final release now.
- Gaphor is an open source modeling tool written in Python.
- Together they form a great combination for you to quickly complete STPA for your next project.

12:40-01:00 **Open Discussion**