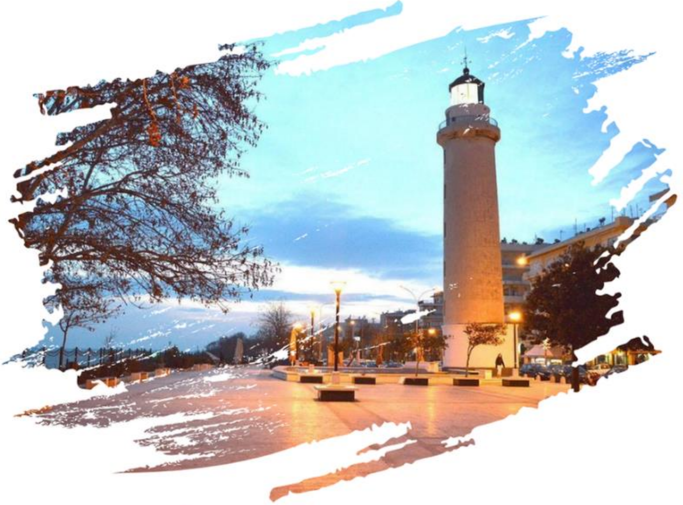
50 YEARS 1973-2023 DEMOCRITUS UNIVERSITY OF THRACE

ESWC European STAMP Workshop and Conference

CONFERENCE PROCEEDINGS



11th EUROPEAN STAMP WORKSHOP AND CONFERENCE

ADVANCING SAFETY IN A COMPLEX WORLD

ALEXANDROUPOLIS, GREECE
OCTOBER 2-4, 2024

ORGANIZING COMMITTEE

- Ioannis Dokas, Democritus University of Thrace, GR
- Maria Mikela Chatzimichailidou, University College London, UK
- Georgios Charalampos Kafoutis, Democritus University of Thrace, GR

SPONSORS

Table of Contents

Preface

Welcome to the 11th European STAMP Workshop and Conference, which marks two decades since Nancy Leveson's seminal paper, "A New Accident Model for Engineering Safer Systems." This groundbreaking work introduced the Systems-Theoretic Accident Model and Processes (STAMP), revolutionizing our approach to system safety and paving the way for innovative methodologies like STPA and CAST.

Over the past 20 years, STAMP has evolved from a novel concept to a widely adopted framework, influencing safety practices across diverse industries. This conference is a testament to the model's enduring relevance and continuous adaptation to emerging challenges in our increasingly complex technological landscape.

The abstracts compiled in this book represent the cutting-edge research and practical applications of STAMP and its associated techniques. From aviation and maritime systems to artificial intelligence and urban planning, the breadth of topics showcases the versatility and far-reaching impact of systemic approaches to safety.

We thank our esteemed keynote speakers, whose insights will undoubtedly enrich our understanding and inspire future directions in the field. We also wish to express our sincere appreciation to the scientific committee members. Their expertise and diligence have ensured the high quality and relevance of the presentations at this conference.

A special thanks goes to the Laboratory of Project Management members and students at the Democritus University of Thrace. Their tireless efforts in organizing this conference, from managing logistics to coordinating with presenters and attendees, have been instrumental in bringing this event to its success.

May this conference serve as a platform for fostering collaboration, sparking new insights, and advancing our collective mission of engineering safer systems for a complex world.

We hope you find this book of abstracts both informative and inspiring.

Ioannis M. Dokas

Associate Professor, DUTH

Chair, 11th European STAMP Workshop and Conference

11th European STAMP Workshop and Conference
Scientific Committee

Martin Rejzek, Zurich University of Applied Sciences, CH

Nektarios Karanikas , Queensland University of Technology, AU

Svana Helen Björnsdottir, Stiki, IS

John Thomas, Massachusetts Institute of Technology, US

Stefan Wagner, University of Stuttgart, DE

Reyhaneh Sadeghi, Metrolinx, CA

Anastasios Plioutsias, Coventry University, UK

Ioannis Dokas, Democritus University of Thrace, GR

Simon Whiteley, Whiteley Aerospace Safety Engineering & Management Limited, UK

Osiris A. Valdez Banda, Aalto University, FI

Jakub Montewka, Gdynia Maritime University, PL

Floris Goerlandt, Dalhousie University, CA

Apostolis Zeleskidis, Airbus, DE

Maria Mikela Chatzimichailidou, University College London, UK

Stavroula Charalabidou, Democritus University of Thrace, GR

Georgios Charalampos Kafoutis, Democritus University of Thrace, GR

Tom Kontogiannis, Technical University of Crete, GR

Ioana Koglbauer, Airbus Defence and Space, DE

Riccardo Patriarca, Sapienza University of Rome, IT

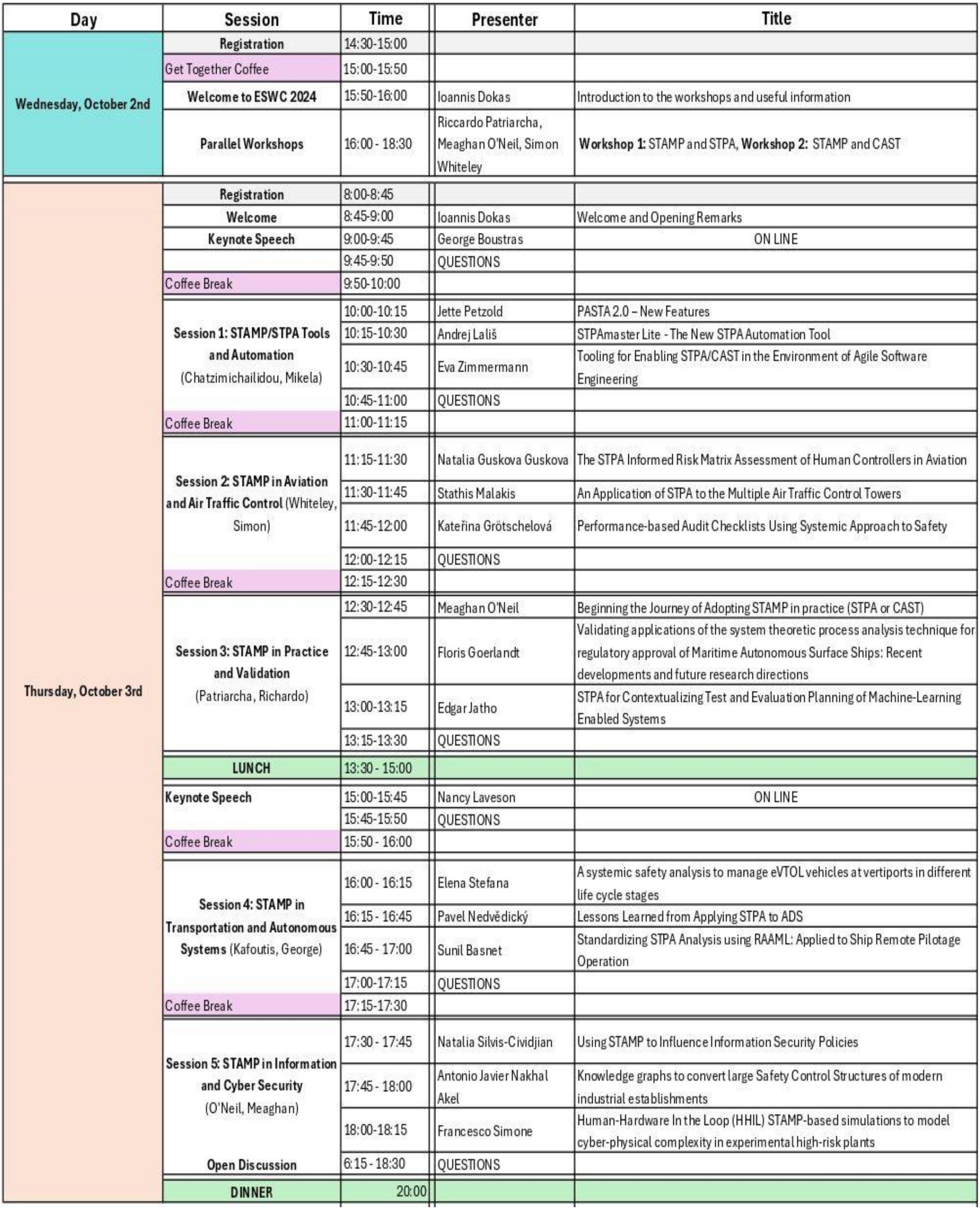
Gulsum Kubra Kaya, Cranfield University, UK

Stathis Malakis, Hellenic Civil Aviation Authority, GR

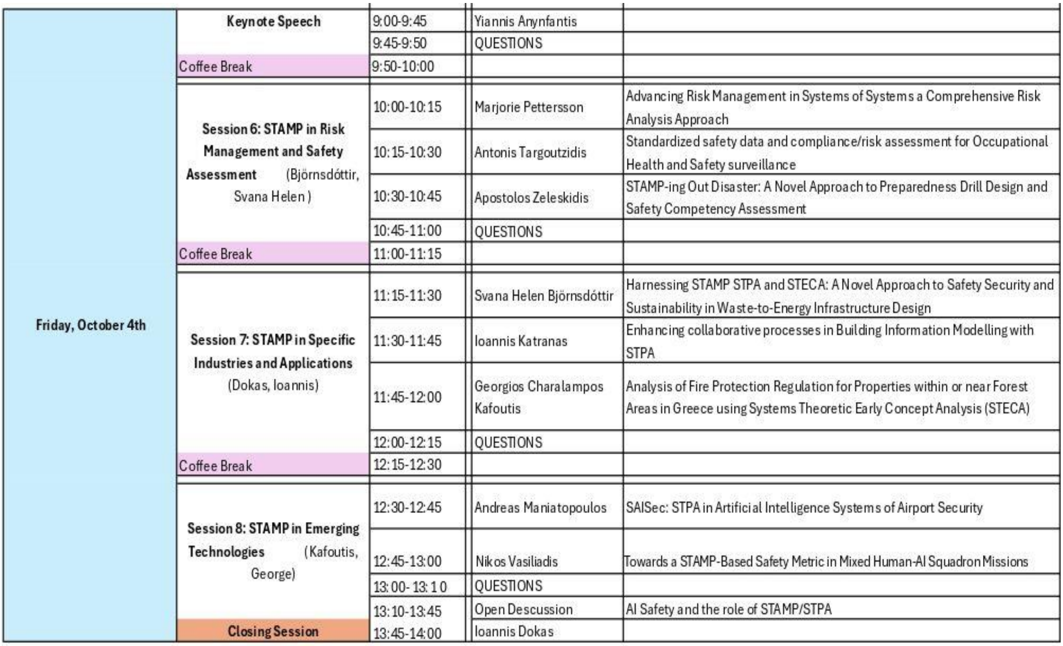
Special Thanks

Sincere thanks to Apostolos Vasileiou, Ioannis Katranas and Konstantinos Chatzigiannakis for their administrative support and Zoe Doka for the assistance with the cover design

Conference Program



Day	Session	Time	Presenter	Title
Wednesday, October 2nd	Registration	14:30-15:00		
	Get Together Coffee	15:00-15:50		
	Welcome to ESWC 2024	15:50-16:00	Ioannis Dokas	Introduction to the workshops and useful information
	Parallel Workshops	16:00 - 18:30	Riccardo Patriarcha, Meaghan O'Neil, Simon Whiteley	**Workshop 1:** STAMP and STPA, **Workshop 2:** STAMP and CAST
Thursday, October 3rd	Registration	8:00-8:45		
	Welcome	8:45-9:00	Ioannis Dokas	Welcome and Opening Remarks
	Keynote Speech	9:00-9:45	George Boustras	ON LINE
		9:45-9:50	QUESTIONS	
	Coffee Break	9:50-10:00		
	Session 1: STAMP/STPA Tools and Automation (Chatzimichailidou, Mikela)	10:00-10:15	Jette Petzold	PASTA 2.0 – New Features
		10:15-10:30	Andrej Lališ	STPAmaster Lite - The New STPA Automation Tool
		10:30-10:45	Eva Zimmermann	Tooling for Enabling STPA/CAST in the Environment of Agile Software Engineering
		10:45-11:00	QUESTIONS	
	Coffee Break	11:00-11:15		
	Session 2: STAMP in Aviation and Air Traffic Control (Whiteley, Simon)	11:15-11:30	Natalia Guskova Guskova	The STPA Informed Risk Matrix Assessment of Human Controllers in Aviation
		11:30-11:45	Stathis Malakis	An Application of STPA to the Multiple Air Traffic Control Towers
		11:45-12:00	Kateřina Grötschelová	Performance-based Audit Checklists Using Systemic Approach to Safety
		12:00-12:15	QUESTIONS	
	Coffee Break	12:15-12:30		
	Session 3: STAMP in Practice and Validation (Patriarcha, Richardo)	12:30-12:45	Meaghan O'Neil	Beginning the Journey of Adopting STAMP in practice (STPA or CAST)
		12:45-13:00	Floris Goerlandt	Validating applications of the system theoretic process analysis technique for regulatory approval of Maritime Autonomous Surface Ships: Recent developments and future research directions
		13:00-13:15	Edgar Jatho	STPA for Contextualizing Test and Evaluation Planning of Machine-Learning Enabled Systems
		13:15-13:30	QUESTIONS	
	LUNCH	13:30 - 15:00		
	Keynote Speech	15:00-15:45	Nancy Leveson	ON LINE
		15:45-15:50	QUESTIONS	
	Coffee Break	15:50 - 16:00		
	Session 4: STAMP in Transportation and Autonomous Systems (Kafoutis, George)	16:00 - 16:15	Elena Stefana	A systemic safety analysis to manage eVTOL vehicles at vertiports in different life cycle stages
		16:15 - 16:45	Pavel Nedvědický	Lessons Learned from Applying STPA to ADS
		16:45 - 17:00	Sunil Basnet	Standardizing STPA Analysis using RAAML: Applied to Ship Remote Pilotage Operation
		17:00-17:15	QUESTIONS	
	Coffee Break	17:15-17:30		
	Session 5: STAMP in Information and Cyber Security (O'Neil, Meaghan)	17:30 - 17:45	Natalia Silvis-Cividjian	Using STAMP to Influence Information Security Policies
		17:45 - 18:00	Antonio Javier Nakhal Akel	Knowledge graphs to convert large Safety Control Structures of modern industrial establishments
		18:00-18:15	Francesco Simone	Human-Hardware In the Loop (HHIL) STAMP-based simulations to model cyber-physical complexity in experimental high-risk plants
	Open Discussion	6:15 - 18:30	QUESTIONS	
	DINNER	20:00		



Friday, October 4th	**Keynote Speech**	9:00-9:45	Yiannis Anynfantis	
		9:45-9:50	QUESTIONS	
	Coffee Break	9:50-10:00		
	Session 6: STAMP in Risk Management and Safety Assessment (Björnsdóttir, Svana Helen)	10:00-10:15	Marjorie Pettersson	Advancing Risk Management in Systems of Systems a Comprehensive Risk Analysis Approach
		10:15-10:30	Antonis Targoutzidis	Standardized safety data and compliance/risk assessment for Occupational Health and Safety surveillance
		10:30-10:45	Apostolos Zeleskidis	STAMP-ing Out Disaster: A Novel Approach to Preparedness Drill Design and Safety Competency Assessment
		10:45-11:00	QUESTIONS	
	Coffee Break	11:00-11:15		
	Session 7: STAMP in Specific Industries and Applications (Dokas, Ioannis)	11:15-11:30	Svana Helen Björnsdóttir	Harnessing STAMP STPA and STECA: A Novel Approach to Safety Security and Sustainability in Waste-to-Energy Infrastructure Design
		11:30-11:45	Ioannis Katranas	Enhancing collaborative processes in Building Information Modelling with STPA
		11:45-12:00	Georgios Charalampos Kafoutis	Analysis of Fire Protection Regulation for Properties within or near Forest Areas in Greece using Systems Theoretic Early Concept Analysis (STECA)
		12:00-12:15	QUESTIONS	
	Coffee Break	12:15-12:30		
	Session 8: STAMP in Emerging Technologies (Kafoutis, George)	12:30-12:45	Andreas Maniatopoulos	SAISec: STPA in Artificial Intelligence Systems of Airport Security
		12:45-13:00	Nikos Vasiliadis	Towards a STAMP-Based Safety Metric in Mixed Human-AI Squadron Missions
		13:00- 13:10	QUESTIONS	
		13:10-13:45	Open Descussion	AI Safety and the role of STAMP/STPA
	Closing Session	13:45-14:00	Ioannis Dokas	

Abstracts & Presentations during the conference

Session1 STAMP/STPA Tools and Automation

PASTA 2.0 – New Features

Jette Petzold[1],[1] and Reinhard von Hanxleden[1]
[1] Department of Computer Science, Kiel University, Germany

ABSTRACT

Pragmatic-Automatic System Theoretic Process Analysis (PASTA) is an open-source VS Code extension providing a textual Domain Specific Language (DSL) for STPA with an automatic visualization of the control structure and the relationships between the components of the other STPA aspects. The relationships are visualized with a graph in which each STPA component is represented by a rectangular node. If a component references another component, this is visualized by an edge connecting the corresponding nodes.

To aid in the STPA process, PASTA checks an analysis for *completeness*, e.g., that for each Unsafe Control Action (UCA) a constraint is defined. Each of these checks can be disabled by the analyst. The UCAs can be stated informally, or with the help of a context table as proposed by John Thomas. Another feature of PASTA is *ID enforcement*. The analyst does not have to state the ID of a component, instead it is generated automatically. If a component is deleted or added in between existing components, the IDs of the components underneath the new/deleted one and all the references to them are automatically adjusted so that the numbering of the IDs is kept consistent.

The visualization of the control structure and relationship graph can be further adjusted by the analyst via a sidebar containing *synthesis options*. A synthesis option influences how the two graphs are created from an STPA file. For each aspect of STPA, the analyst can decide whether the components are shown. Additionally, there is an option to select for which aspect the description of components are shown alongside the ID. This option can be set to “automatic”, meaning that the aspect(s) for which the

[1] Corresponding author: email address: jep@informatik.uni-kiel.de

component descriptions are shown is determined automatically based on the current cursor position i.e. the most recent aspect for which components were defined. The sidebar contains a *filtering option* that reduces the diagram to the UCAs of a certain control action guaranteeing that the diagram is still useful if a large number of UCAs exist. Furthermore, selecting a node in the diagram highlights all connected components while all others are faded out allowing to see the relationships more clearly. For the control structure the analyst can decide whether or not the process models of the controllers are shown.

When the analysis is finished, a result report can be created in which each aspect has its own section with the defined components. Additionally, each section contains a diagram in which the components defined so far are shown. For the UCAs, controller constraints, and scenarios, a diagram is added for each control action filtered by this control action. At the end of the file, a summary section states all defined constraints. The markdown file can be exported as PDF using an appropriate VS Code Extension or another tool.

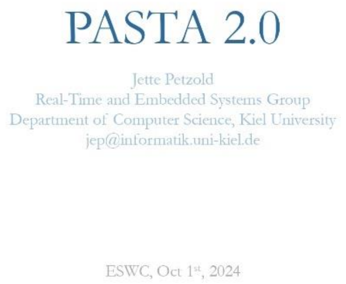
Besides STPA, PASTA also supports Fault Tree Analysis (FTA). A textual DSL with an automatic visualization is provided by PASTA. Options to further adjust the FTA diagram exist, e.g., showing the descriptions of gates or components. To analyze the Fault Tree, a cut set analysis can be triggered by the analyst. The visualization of the resulting cut sets as well as the single points of failure can be shown by selecting a cut set in a dropdown menu in the sidebar.

After STPA is performed, PASTA offers to automatically generate Fault Trees based on the analysis. For each hazard a Fault Tree with that hazard as the top event is created. The scenarios leading to the hazard are grouped based on their causal factor with an OR gate and all groups are combined with an OR gate leading to the top event. Scenarios for which no causal factor is stated are sorted into their own group. This helps to analyze especially the component failures found with STPA even further.

The UCAs identified with STPA can be transformed to LTL formulas. When modeling a system with Sequentially Constructive Statecharts (SCCharts) using the KIELER VS Code extension, these formulas can be automatically generated and imported from an STPA file the user chooses. SCCharts are statecharts that can contain several states, transitions with priorities, and input, output, and internal variables. Furthermore, PASTA offers to automatically generate an SCChart for a controller depicting its behavior model. For that, the UCAs belonging to the control actions of the controller are translated to LTL formulas and these formulas are translated to a statechart. The resulting SCChart is safe but does not yet fulfill the system goals. To that end, we extended PASTA to also allow the definition of Desired Control Actions (DCAs). These are stated just like UCAs with a control action, type, and context and hence can be translated to LTL formulas the same way. With these DCAs the generated SCChart fulfills safety properties as well as liveness properties. Still, it is not necessarily complete because internal calculations cannot be inferred. However, it offers a good foundation that fulfills the safety properties identified with STPA.

Keywords: Tool Support; VS Code Extension; Safety Analysis; Verification

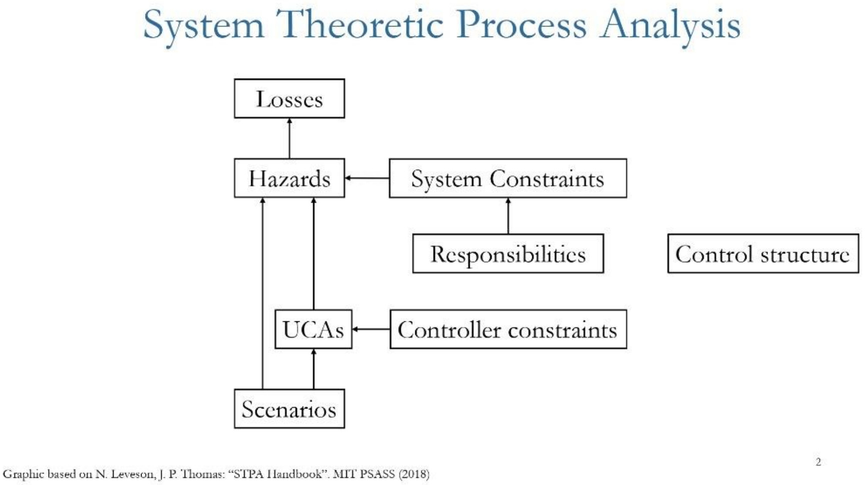
PRESENTATION



PASTA 2.0

Jette Petzold
Real-Time and Embedded Systems Group
Department of Computer Science, Kiel University
jep@informatik.uni-kiel.de

ESWC, Oct 1st, 2024



System Theoretic Process Analysis

Losses

Hazards

System Constraints

Responsibilities

Control structure

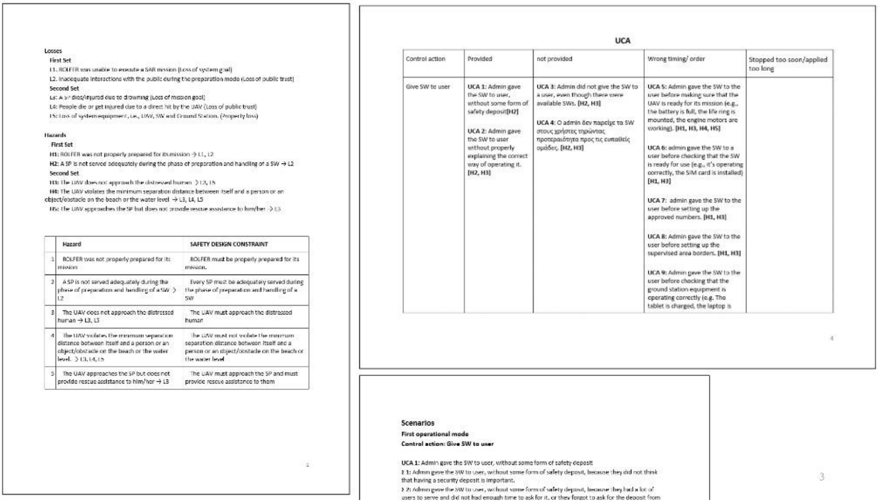
UCAs

Controller constraints

Scenarios

Graphic based on N. Leveson, J. P. Thomas: "STPA Handbook". MIT PSASS (2018)

2



Losses

First Set

L1. ROLFER was unable to execute a SAR mission (Loss of system goal)

L2. Inadequate interactions with the public during the preparation mode (Loss of public trust)

Second Set

L3: A SP dies/injured due to drowning (Loss of mission goal)

L4: People die or get injured due to a direct hit by the UAV (Loss of public trust)

L5: Loss of system equipment, i.e., UAV, SW and Ground Station. (Property loss)

Hazards

First Set

H1: ROLFER was not properly prepared for its mission → L1, L2

H2: A SP is not served adequately during the phase of preparation and handling of a SW → L2

Second Set

H3: The UAV does not approach the distressed human → L3, L5

H4: The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5

H5: The UAV approaches the SP but does not provide rescue assistance to him/her → L3

	Hazard	SAFETY DESIGN CONSTRAINT
1	ROLFER was not properly prepared for its mission	ROLFER must be properly prepared for its mission.
2	A SP is not served adequately during the phase of preparation and handling of a SW → L2	Every SP must be adequately served during the phase of preparation and handling of a SW
3	The UAV does not approach the distressed human → L3, L5	The UAV must approach the distressed human
4	The UAV violates the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level. → L3, L4, L5	The UAV must not violate the minimum separation distance between itself and a person or an object/obstacle on the beach or the water level
5	The UAV approaches the SP but does not provide rescue assistance to him/her → L3	The UAV must approach the SP and must provide rescue assistance to them

1

UCA

Control action	Provided	not provided	Wrong timing/ order	Stopped too soon/applied too long
Give SW to user	**UCA 1**: Admin gave the SW to user, without some form of safety deposit**[H2]** **UCA 2**: Admin gave the SW to user without properly explaining the correct way of operating it. **[H2, H3]**	**UCA 3**: Admin did not give the SW to a user, even though there were available SWs. **[H2, H3]** **UCA 4**: O admin δεν παρείχε τα SW στους χρήστες τηρώντας προτεραιότητα προς τις ευπαθείς ομάδες. **[H2, H3]**	**UCA 5:** Admin gave the SW to the user before making sure that the UAV is ready for its mission (e.g., the battery is full, the life ring is mounted, the engine motors are working). **[H1, H3, H4, H5]** **UCA 6:** admin gave the SW to a user before checking that the SW is ready for use (e.g., it's operating correctly, the SIM card is installed) **[H1, H3]** **UCA 7**: admin gave the SW to the user before setting up the approved numbers. **[H1, H3]** **UCA 8:** Admin gave the SW to the user before setting up the supervised area borders. **[H1, H3]** **UCA 9:** Admin gave the SW to the user before checking that the ground station equipment is operating correctly (e.g. The tablet is charged, the laptop is	

4

Scenarios

First operational mode

Control action: Give SW to user

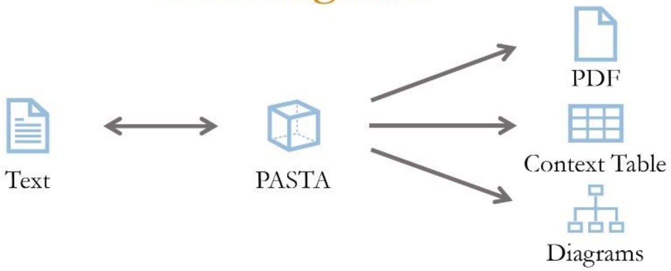
UCA 1: Admin gave the SW to user, without some form of safety deposit

Σ 1: Admin gave the SW to user, without some form of safety deposit, because they did not think that having a security deposit is important.

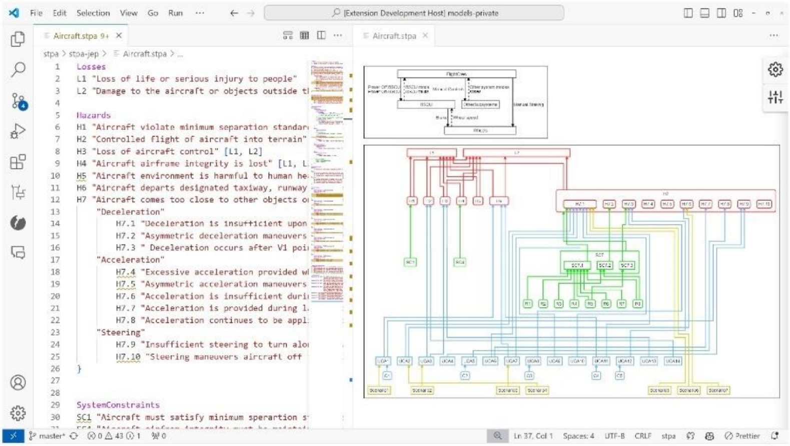
Σ 2: Admin gave the SW to user, without some form of safety deposit, because they had a lot of users to serve and did not had enough time to ask for it, or they forgot to ask for the deposit from

3

Combine **Textual** Descriptions with **Diagrams**



4


File Edit Selection View Go Run ···
[Extension Development Host] models-private
Aircraft.stpa 9+
Aircraft.stpa
stpa > stpa-jep > Aircraft.stpa > ...
master* ⓧ 0 △ 43 ⓘ 1 🕪 0
Ln 37, Col 1 Spaces: 4 UTF-8 CRLF stpa Prettier

```
Losses
L1 "Loss of life or serious injury to people"
L2 "Damage to the aircraft or objects outside tl

Hazards
H1 "Aircraft violate minimum separation standar
H2 "Controlled flight of aircraft into terrain"
H3 "Loss of aircraft control" [L1, L2]
H4 "Aircraft airframe integrity is lost" [L1, L
H5 "Aircraft environment is harmful to human he
H6 "Aircraft departs designated taxiway, runway
H7 "Aircraft comes too close to other objects o
    "Deceleration"
        H7.1 "Deceleration is insufficient upon
        H7.2 "Asymmetric deceleration maneuvers
        H7.3 " Deceleration occurs after V1 poi
    "Acceleration"
        H7.4 "Excessive acceleration provided w
        H7.5 "Asymmetric acceleration maneuvers
        H7.6 "Acceleration is insufficient duri
        H7.7 "Acceleration is provided during l
        H7.8 "Acceleration continues to be appl
    "Steering"
        H7.9 "Insufficient steering to turn alo
        H7.10 "Steering maneuvers aircraft off
}


SystemConstraints
SC1 "Aircraft must satisfy minimum sperartion s
```

Features

Validation / Completeness Checks

ID Generation

Automatic Generation of Constraints

Automatic Display of Descriptions

Result Report

Fault Tree Analysis

Textual description

Automatic Diagram Generation

Fault Tree Generation based on STPA result

Safe Behavior Model

Safe Behavior Model Synthesis

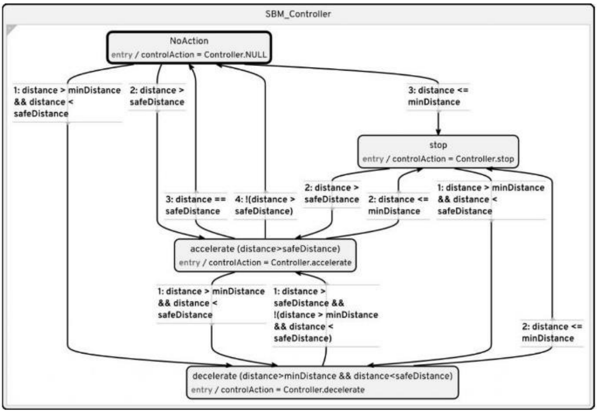
Unsafe Control Actions

Linear Temporal Logic Formulas

Safe Behavior Model

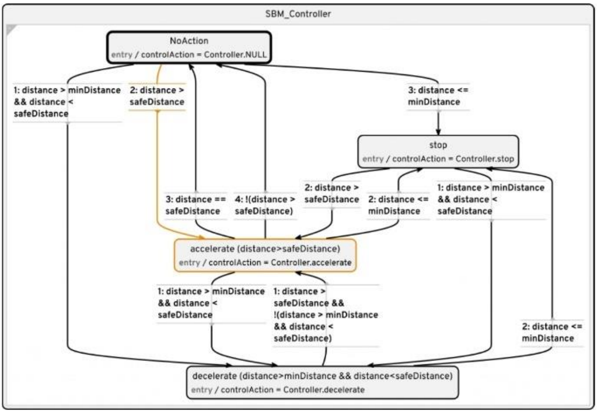
Safe Behavior Model Synthesis

UCA1: "Controller does not send *accelerate* while the distance is above the safe distance" [H1]


SBM_Controller
NoAction
entry / controlAction = Controller.NULL
1: distance > minDistance && distance < safeDistance
2: distance > safeDistance
3: distance <= minDistance
stop
entry / controlAction = Controller.stop
3: distance == safeDistance
4: !(distance > safeDistance)
2: distance > safeDistance
2: distance <= minDistance
1: distance > minDistance && distance < safeDistance
accelerate (distance>safeDistance)
entry / controlAction = Controller.accelerate
1: distance > minDistance && distance < safeDistance
1: distance > safeDistance && !(distance > minDistance && distance < safeDistance)
2: distance <= minDistance
decelerate (distance>minDistance && distance<safeDistance)
entry / controlAction = Controller.decelerate

Safe Behavior Model Synthesis

UCA1: "Controller does not send *accelerate* while the distance is above the safe distance" [H1]



SBM_Controller

NoAction
entry / controlAction = Controller.NULL

1: distance > minDistance && distance < safeDistance

2: distance > safeDistance

3: distance <= minDistance

stop
entry / controlAction = Controller.stop

3: distance == safeDistance

4: !(distance > safeDistance)

2: distance > safeDistance

2: distance <= minDistance

1: distance > minDistance && distance < safeDistance

accelerate (distance>safeDistance)
entry / controlAction = Controller.accelerate

1: distance > minDistance && distance < safeDistance

1: distance > safeDistance && !(distance > minDistance && distance < safeDistance)

2: distance <= minDistance

decelerate (distance>minDistance && distance<safeDistance)
entry / controlAction = Controller.decelerate

PASTA

GitHub Project

https://github.com/kieler/stpa

VSCode Marketplace

https://marketplace.visualstudio.com/items?itemName=kieler.pasta

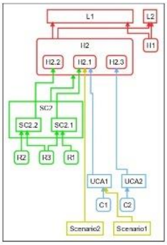
Feedback and feature requests are very welcome!

jep@informatik.uni-kiel.de

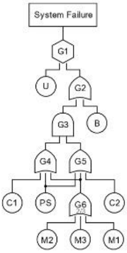
Appendix

Summary

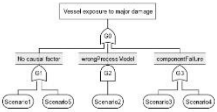
STPA Support



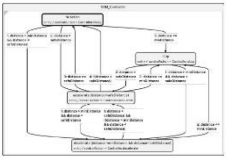
FTA Support



STPA to FTA



SBM Synthesis



System Theoretic Process Analysis

Define purpose of the analysis:
Losses Hazards System Constraints

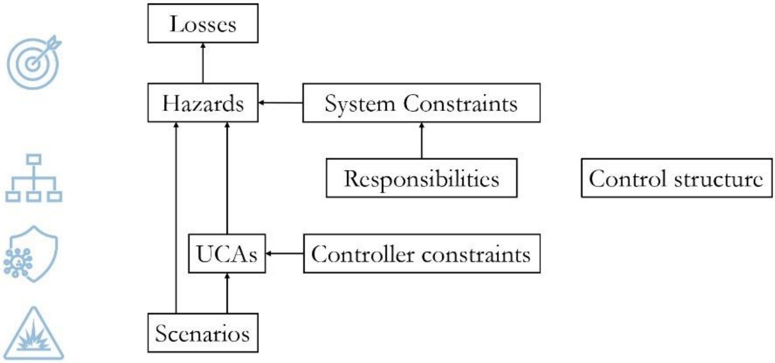
Model the control structure:
Responsibilities Control structure

Identify Unsafe Control Actions (UCAs):
UCAs Controller constraints

Identify loss scenarios:
Scenarios

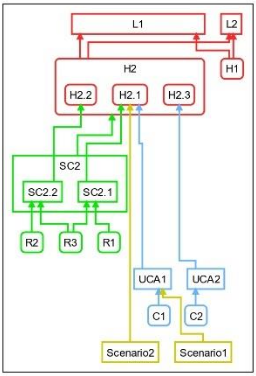
Graphic based on N. Leveson, J. P. Thomas: "STPA Handbook". MIT PSASS (2018)

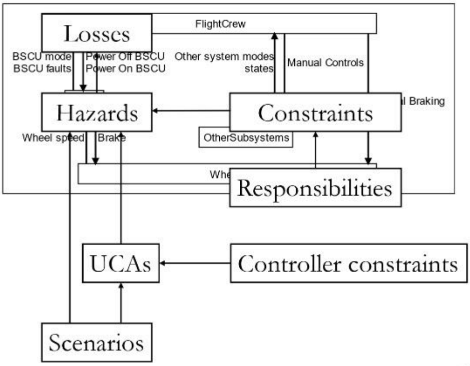
System Theoretic Process Analysis



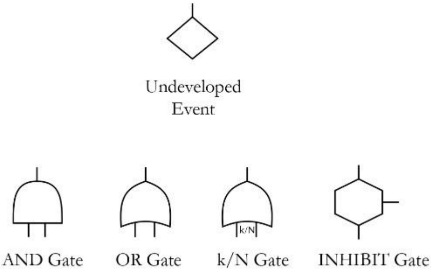
Graphic based on N. Leveson, J. P. Thomas: "STPA Handbook". MIT PSASS (2018)

Visualization





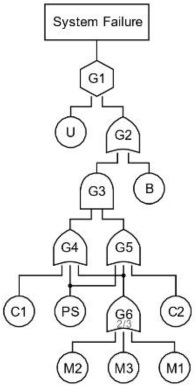
Fault Tree Analysis in PASTA



E. Ruijters, M. Stoelinga: "Fault Tree Analysis: A survey of the state-of-the-art in modeling, analysis and tools"
Computer Science Review, 2015

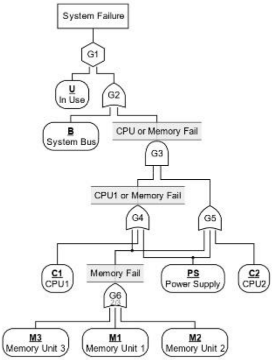
Fault Tree Analysis in PASTA

```
Components
M1 "Memory Unit 1"
M2 "Memory Unit 2"
…

TopEvent
U "In Use"

TopEvent
"System Failure" = G1

Gates
G1 = U inhibits G2
G2 = G3 or B
G3 "CPU or Memory Fail" = G4 and G5
G4 "CPU1 or Memory Fail" = C1 or PS or G6
…
```

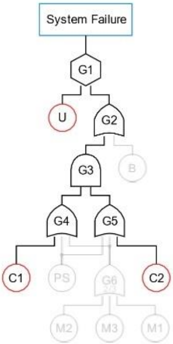


Fault Tree Analysis

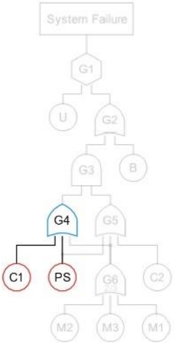
Fault Tree with Descriptions

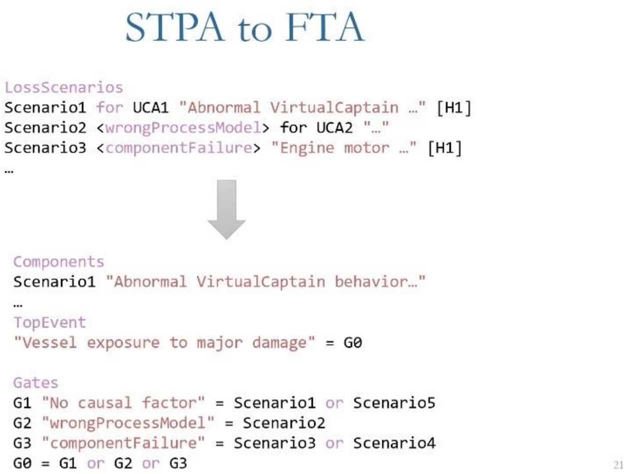


Minimal Cut Set
{U, C1, C2}



Single Points of Failure
for subtree G4

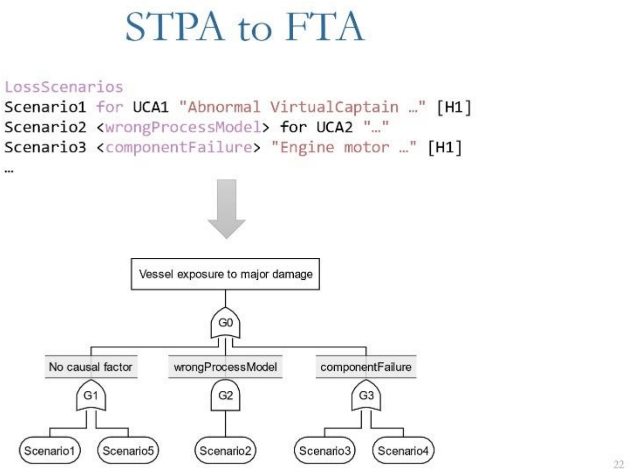




STPA to FTA

```
LossScenarios
Scenario1 for UCA1 "Abnormal VirtualCaptain …" [H1]
Scenario2 <wrongProcessModel> for UCA2 "…"
Scenario3 <componentFailure> "Engine motor …" [H1]
…
```

```
Components
Scenario1 "Abnormal VirtualCaptain behavior…"
…
TopEvent
"Vessel exposure to major damage" = G0

Gates
G1 "No causal factor" = Scenario1 or Scenario5
G2 "wrongProcessModel" = Scenario2
G3 "componentFailure" = Scenario3 or Scenario4
G0 = G1 or G2 or G3
```



STPA to FTA

```
LossScenarios
Scenario1 for UCA1 "Abnormal VirtualCaptain …" [H1]
Scenario2 <wrongProcessModel> for UCA2 "…"
Scenario3 <componentFailure> "Engine motor …" [H1]
…
```

Safe Behavior Model Synthesis

Unsafe Control Action

↓

Linear Temporal Logic Formulas

↓

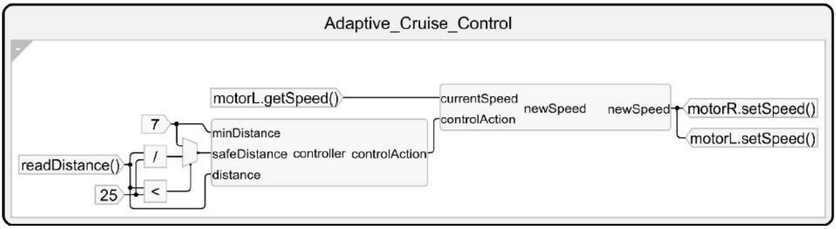
Safe Behavior Model

control action	distance	Hazardous control action?		
		Provided any time	Provided too early	Provided too late
accelerate	underSafe Distance	UCA1	…	
…				

↓

G(distance < minDistance → !accelerate)

Safe Behavior Model Synthesis



Safe Behavior Model Synthesis

Video

STPAmaster Lite-The New STPA Automation Toolsilvis

Andrej Lališ

AKAENE Partners, Czech Republic

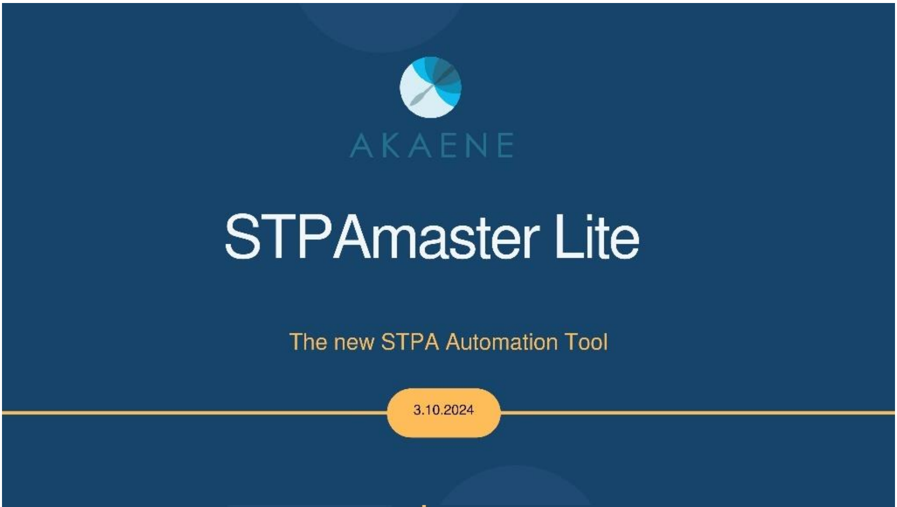
ABSTRACT

Currently available tools for STPA analyses exhibit limitations that prevent their wider adoption by the industry and practitioners. Some are prototypes only, others support only part of the analysis or are limited to a specific domain, while existing proprietary solutions are not easily available for the community. “STPA master Lite” is a free Google Sheets-based STPA tool following the “STPA Automation Tool” by Andrew Miller, recent MIT research and the experience from using STPA in the Czech aviation industry, to support industry application and standardization of the STAMP-based methods. The Lite version implements some of the core functionality of “STPAmaster”, a solution being developed by AKAENE and Czech Technical University in Prague to overcome practical limitations of the current STPA tools, specifically their seamless integration with safety management systems and systems engineering applications. The new tool allows anyone to try or perform a complete STPA in a free and user-friendly environment, with automation of routine efforts and checks for basic errors to perform a valid STPA analysis. Specifically, it supports all steps of the STPA, importing safety control structure from external diagramming editors (draw.io and yEd editor) with automatic recognition of control actions and feedbacks, pre-generation of unsafe control actions and loss scenarios, management of all types of safety constraints and check for basic consistency and traceability errors. It provides improved user environment and, similar to the STPA Automation Tool, it integrates with common

software tools, e.g., analysis inputs and outputs can be handled by spreadsheet editors, such as Google Sheets or Microsoft Excel, PDF export is natively supported etc. The tool has significant potential to compensate for the lack of accessible and user-friendly STPA tools and to support further growth of the STAMP community.

Keywords: Automation; Software tools; System-Theoretic Accident Model and Processes; System-Theoretic Process Analysis

PRESENTATION

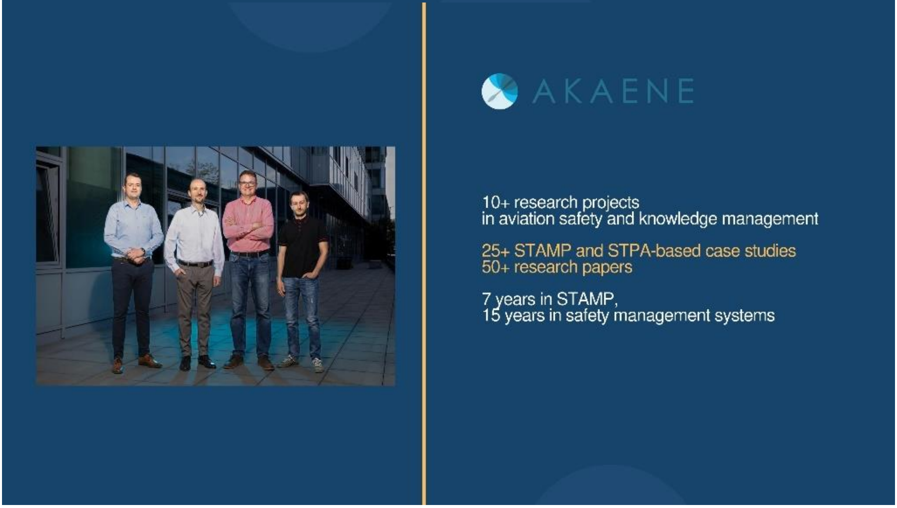


AKAENE

STPAmaster Lite

The new STPA Automation Tool

3.10.2024



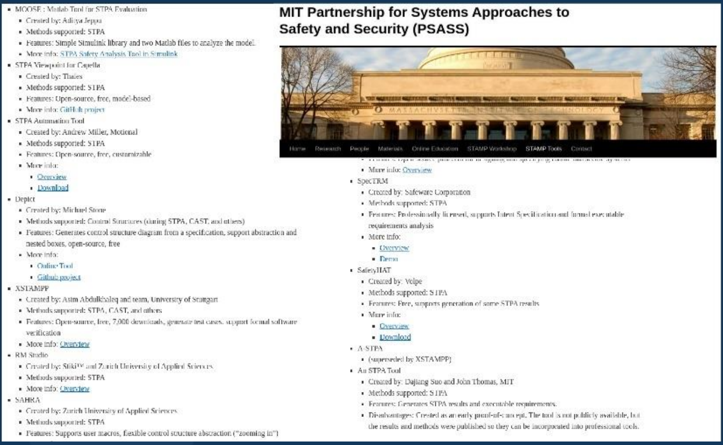
AKAENE

10+ research projects
in aviation safety and knowledge management

25+ STAMP and STPA-based case studies
50+ research papers

7 years in STAMP,
15 years in safety management systems

AKAENE



MIT Partnership for Systems Approaches to Safety and Security (PSASS)

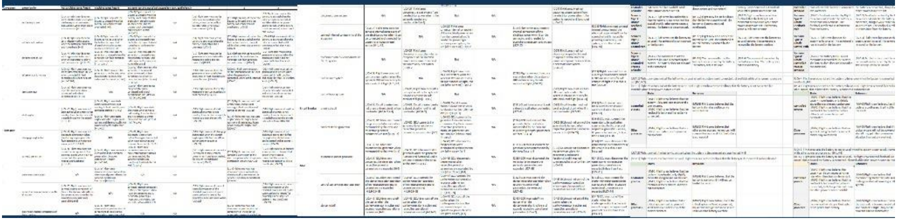
- MOOSE : Matlab Tool for STPA Evaluation
  - Created by: Aditya Jeppu
  - Methods supported: STPA
  - Features: Simple Simulink library and two Matlab files to analyze the model.
  - More info: STPA Safety Analysis Tool in Simulink
- STPA Viewpoint for Capella
  - Created by: Thales
  - Methods supported: STPA
  - Features: Open-source, free, model-based
  - More info: GitHub project
- STPA Automation Tool
  - Created by: Andrew Miller, Motional
  - Methods supported: STPA
  - Features: Open-source, free, customizable
  - More info:
    - Overview
    - Download
- Depict
  - Created by: Michael Stone
  - Methods supported: Control Structures (during STPA, CAST, and others)
  - Features: Generates control structure diagram from a specification, support abstraction and nested boxes, open-source, free
  - More info:
    - Online Tool
    - Github project
- XSTAMPP
  - Created by: Asim Abdulkhaleq and team, University of Stuttgart
  - Methods supported: STPA, CAST, and others
  - Features: Open-source, free, 7,000 downloads, generate test cases. support formal software verification
  - More info: Overview
- RM Studio
  - Created by: Stiki™ and Zurich University of Applied Sciences
  - Methods supported: STPA
  - More info: Overview
- SAHRA
  - Created by: Zurich University of Applied Sciences
  - Methods supported: STPA
  - Features: Supports user macros, flexible control structure abstraction ("zooming in")

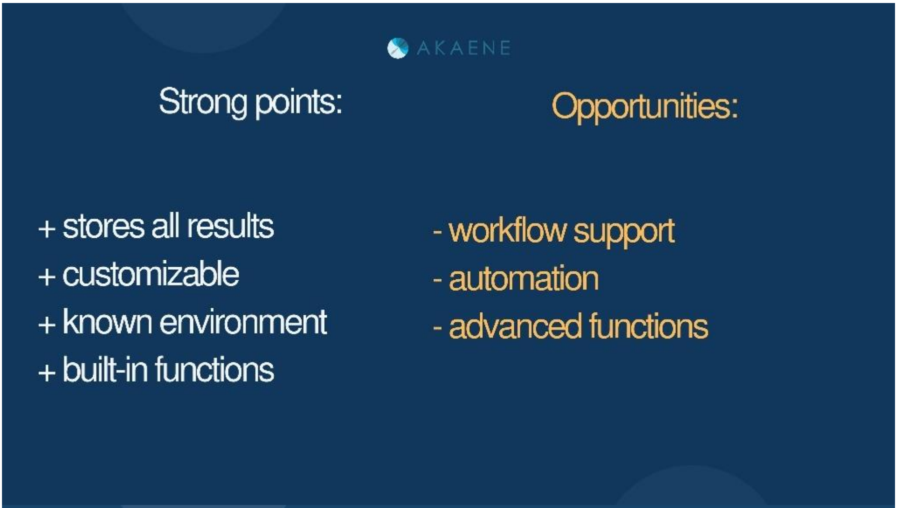
  - [illegible]
  - More info: Overview
- SpecTRM
  - Created by: Safeware Corporation
  - Methods supported: STPA
  - Features: Professionally licensed, supports Intent Specification and formal executable requirements analysis
  - More info:
    - Overview
    - Demo
- SafetyHAT
  - Created by: Volpe
  - Methods supported: STPA
  - Features: Free, supports generation of some STPA results
  - More info:
    - Overview
    - Download
- A-STPA
  - (superseded by XSTAMPP)
- An STPA Tool
  - Created by: Dajiang Suo and John Thomas, MIT
  - Methods supported: STPA
  - Features: Generates STPA results and executable requirements.
  - Disadvantages: Created as an early proof-of-concept. The tool is not publicly available, but the results and methods were published so they can be incorporated into professional tools.

AKAENE

Which of the STAMP tools is the most popular?

Microsoft Office





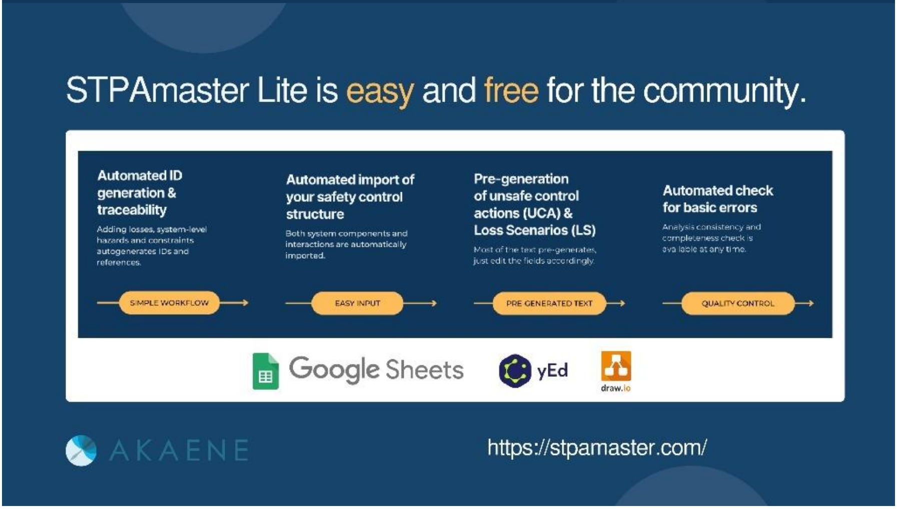
AKAENE

Strong points:

+ stores all results
+ customizable
+ known environment
+ built-in functions

Opportunities:

- workflow support
- automation
- advanced functions



STPAmaster Lite is easy and free for the community.

Automated ID generation & traceability

Adding losses, system-level hazards and constraints autogenerates IDs and references.

SIMPLE WORKFLOW

Automated import of your safety control structure

Both system components and interactions are automatically imported.

EASY INPUT

Pre-generation of unsafe control actions (UCA) & Loss Scenarios (LS)

Most of the text pre-generates, just edit the fields accordingly.

PRE GENERATED TEXT

Automated check for basic errors

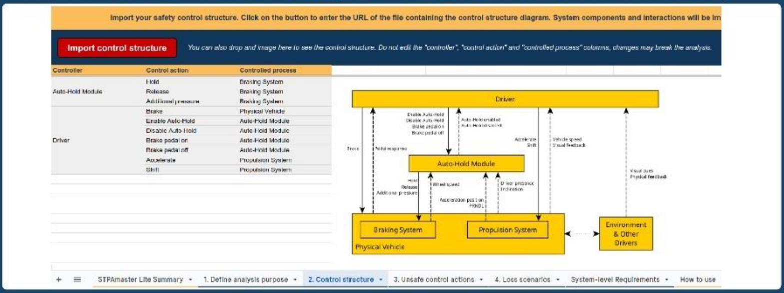
Analysis consistency and completeness check is ava lable at any time.

QUALITY CONTROL

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy and free for the community.



Import your safety control structure. Click on the button to enter the URL of the file containing the control structure diagram. System components and interactions will be im

Import control structure

You can also drop and image here to see the control structure. Do not edit the "controller", "control action" and "controlled process" columns, changes may break the analysis.

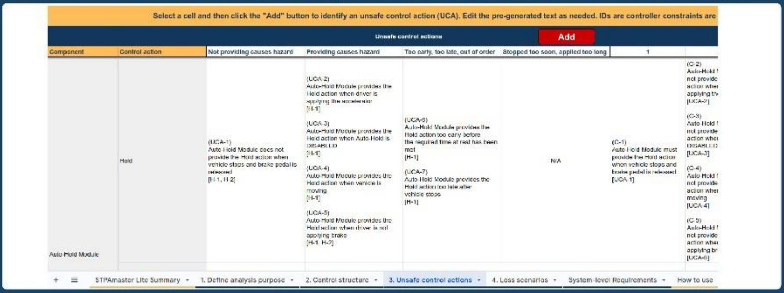
Controller	Control action	Controlled process
Auto-Hold Module	Hold	Braking System
	Release	Braking System
	Additional pressure	Braking System
Driver	Brake	Physical Vehicle
	Enable Auto-Hold	Auto-Hold Module
	Disable Auto-Hold	Auto-Hold Module
	Brake pedal on	Auto-Hold Module
	Brake pedal off	Auto-Hold Module
	Accelerate	Propulsion System
	Shift	Propulsion System

+
≡
STPAmaster Lite Summary
1. Define analysis purpose
2. Control structure
3. Unsafe control actions
4. Loss scenarios
System-level Requirements
How to use

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy and free for the community.



Select a cell and then click the "Add" button to identify an unsafe control action (UCA). Edit the pre-generated text as needed. IDs are controller constraints are

Unsafe control actions

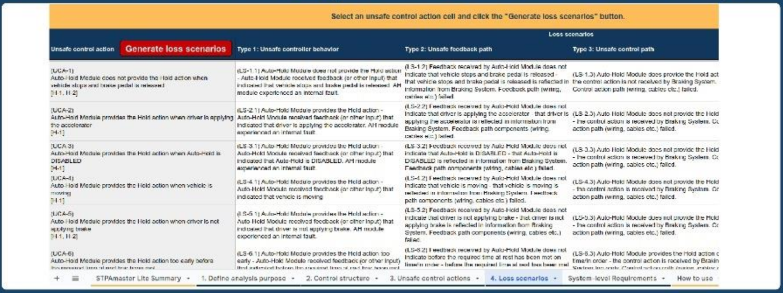
Component	Control action	Not providing causes hazard	Providing causes hazard	Too early, too late, out of order	Stopped too soon, applied too long	1	
Auto-Hold Module	Hold	(UCA-1) Auto-Hold Module does not provide the Hold action when vehicle stops and brake pedal is released [H-1, H-2]	(UCA-2) Auto-Hold Module provides the Hold action when driver is applying the accelerator [H-1] (UCA-3) Auto-Hold Module provides the Hold action when Auto-Hold is DISABLED [H-1] (UCA-4) Auto-Hold Module provides the Hold action when vehicle is moving [H-1] (UCA-5) Auto-Hold Module provides the Hold action when driver is not applying brake [H-1, H-2]	(UCA-6) Auto-Hold Module provides the Hold action too early before the required time at rest has been met [H-1] (UCA-7) Auto-Hold Module provides the Hold action too late after vehicle stops [H-1]	N/A	(C-1) Auto-Hold Module must provide the Hold action when vehicle stops and brake pedal is released [UCA-1]	(C-2) Auto-Hold I not provide action whe applying th [UCA-2] (C-3) Auto-Hold I not provide action whe DISABLED [UCA-3] (C-4) Auto-Hold I not provide action whe moving [UCA-4] (C-5) Auto-Hold I not provide action whe applying br [UCA-5]

+
≡
STPAmaster Lite Summary
1. Define analysis purpose
2. Control structure
3. Unsafe control actions
4. Loss scenarios
System-level Requirements
How to use

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy and free for the community.



Select an unsafe control action cell and click the "Generate loss scenarios" button.

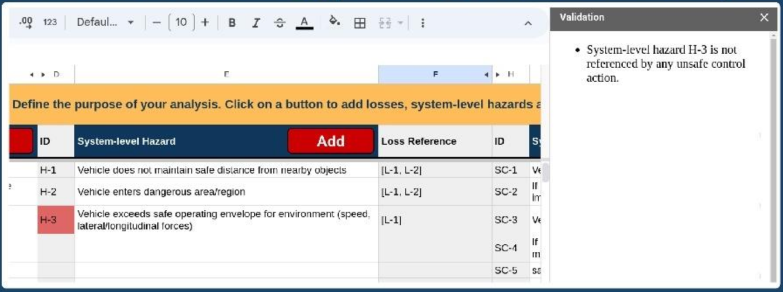
		Loss scenarios	
Unsafe control action **Generate loss scenarios**	Type 1: Unsafe controller behavior	Type 2: Unsafe feedback path	Type 3: Unsafe control path
(UCA-1) Auto-Hold Module does not provide the Hold action when vehicle stops and brake pedal is released [H-1, H-2]	(LS-1.1) Auto-Hold Module does not provide the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle stops and brake pedal is released. AH module experienced an internal fault.	(LS-1.2) Feedback received by Auto-Hold Module does not indicate that vehicle stops and brake pedal is released - that vehicle stops and brake pedal is released is reflected in information from Braking System. Feedback path (wiring, cables etc.) failed.	(LS-1.3) Auto-Hold Module does provide the Hold act the control action is not received by Braking System. Control action path (wiring, cables etc.) failed.
(UCA-2) Auto-Hold Module provides the Hold action when driver is applying the accelerator [H-1]	(LS-2.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that driver is applying the accelerator. AH module experienced an internal fault.	(LS-2.2) Feedback received by Auto-Hold Module does not indicate that driver is applying the accelerator - that driver is applying the accelerator is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-2.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Co action path (wiring, cables etc.) failed.
(UCA-3) Auto-Hold Module provides the Hold action when Auto-Hold is DISABLED [H-1]	(LS-3.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that Auto-Hold is DISABLED. AH module experienced an internal fault.	(LS-3.2) Feedback received by Auto-Hold Module does not indicate that Auto-Hold is DISABLED - that Auto-Hold is DISABLED is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-3.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Co action path (wiring, cables etc.) failed.
(UCA-4) Auto-Hold Module provides the Hold action when vehicle is moving [H-1]	(LS-4.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that vehicle is moving	(LS-4.2) Feedback received by Auto-Hold Module does not indicate that vehicle is moving - that vehicle is moving is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-4.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Co action path (wiring, cables etc.) failed.
(UCA-5) Auto-Hold Module provides the Hold action when driver is not applying brake [H-1, H-2]	(LS-5.1) Auto-Hold Module provides the Hold action - Auto-Hold Module received feedback (or other input) that indicated that driver is not applying brake. AH module experienced an internal fault.	(LS-5.2) Feedback received by Auto-Hold Module does not indicate that driver is not applying brake - that driver is not applying brake is reflected in information from Braking System. Feedback path components (wiring, cables etc.) failed.	(LS-5.3) Auto-Hold Module does not provide the Hold - the control action is received by Braking System. Co action path (wiring, cables etc.) failed.
(UCA-6) Auto-Hold Module provides the Hold action too early before the required time at rest has been met	(LS-6.1) Auto-Hold Module provides the Hold action too early - Auto-Hold Module received feedback (or other input) that indicated before the required time at rest has been met	(LS-6.2) Feedback received by Auto-Hold Module does not indicate before the required time at rest has been met on time/in order - before the required time at rest has been met	(LS-6.3) Auto-Hold Module provides the Hold action c time/in order - the control action is received by Brakin System too early. Control action path (wiring, cables e

+
STPAmaster Lite Summary
1. Define analysis purpose
2. Control structure
3. Unsafe control actions
4. Loss scenarios
System-level Requirements
How to use

AKAENE

https://stpamaster.com/

STPAmaster Lite is easy and free for the community.



Define the purpose of your analysis. Click on a button to add losses, system-level hazards a

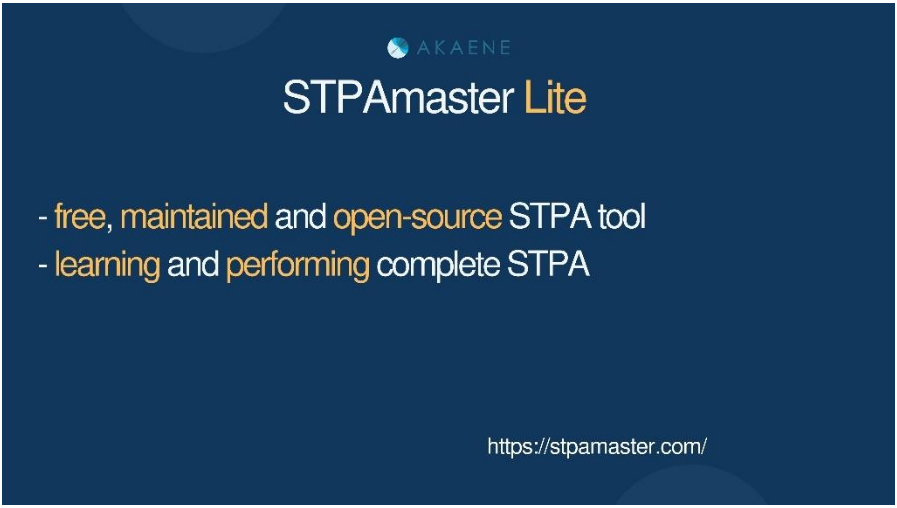
	ID	System-level Hazard **Add**	Loss Reference	ID	S
	H-1	Vehicle does not maintain safe distance from nearby objects	[L-1, L-2]	SC-1	Ve
	H-2	Vehicle enters dangerous area/region	[L-1, L-2]	SC-2	If im
	H-3	Vehicle exceeds safe operating envelope for environment (speed, lateral/longitudinal forces)	[L-1]	SC-3	Ve
				SC-4	If m
				SC-5	sa

Validation

- System-level hazard H-3 is not referenced by any unsafe control action.

AKAENE

https://stpamaster.com/



AKAENE

STPAmaster Lite

- free, maintained and open-source STPA tool
- learning and performing complete STPA

https://stpamaster.com/

Tooling for Enabling STPA/CAST in the Environment of Agile Software Engineering

Eva Zimmermann[2], Pavel Nedvědický and Stefan Wagner
Technical University of Munich, Germany

ABSTRACT

It has been demonstrated that STPA effectively ensures safety in complex systems. Nevertheless, integrating STPA into modern DevOps practices presents a significant challenge. Our aim to combine this arises from the need for faster and more efficient cycles in developing software systems, for which DevOps is a crucial point. We bridge the gap between STPA and the software development process in software-intensive systems to achieve efficiency and higher safety standards in the development process itself. This is especially important for industries such as the automotive industry, where the software intensity continuously increases. To address this, we built a tool that we integrated into the DevOps process. By implementing this approach, we not only achieve integration but also improve the early and continuous mitigation of hazards. When the hazard analysis becomes a crucial part of the development workflow, we can provide feedback faster and ensure that we continuously improve the system. Thereby, safety issues can then be addressed proactively as soon as they appear.

Our tool support incorporates STPA and CAST and offers various additional features, such as existing extensions to these analysis methods.

All four steps of STPA are included in our tool. The documentation for Losses, Hazards, and Constraints and a system description are included in step 1. Additionally, documents can be linked to the system description, providing further information regarding the system's crucial components.

In the second step, we can model the control structure and the responsibilities. The tool also allows you to document process models and variables. The third step allows the documentation of UCAs and the associated controller constraints of the previously defined control actions. In the last step, loss scenarios can be determined. In addition to the STPA handbook steps, we extended the UCA in step 4 with a “UCA refinement.”

[2] Eva Zimmermann, e.zimmermann@tum.de

Here, a model-checking component is integrated to create and connect terms that enable formalization to check them with SPIN or NuSVM.

Furthermore, we implemented support for safety engineers during the CAST analysis to analyze the causes of accidents. Here, we followed the handbook and the corresponding steps 1 – 4.

We integrated the tool into the DevOps cycle to address and fill the previously mentioned gap.

First, we enable the connection of our tool with the Version Control System (VCS). Git integration allows easy tracking of the emerging safety artifacts throughout the development lifecycle. Furthermore, the STPA results can be directly used in the planning phase for the following software cycle. It also ensures that safety requirements derived from STPA can be used and established in the software development process.

Another feature of our tool is that we can open both STPA and CAST in parallel.

If an accident happens and there is a corresponding STPA analysis, then these resources and information can be reused for the CAST analysis if we integrate it into the DevOps cycle. Initially, we were able to observe the most recent modifications in both the system and STPA through the VCS.

Through this, we might be able to narrow down the range of possible causes, or we can identify more apparent points where the cause of the accident could be lying. If we find the reason for the accident, this artifact, including the recommendations, is consistently stored. In the following steps, the recommendations can be used and checked if the system implements them.

Our tool, together with the DevOps integration, benefits the industry when we consider safety from the beginning of shaping and designing the software. The process will contribute to achieving safety by design because, in every iteration of the software, our safety process will be integrated into the software development process. Furthermore, we want to enrich and improve the collaboration and communication between the software and safety engineers. By using our tool in multiple projects, we can also enable collaboration between them and share knowledge on different projects. Moreover, as emphasized in the STPA and CAST handbooks, it helps with the team's communication and learning, leading to more informed decision-making and improved project outcomes.

This also brings cost and time savings because the system should always be compliant with the defined safety requirements. Furthermore, checking minor changes against the existing STPA analysis and integrating them as the system grows, can speed up the safety checks before the release, resulting in cost savings and accelerating the time-to-market.

From a technical standpoint, we have developed a standalone application that can be utilized on macOS, Windows, and Linux. The application consists of an Angular frontend and a Typescript backend, while we are utilizing RxDB for the database. Furthermore, the components are loosely coupled, allowing us to relocate the backend to a server and use our tool on the web. The team could then examine STPA/CAST in a synchronized manner. The STPA/CAST project file for the current project is being pushed into a Git repository, where the system's other files are also stored. By utilizing this method, the system state and the modifications in the analysis are concurrently tracked. We claim that this aids in maintaining and establishing consistency in larger software projects.

In summary, our tool aims to move forward towards helping software and safety engineers work closer together. We combine the software engineering DevOps principles and safety engineering processes to better bridge them. To extend the support and acceleration for the safety engineers, we will extend the tool with helpful automatizations and helpful patterns. A planned contribution is an automatization to write down UCAs by generating patterns to create them faster. The integration of the context tables by Thomas is a further planned extension. Furthermore, there are plans to enhance the tool's utility for the testing and monitoring phases of the DevOps cycle.

Keywords: STPA; CAST; Tooling; DevOps; Software Engineering.

Session 2: STAMP in Aviation and Air Traffic Control

The STPA Informed Risk Matrix Assessment of Human Controllers in Aviation

Natalia Guskova[1,3], Marek Šudoma[1] and Max Chopart[1]

[1] Department of Air Transport, Czech Technical University in Prague, Prague, Czech Republic

ABSTRACT

The implementation of STAMP-based (Systems-Theoretic Accident Model and Processes) methods for safety analysis in large-scale aviation organizations brings several challenges, particularly transitioning from present risk assessment approaches to systemic ones. The new STPA-Informed Risk Matrix (SIRM) provides a methodology for assessing risks identified with System-Theoretic Process Analysis (STPA). However, the mitigation assessment in SIRM, derived from the MIL-STD-882E does not adequately consider the roles, skills, and responsibilities of personnel in the operations domain. Consequently, the resulting level of risk may be high or serious, despite practitioners' different views or opinions. This research is aimed to find a solution to these practical issues. Research questions are focused on issues related to where SIRM could be applied in the aviation operations and how the description of mitigation effectiveness scores (MES) should be expanded.

STPA was performed and risks assessed using the SIRM across three different aviation entities: aviation maintenance organizations, air traffic procedures related to U-Space operations, and Cessna C172 flight procedures. Then, the roles of key human controllers in these entities were

[3] Corresponding author: guskonat@fd.cvut.cz

evaluated. These included examination of their skills, capabilities, responsibilities, and training.

Our findings revealed that air traffic controllers (ATC), pilots in command (PIC), and mechanics are assessed with a mitigation effectiveness score (MES) of 1 – Training and Procedures, as their roles primarily rely on training and established procedures. However, their actual MES can vary based on their role and capabilities. For some scenarios, their MES can be assessed as 2 - Detected with Response, in other cases, their MES can be assessed as 3 - Reduction Through Design. ATC controllers monitor and proactively control air traffic, and can be assigned MES of 3, as integrating trained ATC personnel into air control systems can proactively reduce and control causal factors through system design. Similarly, PICs can adjust procedures in emergencies, operate reactively by detecting causal factors and responding to occurrences, and can be assigned MES of 2. The MES for mechanics varies based on qualifications and responsibilities. Some may inspect, perform, or supervise maintenance tasks, requiring different licenses and training. Mechanics with basic licenses and minimal training receive MES of 1, as they rely solely on procedures and brief training for task performance. However, mechanics with additional responsibilities, such as type ratings, exhibit a reactive approach, detecting problems and responding accordingly, qualifying for MES of 2. Mechanics becoming certifying staff, qualify for MES of 3, as they are integral part of to the system's proactive problem detection and resolution.

In the research it was demonstrated how the SIRM can be applied in the aviation organizations(entities). To utilise the SIRM to assess risks related to human controllers, it is necessary to reconsider respective mitigation effectiveness scores. They should account for the skills, role, and responsibility of human controllers, as well as assess whether human controller-related risks are mitigated solely by procedures or if human controllers are fully integrated into the system design to proactively mitigate risks. The primary implication of this research is the applicability study of the SIRM in the aviation domain, particularly in operations where human controllers have a substantial influence on safety. The study proposes

solutions to enhance the clarity and applicability of SIRM in real-world operations. These solutions can support the implementation of STAMP-based methods in large-scale organizations. The implementation of SIRM in aviation operations is feasible, and expanding the description of mitigation effectiveness scores can improve the application of STAMP-based methods in practical scenarios.

Keywords: Risk assessment; System-Theoretic Process Analysis; STPA-Informed Risk Matrix; Human controllers; Mitigation effectiveness

An Application of STPA to the Multiple Air Traffic Control Towers

Malakis Stathis[4], Kontogiannis Tom [2]

[1] Air Traffic Control Safety Management Systems Section, Hellenic Aviation Service Provider, Athens, Greece

[2] Cognitive Ergonomics & Industrial Safety Laboratory, Department of Production Engineering & Management, Technical University of Crete, Chania Hellas

ABSTRACT

Changes in the Air Traffic Control domain are made on a continuous basis which poses many research and development challenges to Air Navigation Service Providers. The concept of 'remote provision of aerodrome air traffic services' (commonly known as remote tower operations) enables the provision of aerodrome Air Traffic Control from locations where direct visual observation is not available. Instead, provision of aerodrome ATS is based on a view of the aerodrome and its vicinity through technological means. Multiple Mode of operation is arguably the most demanding element of the Remote Towers concept. Single European Air Traffic Management Research Joint Undertaking (SESAR JU) has published one SESAR Solution related to the multiple mode of operation, with further research underway. Yet no operational implementation of this concept exists, and subsequently operational experience is limited to validation and trial activities. Nevertheless, implementation plans comprising the multiple mode of operation exist among providers within the European Aviation Safety Authorities (EASA) Members States. EASA considers that there is already sufficient information and data available to provide support and guidance to

[4] Corresponding author: phone and email address

facilitate its safe implementation, as well as to provide a basis for further development.

The overarching recommendation about multiple mode operations is that it is to be used only when the operational circumstances allow and when workload and complexity can be managed. It is the responsibility of the Air Navigation Service Providers to define the suitable operational circumstances, which require careful considerations, as well as to provide sufficient evidence for an acceptable level of safety (as is always the case). In this context, we have applied STPA to the concept of multiple Remote Tower operations. The application of STPA turned out to be less costly in terms of time and resources than the traditional methods. STPA identified more hazards and more nuances hazards than SESAR JU had already documented. This fact has significant operational implications for the fielding of multiple remate towers concept.

Keywords: Air Traffic Control; Remote Towers, Multiple Remote Towers, STPA

Performance-based Audit Checklists Using Systemic Approach to Safety

Kateřina Grötschelová[1,5], Andrej Lališ[1] and Natalia Guskova[1]
[1] Department of Air Transport, Czech Technical University in Prague, Czech Republic

ABSTRACT

Audits are one of the essential means of safety assurance. Although used in practice for quite some time, their preparation, execution, and evaluation may pose challenges related to audit effectiveness and efficiency. Authorities in civil aviation and other high-risk industries are currently making a progressive shift from compliance-based to performance-based oversight. This entails many challenges where among the foundational ones lies the issue of establishing effective performance-based checklists to be used when auditing organizations. Compliance-based audits dominate because they are easier to assure and track, while well supported by guidance materials by authorities. Yet, their effectiveness remains an open issue: it is possible that a fully compliant organization may exhibit insufficient safety achievement. This is the point where the need for performance-based audits comes to the fore as they are linked to the actual safety performance. But to have an audit linked with safety performance requires a well-established performance monitoring, which brings many challenges rooted in the understanding of how safety works in practice. Many officials compensate for lack of guidance or clear framework by their own skills and knowledge acquired from previous experience. This, however, leads to a subjective approach making an audit different depending on the audit team. Our research addresses the issue with a systemic approach to safety, namely the System-Theoretic Accident Model and Processes (STAMP). The model is used to infer performance-based audit questions for selected type of aviation organization based on regulatory requirements, extending the compliance-based approach by broader reasoning about safety issues.

System-Theoretic Process Analysis (STPA) was chosen as the core method because it allows safety issues prediction based on system specification. The basis for creating audit questions was the safety control structure. For creating the control structure, regulations and other prescriptive documentation used in compliance-based audits were used. In

[5] Corresponding author: grotskat@fd.cvut.cz

cooperation with the Civil Aviation Authority of the Czech Republic, Easy Access Rules for Aircrew (Regulation (EU) No 1178/2011) was chosen, according to which Authority audits training organizations. Important parts necessary for the application of STPA were highlighted (e.g. roles and processes), and subsequently converted into a graphical form, i.e. into the control structure. Next, all remaining STPA steps were applied. Once the STPA analysis was completed, audit questions were created from its outputs. In our case, the questions were created by a combination of loss scenario-based safety requirements with controller constraints. Loss scenario-based requirements form the basis of the question, and the controller constraints give the necessary context. The developed audit questions were linked to the source requirements. The resulting list of audit questions consists of one main question that defines the scope, followed by a list of detailed questions that focus on how the organization performs a particular activity. Other columns would be added to record answers and potential finings, i.e. whether the organization meets fully, partially, or does not meet the respective requirement.

Audit questions based on the STPA serve more the purpose of the performance-based audits, addressing questions like How does it work?, Have you ever done an activity differently and why? or asking for practical examples etc. In addition, connecting a newly created audit checklist with a specific documentation gives the authority the possibility to combine compliance-based and performance-based questions. The questions are structured so that the auditor can ask in a given order according to the documentation and, at the same, time the questions are linked thus forming an organized structure. The new audit checklist was tested during a routine audit of the Civil Aviation Authority of the Czech Republic. STAMP-based audit questions and conclusions were compared with those of the Authority. The conclusions were found consistent and at the same time, it was found that even a person who has limited experience with auditing the given area would be able to ask and assess the organization with the proposed checklist.

The results showed that the questions are well usable within the performance-based audits and correspond to the questions asked by experienced auditors for the given audited area. A limitation of creating STAMP-based audit questions is that the systemic approach is currently not used in aviation state safety oversight, so authorities may initially have a problem with training their employees. Also, the validation process of the checklist was limited, as it was only tested on a few cases. For better validation, it is advisable to validate the checklist through several audits in

different organizations. In addition, it will be necessary to further focus on the part of the checklist that deals with the recording of the answers and their assessment. Our evaluation showed that for the needs of performance-based audit, the current form using meets fully, partially, or does not meet categories is insufficient for the purpose. Especially important is to focus on the meets partially category, because it may include both small findings that need to be corrected and more significant findings.

Our result will contribute to supporting auditors in executing performance-based audits. It will help them to understand the processes of the organization and can be supportive in the assessment of the audit. STPA brings a new, systemic perspective to the state safety oversight process which can help to better explain some of the state safety oversight issues.

Keywords: Aviation safety; Performance-based audit; State safety oversight; System-Theoretic Accident Model and Processes; System-Theoretic Process Analysis.

Session 3: STAMP in Practice and Validation

Beginning the Journey of Adopting STAMP in practice (STPA or CAST)

Meaghan O'Neil[1][6],

[1] Director (System Design and Strategy Ltd, UK)

ABSTRACT

Systems Theoretic Process Analysis (STPA) is a hazard identification and analysis approach. It is based on the Systems-Theoretic Accident Model and Process (STAMP) causality model which is founded in systems engineering principles and system control theory. The Causal Analysis using System Theory (CAST) is also based on the same foundation theory. Numerous tutorials and references are available to guide new practitioners to learn the basics STPA and CAST. Whilst learning the basic techniques in a tutorial or classroom environment begins the learning journey – for many, the process of successfully adopting the techniques into practice of system design or improvement can be challenging. This presentation will present common challenges as well as recommendations for new adoption of STAMP accumulated over 10 years of practitioner's experience with CAST and STPA.

Keywords: STAMP, CAST, STPA, adoption, engineering practice

[6] Moneil@systemdesignstrategy.co.uk

Validating applications of the system theoretic process analysis technique for regulatory approval of Maritime Autonomous Surface Ships: Recent developments and future research directions

Floris Goerlandt[1,7], Valtteri Laine [2]

[1] Department of Industrial Engineering, Dalhousie University, Halifax, NS, Canada

[2] Department of Mechanical Engineering, Marine Technology, Aalto University, Espoo, Finland

ABSTRACT

Maritime Autonomous Surface Ships (MASS), covering a variety of automated functions for ship operation, are fast becoming a reality in various application contexts. Under the purview of the Maritime Safety Committee (MSC) of the International Maritime Organization (IMO), work is currently ongoing to develop a non-mandatory MASS Code. Taking a goal-based approach, building on functional requirements for the automated functions of MASS, this Code aims to be a key regulatory vehicle through which vessel designs with MASS functions will obtain regulatory approval. While still under development, risk assessment is likely to be a central feature of this Code, and it is considered that systemic failures related to human and technical controls are of key importance to identify and mitigate. To achieve this, the system theoretic process analysis (STPA) technique has been proposed for hazard analysis in a section on risk assessment of the draft Code. An important issue for regulatory approval of hazard analyses and risk assessments is whether these are valid, in the sense that the results are comprehensive, accurate, and credible. The need for maritime authorities to be able to assess the quality of hazard and risk assessments is readily

[7] Corresponding author: floris.goerlandt@dal.ca

understandable, as potential losses due to non-identified hazards of poorly executed risk assessments can lead to major consequences in terms of loss of human life, environmental damage, and economic costs. Nevertheless, this issue of the validity of STPA-based hazard analyses has not yet received much explicit attention in the academic literature, in industrial applications, or in regulatory development work towards the MASS Code. In this work, recent academic work proposing a validation framework for an STPA analysis is presented. The framework, still under development, is based on theoretical notions of validation concepts in the pertinent literature on risk science, social science, and operations research, systems dynamics, and simulation modelling disciplines. It takes a formative approach to validation, i.e. the validation process aims to improve the analysis through a (possibly iterative) interactive interplay between analysts and a review team, rather than summatively declaring the analysis of a certain quality level. To achieve this, each execution step of an STPA analysis (purpose of the analysis, control structure, Unsafe Control Actions, loss scenarios, and documenting results) is accompanied with a set of tests, which are operationalized through a series of guide questions to focus on specific aspects of the analysis. Results of a further study investigating the reasonableness of the proposed theory-based validation framework as judged by STPA users confirms that most tests are believed to be useful in practice, and that the approach of using guide questions is suitable, although several interviewees recommended to provide further clarity for some guide questions. Finally, directions for future research to test the effectiveness of the validation framework are outlined, as it is considered important to ascertain that applying the framework serves its purpose.

Keywords: Maritime Autonomous Surface Ships (MASS), systems theoretic process analysis (STPA), Systems theory, Validation, MASS Code

STPA for Contextualizing Test and Evaluation Planning of Machine-Learning Enabled Systems

Edgar W. Jatho, III[1,8], Logan O. Mailloux[2], Eugene Williams[2], Patrick McClure[2], and Joshua A. Kroll[2,*]

[1] U.S. Naval Academy (Computer Science Department, USA)

[2] Naval Postgraduate School (Computer Science Department, USA)

ABSTRACT

Traditional modalities of test, evaluation, and assurance break down for systems based on machine learning (ML) for the implementation of controllers. ML provides the input-to-output function for complex controllers through imputation, not specifying specific component behaviors but rather criteria such as training data and optimization parameters. This poses two challenges for testing and assurance: first, because the imputed control function is not concisely described, it can be difficult to bound testing efforts or generate a sufficient set of test cases, especially in composed systems. Second, because ML-derived functions are imputed rather than specified by chosen behaviors, once hazards are identified, avoiding them presents new challenges. In high-stakes applications, these general assurance challenges reinforce concerns of unintended social harms or ethical violations in the use of systems that have ML-derived components. The complex outcomes of ML systems often emerge after deployment: over time, across populations, and through interactions between models, system components, and their environments. STPA provides a useful and coherent framework to relate ML component behaviors to system-level hazards, capturing requirements for ML engineering and test plans including acceptance criteria for delivered models, overcoming these twin challenges by tying component properties and behaviors to contextual hazards and use-driven safety criteria. We offer several case examples applying STPA to ML-enabled systems demonstrating the translation from identified system-level hazards to actionable requirements development, test planning, and use-case enabled system assessment. Our case examples range from risk-score-aided decision-making (in the context of managing the abuse of controlled

[8] Edgar W. Jatho: jatho@usna.edu

[*] Joshua A. Kroll: jkroll@nps.edu

pharmeceuticals) to governing the support of law enforcement investigation based on biometric evidence (facial recognition as a tool for law enforcement prioritization of investigative leads) to the relationship between levels of human oversight and degrees of autonomy in perception-to-action loops from systems which support human decision-making (e.g., classification of objects in persistent perception-oriented systems such as passive sonar) to highly autonomous applications (e.g., supervisory control of navigation in an uncrewed surface vessel).

Traditional work on ML assessment focuses on properties of the ML-derived functions themselves: predictive performance, robustness to input perturbation or covariate shift, the quantification of uncertainty over choice of model or available data, reproducibility either of specific model behaviors or of decisions driven by model outputs. However, these model-intrinsic measures are insufficient to provide assurance as they do not answer the challenges of testing sufficiency or of hazard avoidance and risk mitigation. Especially as new requirements to test and manage these systems come online, such as the conformity assessments soon to be required at law under the European Union's AI Act and comparable laws under development in many other jurisdictions, it is critical to develop the capacity to test, evaluate, and assure systems that include ML-derived components. Instead, assurance must be contextual and extrinsic, situating models in larger systems to identify and mitigate hazards. The state-of-the-art in this domain relies on ad-hoc composition of model-intrinsic evaluation measures to develop model-driven assurance arguments. These component-based arguments often prove insufficient, missing issues that arise during system employment. Simultaneously, ad-hoc top-down review of system-level performance can, with substantial effort, identify hazards based on use cases, but struggle to tie these back to actionable decision-making at the component implementation or system design levels.

Consider one of our example use cases: facial recognition in a criminal justice context. Arguments in favor of the suitability of such tools generally rely on component-based performance measures: overall accuracy, stratified accuracy by demographic group, differential performance in common use-driven scenarios (e.g., error rates under conditions of partial face occlusion; varying camera angle, lighting, or facial expression; differing camera resolutions or focal distances), likelihood that the correct identification occurs in the top-*k* matches, etc. Simultaneously, criticisms of these tools rely on anecdotal or scenario-based failure descriptions of the composed system: misidentification leading in particular cases or structurally to ungrounded law enforcement activities, up to and including the detention of suspected criminals based on automated facial matching. However, neither line of evaluation provides actionable technical decision-making for considerations even as simple as setting the decision threshold between a match and a non-match given a probe facial photograph and a background database of identified images. Using STPA, we demonstrate how to develop implementable assessment plans to close this gap, linking hazards in the composed system (e.g., representativeness of the background database for the query population) to requirements on system design, component performance, and acceptance tests (e.g., a system is suitable for referring matches for law-enforcement follow-up when its false match rate is low enough that officer training is sufficient to prevent ungrounded detention, coupled with the design requirement that officers be provided the matched background database photo for human comparison). Our analysis recovers many known hazards, subsuming prior failure analysis into straightforward design-level exercises yielding system requirements and test plans based on measures of effectiveness, performance, and suitability given requirements and use cases.

Connecting system-level failures to actionable development and evaluation requirements presents a novel approach to assessing social and ethical risks from high-consequence systems with ML-derived components. A similar gap exists around these risks: the state of the art in risk evaluation and management relies either on component-level assessment (e.g., measurements of data bias; metrics for balance in allocation of classification outcomes or error rates across implicated subgroups of the population; functional requirements around the representation of traditionally subordinated minority subpopulations; etc.), which struggle with composition of components into systems as well as in validating assumptions, or on high-level impact assessments, which document risks without providing paths to engineering improvements or criteria for system acceptance. Throughout our STPA cases, we consider how our findings can organize component-level assessment so that it responds to concerns of

social harms or risk of unethical use by modeling these failure modes as losses and identifying hazard scenarios which prefigure them. Introducing controls or redesigning systems to avoid these hazards then reveals effective methods for foreseeing and mitigating socially consequential risks in addition to traditional assurance.

From a series of four pilot applications of STPA to systems with ML-derived components, we find that STPA provides a useful framework for connecting use-case concerns (including social and ethical risks) back to requirements on system design and concrete test and evaluation planning, including the development of acceptance criteria that define both system design and component properties. STPA is an effective developmental testing tool for ML-enabled systems, providing foresight linking traditional model-intrinsic performance properties to system-level assurance needs. This connection between low-level component assessment and performance in the context of use sidesteps key difficulties in the assurance of ML-enabled systems: the inability to determine the sufficiency of test case plans, and the difficulty of introducing offsetting control once hazards have been identified via analysis or experience. Our work can inform the development of assurance and assessment standards for ML-enabled systems, such as emerging requirements for conformity assessment of “high risk” systems under new legal regimes around the world.

Keywords: Machine Learning; Test & Evaluation; Social & Ethical Risk; Contextual Evaluation; Developmental Test Planning

Session 4: STAMP in Transportation and Autonomous Systems

A systemic safety analysis to manage eVTOL vehicles at vertiports in different life cycle stages

Elena Stefana[1,9], Manuel Lombardi[1] and Riccardo Patriarca[1]

[1] Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Rome, Italy

Context

Advanced Air Mobility (AAM) vehicles, e.g., Vertical Take-Off and Landing (VTOL) and electric Vertical Take-Off and Landing (eVTOL) aircraft, are expected to be soon integrated in the current transportation systems across cities. Accordingly, their operations should be safely conducted and integrated into air and ground infrastructures, e.g., vertiports located on land, water, or structure for aircraft landing, take-off, and movement (FAA, 2022). Such integrated system represents a system of systems characterised by continuous interactions within the existing rule and regulation framework (Stanton et al., 2019). This calls for the adoption of a systemic perspective for safety risk management. In this domain, Systems Theoretic Accident Modelling and Processes (STAMP) and its nested techniques permit considering safety as a continuous control task managed by a control structure embedded in an adaptive socio-technical system (Leveson, 2004). Some scientific studies leverage on STAMP and/or its related techniques, i.e., System-Theoretic Process Analysis (STPA) and Causal Analysis based on System Theory (CAST), for the safety management of AAM systems and eVTOL vehicles (e.g., Markov et al., 2022). Additionally, some research has been conducted to assess the risks associated with the operations of eVTOL vehicles at a vertiport located inside an airport (Stefana et al., 2024). However, these studies mainly focus on a specific stage of the system life cycle for identifying effective safety recommendations, missing the potentialities emerging from the integration of these approaches across the

[9] Corresponding author: elena.stefana@uniroma1.it

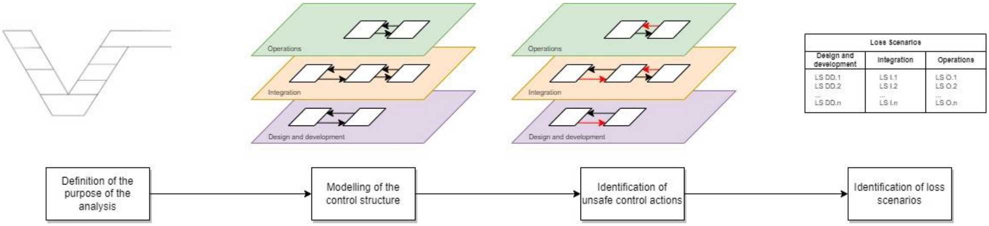
entire engineering process. Vertiports exemplify an ideal system for integrated assessment, due to their recent emergence and inherent complexity.

Objective

This study aims to perform a systemic analysis for assuring a holistic safety management of eVTOL vehicles at vertiports, which are expected to be located inside airports, throughout the different stages of their engineering process. This process comprises the following system phases: (i) design and development (including the concept development and requirements engineering), (ii) integration (i.e., localisation of the vertiport within a geographical area), and (iii) operations (including maintenance). The proposed approach has the objective to support decision-makers in generating relevant requirements and safety management plans, in addition to design and develop usable systems compliant with stakeholder needs (Leveson & Thomas, 2018).

Methodology

To achieve such objective, we employ the STPA technique (Figure 1), derived from STAMP. We clearly delineate the system engineering process: for each of its phases, we modelled a specific control structure, and identified Unsafe Control Actions (UCAs) and loss scenarios.


Operations
Integration
Design and development
Operations
Integration
Design and development
Definition of the purpose of the analysis
Modelling of the control structure
Identification of unsafe control actions
Identification of loss scenarios

Loss Scenarios		
Design and development	Integration	Operations
LS DD.1 LS DD.2 ... LS DD.n	LS I.1 LS I.2 ... LS I.n	LS O.1 LS O.2 ... LS O.n

Figure 1: STPA in the engineering process, across different life cycle stages

Results

1. Definition of the purpose of the analysis: We considered the set of regulations and rules currently available for eVTOL vehicles and vertiport infrastructures. For instance, European Aviation Safety Agency (EASA) recently published means of compliance for AAM and VTOL missions (EASA, 2023). We identified losses and system-level hazards for each phase of the system engineering process. Relevant losses include loss of life or injury to people, loss of or damage to infrastructure, loss of mission, loss of customers, and loss of vertiport performance. They can be caused by different hazards: e.g., vertiport is not properly designed, vertiport is not located in an effective position, eVTOL is no longer airworthy. To analyse these hazards, we built the control structure of the system.
2. Modelling of the control structure: An excerpt of the control structures for the engineering phases are reported in Figure 2, where similar controllers are identified by boxes of the same colour. Such control structures highlight that several controllers / controlled processes have a different role according to the investigated phase. For instance, Air Navigation Service Provider, Airport Air Traffic Control, Pilot In Command, and eVTOL have interactions within the system only during the operations phase. Note that in these control structures, International Civil Aviation Organization, EASA, and Civil Aviation Authority are not explicitly indicated although they are controllers / controlled processes in each phase.

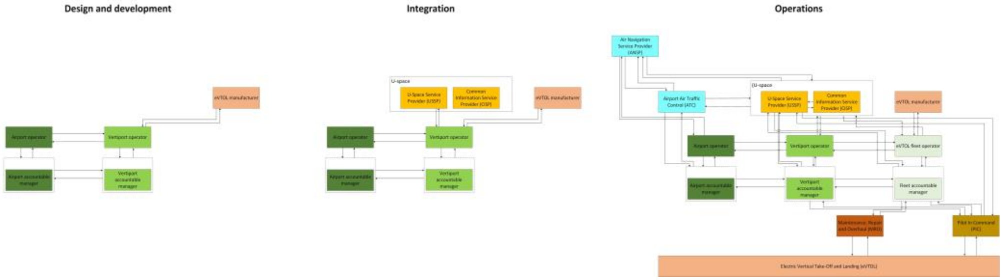

Design and development
eVTOL manufacturer
Airport operator
Vertiport operator
Airport accountable manager
Vertiport accountable manager
Integration
U-space
U-Space Service Provider (USSP)
Common Information Service Provider (CISP)
eVTOL manufacturer
Airport operator
Vertiport operator
Airport accountable manager
Vertiport accountable manager
Operations
Air Navigation Service Provider (ANSP)
Airport Air Traffic Control (ATC)
U-space
U-Space Service Provider (USSP)
Common Information Service Provider (CISP)
eVTOL manufacturer
Airport operator
Vertiport operator
eVTOL fleet operator
Airport accountable manager
Vertiport accountable manager
Fleet accountable manager
Maintenance, Repair and Overhaul (MRO)
Pilot In Command (PIC)
Electric Vertical Take-Off and Landing (eVTOL)

Figure 2: Excerpt of the SCS in the three life cycle stages

3. Identification of UCAs: For each hazard and each engineering process phase, we identified various UCAs that could occur because the control action (i) is not provided, (ii) is provided, (iii) is provided too late, or (iv) is applied too long or is stopped too soon. For example, control actions between the vertiport operator and airport operator could become unsafe if: (a) documentation and data for the integration are not shared or are shared too late, (b) capacity limitations and flight planning are not provided and communicated, or (c) adequate equipment and services are not available or are not made available in the airport.
4. Identification of loss scenarios: The UCAs can be caused by different loss scenarios, spanning from the design and development to the use of the system. They could be related to unsafe controller behaviours, feedback paths, control paths, or controlled process behaviours. This process makes recognise the need of adopting various safety recommendations and integration requirements to improve the safety management of eVTOL vehicles at vertiports throughout the entire engineering process. In this regard, (e.g.), vertiport and airport operators should be informed in advance and in a timely manner about the technical specifications and parameters required for the integration of these infrastructures and the planning operations.

Practical implications

In the literature, some recent contributions integrate systemic approaches into system engineering processes. Abdulkhaleq et al. (2015) present a safety engineering approach based on STPA to develop safe software, Valdez Banda & Goerlandt (2018) propose a safety system engineering process for designing Safety Management Systems based on STAMP, Span et al. (2018) describe a tailored version of the STPA approach for Security (STPA-Sec) to analyse requirements of complex cyber-physical systems, and Mailloux et al. (2019) apply STPA-Sec for the development of secure systems by eliciting systems security requirements for a notional autonomous space system. In the aviation domain, only Scarinci et al. (2019) adopt STPA for requirement generation for complex and highly integrated aircraft systems.

Our study represents a first attempt to integrate STPA into the engineering process of AAM systems and, specifically, the safety management of eVTOL

vehicles at vertiports. This allows a proactive analysis associated with hazards and risks, and supporting the design of these complex systems that are currently under development and cannot rely on accurate historical data. The idea to develop an integrated analysis, rather than a simply set of three complementary iterations of the analysis, is relevant as it allows providing larger insights into operations early in the design stages. As such, it is expected that the outcomes of this methodology remain useful for both designers and operators, as well as for authorities, who could implement the outcomes of such analyses into improved guidelines and specifications. Finally, such a framework integrating STPA into the system engineering process also gives insights into the effectiveness of adopting safety requirements in specific life cycle stages.

Keywords: Safety risk assessment; V-model; Next-generation green aircraft; Urban Air Mobility; Integration requirement.

References

Abdulkhaleq A., Wagner S., Leveson N. (2015). A Comprehensive Safety Engineering Approach for Software-Intensive Systems Based on STPA. *Procedia Engineering*, *128*, 2–11.

EASA (2023). *Fourth Publication of Proposed Means of Compliance with the Special Condition VTOL*.

FAA (2022). *Engineering Brief No. 105 - Vertiport Design*.

Leveson N. (2004). A new accident model for engineering safer systems. *Safety Science*, *42*(4), 237–270.

Leveson N.G., Thomas J.P. (2018). *STPA Handbook*.

Mailloux L.O., Span M.Lt., Mills R.F., Young W.Lb. (2019). A top down approach for eliciting systems security requirements for a notional autonomous space system. *SysCon 2019 - 13th Annual IEEE International Systems Conference, Proceedings*.

Markov A., Bendarkar M., Mavris D. (2022). Improved hazard analysis for novel vehicle configurations using the systems-theoretic process analysis. *AIAA Science and Technology Forum and Exposition, AIAA SciTech Forum 2022*.

Scarinci A., Quilici A., Ribeiro D., Oliveira F., Patrick D., Leveson N.G. (2019). Requirement generation for highly integrated aircraft systems through STPA: An application. *Journal of Aerospace Information Systems*, *16*(1), 9–21.

Span M.T., Mailloux L.O., Grimaila M.R., Young W.B. (2018). A Systems Security Approach for Requirements Analysis of Complex Cyber-Physical Systems. *2018 International Conference on Cyber Security and Protection of Digital Services, Cyber Security 2018*, 1–8.

Stanton N.A., Li W.C., Harris D. (2019). Editorial: Ergonomics and Human Factors in Aviation. *Ergonomics*, *62*(2), 131–137.

Stefana E., Guskova N., Di Gravio G., Patriarca R. (2024). Should I board this Advanced Air Mobility vehicle? A systemic risk assessment of eVTOL in a vertiport. *15th International Conference on Applied Human Factors and Ergonomics (AHFE 2024)*. Forthcoming.

Valdez Banda O.A., Goerlandt F. (2018). A STAMP-based approach for designing maritime safety management systems. *Safety Science*, *109*(June), 109–129.

Acknowledgement

This work is part of the research activities developed by the authors within the framework of PNRR: CN4 “Sustainable Mobility Center” - SPOKE 1 “Air Mobility” - CN_00000023 - CUP B83C22002900007 (E.S., R.P.), and PhD in Industrial and Management Engineering - CUP B53C23002500006 (M.L.).

Lessons Learned from Applying STPA to ADS

Pavel Nedvědický*, Eva Zimmermann and Stefan Wagner

* Corresponding author: pavel.nedvedicky@gmail.com
Technical University of Munich, Germany

ABSTRACT

Safety analysis is a critical aspect of designing and implementing complex systems, particularly in domains like autonomous driving, where failures can have significant consequences. Rigorous analysis and mitigation of potential hazards are required to ensure the safety of such systems. In this context, STPA emerges as a valuable technique for systematically identifying unsafe control actions and their underlying causal factors. In this extended abstract, we present findings and lessons learned from a research project aimed at providing processes, methods, and tools for safe development in the automotive industry, particularly in the context of software-defined vehicles. The research project involves the collaboration of multiple academic and industrial partners working together on a development process proposal, which will also include the application of STPA in relevant stages. We decided to incorporate STPA into the process because it is a well-established hazard analysis technique tailored for the analysis of complex systems, for which it is capable of revealing critical issues that might otherwise remain unnoticed.

To validate the approaches that we propose in the project, we employ an autonomous driving system (ADS) as a demonstrator. As vehicles operate in an open world where they encounter countless possible situations, autonomous driving technology is deployed in incremental steps, with capabilities continually enhanced through frequent updates. To mirror this development strategy, we created a virtual prototype of an extension to the existing ADS. This extension enriches the ADS functionality by enabling autonomous navigation through construction zones. Previously, when encountering such scenarios, the driver was requested to take over the control of the vehicle. After the deployment, the ADS will be able to navigate through predefined types of construction zones in specified conditions, such as weather, road type, and speed restrictions.

We applied STPA during the system development to address the safety concerns and shape the system design. One of the STPA benefits is the possibility to apply it from the early development stages and use it proactively to consider safety throughout the development cycle. Once the functionality of the system, including requirements and architecture, has been defined, we could initiate STPA. Our objective was to analyze the system from a safety perspective to uncover potential hazards and vulnerabilities. STPA is conducted in four steps, and we followed STPA handbook to guide us through the analysis. Additionally, we employed various other recommendations present in the scientific literature to further improve the analysis. During the application of STPA, we encountered several advantages and benefits, along with some pitfalls and challenges. These insights arose from both the analysis itself and its integration into the overall development process. Our hands-on experience resulted in valuable lessons learned that can improve future practical applications of STPA. Below, we highlight the most significant lessons learned.

First, we learned the importance of interdisciplinary collaboration among experts, which is crucial for gaining a holistic understanding of system safety. The involvement of partners from academia and industry, each with unique expertise from different backgrounds, provided multiple perspectives on the system. The communication included both formal channels via artifacts sharing and informal during meetings and email exchanges. The combination of different knowledge contributes to achieving a more complete analysis. Second, we learned the value of early safety considerations. By integrating STPA in the early stages of system development, we were able to proactively identify and address hazards. This proactive approach resulted in a more effective development process by avoiding costly rework and redesign. Another key lesson learned was the importance of iterative refinement. Throughout the STPA process, we continuously refined our analysis based on exchanges with other experts and their feedback. This allowed us to provide more detailed and complete safety recommendations by incorporating the evolving knowledge about the system into the analysis. It has proven worthy to start with the analysis at a high level of abstraction and continuously detail it. Furthermore, we learned the importance of using complementary tools and techniques to enhance the effectiveness of our analysis. Among others, this is necessary to achieve compliance of STPA with the relevant safety standards. In the automotive industry, these include ISO 26262 for functional safety and ISO 21448 for safety of the intended functionality (SOTIF).

In conclusion, the application of STPA to our system has demonstrated its value in ensuring safety and guiding development. However, a smooth alignment of STPA with other activities is necessary for its successful integration into the development lifecycle. Therefore, in this extended abstract, we share our experiences and insights gained from applying STPA to illustrate how it contributed to a more in-depth understanding of system safety. Our findings highlight the importance of interdisciplinary collaboration and early safety considerations in achieving robust development processes. These insights offer guidance for future applications of STPA, enhancing system safety but also optimizing the development process, ultimately contributing to the creation of safer, more reliable systems across domains.

Keywords: STPA; Automotive; ADS; Lessons Learned; Practical Experience.

Standardizing STPA Analysis using RAAML: Applied to Ship Remote Pilotage Operation

Sunil Basnet[1,10], Raheleh Faroukhi[1] and Osiris Alejandro Valdez Banda[1]

[1] Aalto University, Research group on Safe and Efficient Marine and Ship Systems, Finland

ABSTRACT

The advancement of remote pilotage operations, exemplified by a recent successful demonstration in Finland, marks a shift towards increased efficiency and reduced operational costs in maritime navigation. However, the introduction of new technologies and procedures introduces emergent risks that must be identified and managed. While maritime researchers increasingly propose System-Theoretic Process Analysis (STPA) as a promising method for identifying these risks, the lack of standardization in STPA results leads to inconsistencies and ambiguities. Therefore, adopting a standardized modeling approach for STPA is essential for effectively identifying and presenting risks in complex operations such as remote pilotage.

This study explores the use of the Risk Analysis and Assessment Modeling Language (RAAML) to conduct an STPA of remote pilotage operations. RAAML provides standardized notations and semantics, significantly enhancing the traceability and clarity of the safety analysis process. By using RAAML, the analysis identifies loss scenarios related to remote pilotage operations and presents diagrams for communicating the results. The findings indicate that adopting RAAML not only standardizes the hazard analysis process but also facilitates iterative updates and integration with other analytical tools. These advancements underscore the potential for improved safety and operational efficiency in remote pilotage, advocating for the broader implementation of standardized languages in complex system analyses.

Keywords: STPA; RAAML; Remote pilotage; Hazard Identification; MBSE

[10] sunil.basnet@aalto.fi

Session 5: STAMP in Information and Cyber Security

Using STAMP to Influence Information Security Policies in Radiation Therapy

Natalia Silvis-Cividjian (Vrije Universiteit Amsterdam, The Netherlands), Donia Macdonald (Eastern Health, Canada), Greg Salomons (King George Hospital, Canada), Brendan McClean (Saint Luke's Hospital, Ireland)

ABSTRACT

Up to now, we successfully used STAMP to analyze and prevent safety incidents in radiation therapy (RT) and on our university campus, which are places where people come to work with the best intentions. Unfortunately in the last years, both universities and RT information systems worldwide were the target of various disruptive security attacks that led to loss of connectivity, data ownership, financial resources as ransom payments and the worse, delays in cancer patient treatment. This means that we have to extend our analysis to include bad-intentioned, malicious users.
This is a work in progress. We will describe in this presentation (1) how we applied STAMP-CAST to learn from recent security incidents which affected universities and RT departments worldwide, and (2) how we used STAMP-STPA-Sec to issue recommendations towards the information management policy makers, aiming to improve the security robustness in these two types of large organisations.

Keywords: computer networks security, STPA/CAST, information management systems, university, radiation therapy

Knowledge graphs to convert large Safety Control Structures of modern industrial establishments

Antonio Javier Nakhal Akel[1,11], Francesco Simone[1], Elena Stefana[1] and Riccardo Patriarca[1]

[1]Department of Mechanical and Aerospace Engineering,
Sapienza University of Rome (Italy)

Purpose

The industrial and societal landscape is rapidly changing due to technological advances and rise of automation, as well as globalization at different scales. Modern industrial establishments are complex systems, where the interactions and synergies among organizational, human, and technical elements are easily recognized (Pasman, 2009). They are labelled as Socio-Technical Systems (STSs), being characterized by a high number of elements tightly interacting, which make them complex and prone to unexpected variability and highly interdependent behaviours (Dekker et al., 2011). In such a context, the modern industrial systems demand for a paramount concern on safety. Such concern is particularly evident for all the establishments involved in the storing, handling, production, and use of dangerous substances (the so-called Seveso establishments). These latter have the potential to lead to major accidents with severe consequences on equipment and moreover on the population and the plant's surrounding environment. The European Union ruled on the management of these plants through the European Directive 2012/18/EU (i.e., latest version of the European Directive 82/501/EEC). Accordingly, operators of Seveso establishments must adopt effective strategies to prevent major accidents and mitigate their consequences for human health, economic, and environmental damages.

The management and control of Seveso establishments is a complicated and intricate process, in which several agents exchange a large amount of information, and their decisions influence the whole industrial eco-system.

For this purpose, the Systems Theoretic Accident Model and Processes (STAMP) model represents a suitable alternative to support the management of such establishments considering its foundation in control theory and

[11]Corresponding author: antonio.nakhal@uniroma1.it

models in the hierarchical Safety Control Structure (SCS), where the system agents are identified and interactions between them becomes evident.

While the value of STAMP and its nested techniques has been largely proven in literature (Patriarca et al., 2022), a limitation arises when modelling large complex STSs since the resulting SCSs become too complicated to gain useful insights (Nakhal A. et al., 2023). This research presents a possible solution via the adopting of Knowledge Graphs (KGs), meant to be an extension to the SCS development.

Methods

The proposed approach is designed to reproduce the SCS of the STS within a representation of knowledge in the form of a KG. The KG is constructed to foster the navigation of the SCS, via a semantic reasoning. Additionally, the same KG constitutes a knowledge base for any further investigation, i.e. STPA for prospective analyses, or CAST for retrospective cases. The method proposed here is contextualized with respect to Seveso establishments, with a model of the European Directive 2012/18/EU.

The STAMP model has been developed after a thorough analysis of documentation, and it has been enriched with experience derived from a pool of subject matter experts involved in interviews and focus groups with the ultimate purpose of assessing the significance of the resulting SCS. This latter has been translated into a KG using an ad-hoc ontology model (Simone et al., 2023), which provides formal specifications of concepts and relationships within the KG, defining categories, properties, and relationships. Then, the knowledge representation structures data into entities and relationships, and thus facilitates the analysis of complex systems. **Figure 1** depicts a conceptual representation of the conversion process.

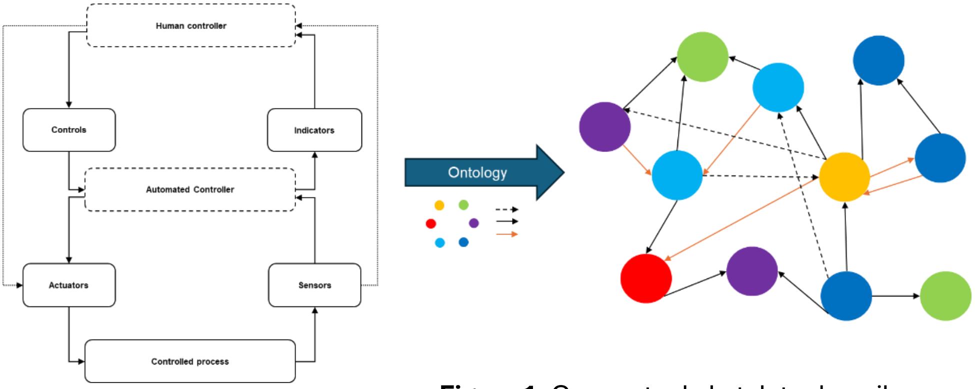


Figure 1. Conceptual sketch to describe the conversion of a SCS into a KG.

Results

The SCS developed for the research considers different agents, spanning from European Commission to the operators in an exemplary industrial facility. The analysis aims to identify critical agents and highlight mutual interactions among them. The development of STPA is considered here out of scope. For demonstration purpose, **Figure 2** shows an excerpt of the case study SCS, via the interactions from the "Operation manager" of a Seveso industrial establishment down to a physical equipment, e.g., "Vessel".

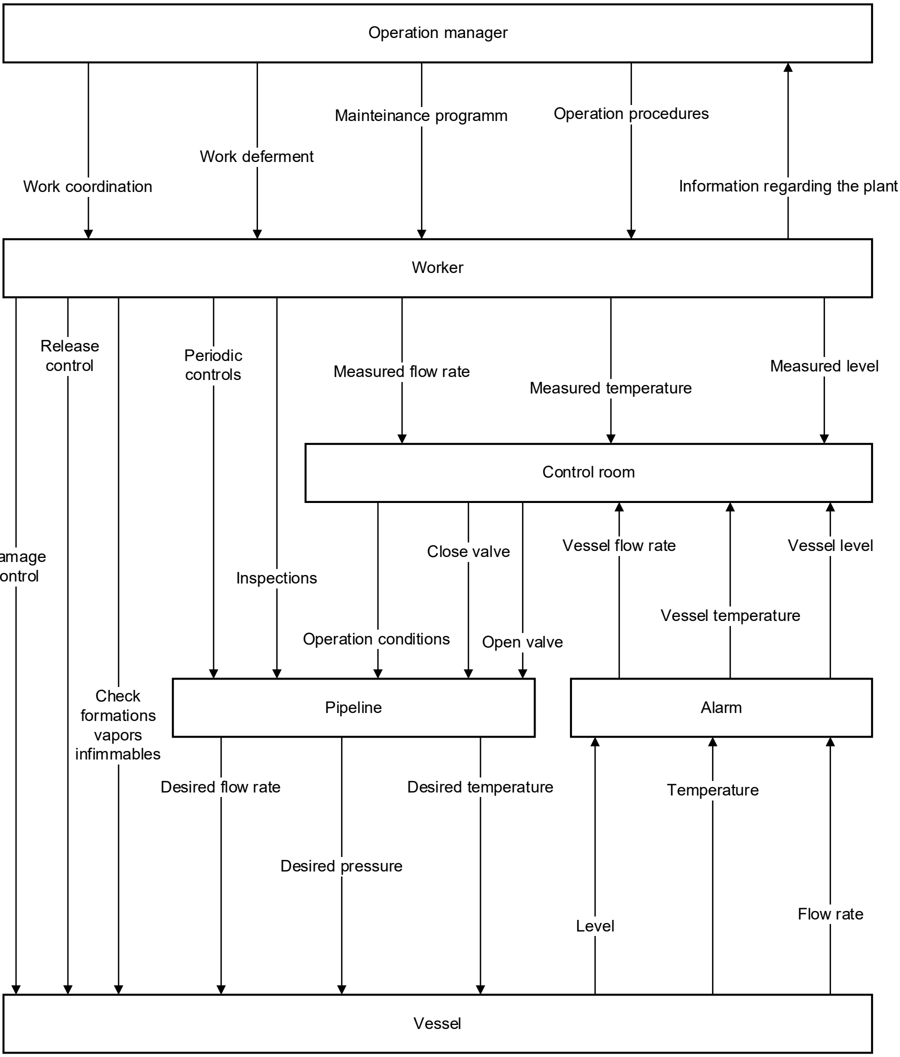


Figure 2. Excerpt of the SCS in the use case, relevant for Seveso establishments in line with the European Directive 2012/18/EU.

This excerpt is used as an example to show the potential of the model for mapping the system elements and their interactions. Therefore, **Figure 2** depicts the following interactions among: (i) the "Operation manager" responsible for setting and complying with the technical-operational requirements of the process; (ii) a “Worker” of the establishment in charge to develop all the manual activities to monitor or control the process; (iii) the "Control room" in charge to control the process; (iv) the "Pipeline" of the plant that fills up the (v) "Vessel"; and (vi) the "Alarm" to notify the parameters of a vessel status Vessel to the control room. These system components are a subset of a bigger model mapping the Safety Management System of a refinery.

The SCS (**Figure 2**) is then processed to tag each element (blocks and arrows) with an ontology and to obtain Resource Description Framework (RDF) data in a table with the following fields:

- From_node_label: label assigned to the node from which an edge starts;
- From_node_value: information in blocks and arrows of the SCS related to nodes from which an edge starts;
- Relationship_label: label of an edge connecting two nodes;
- To_node_label: label assigned to the node to which an edge ends;
- To_node_value: information in blocks and arrows of the SCS related to nodes to which an edge ends.

The resulting graph for the SCS (**Figure 2**) is represented in **Figure 3**. The KG representation of the SCS enables the navigation into the intricate interactions among the system elements presented in the STAMP model. Furthermore, this KG allows for quantitative analyses based on the fundamental principles of network theory and its associated metrics. For instance, this analysis can highlight potential communication paths informing about a specific status of any controlled process node, or paths leading to the execution of a process action of any controller node. In addition, it is possible to calculate network metrics (e.g., betweenness, closeness, etc.) to identify the most associated nodes in the system or the gaps in the system. Moreover, this type of representation has the potential to be updated with real-time process data, serving as a Digital Twin of the system itself. This model allows continuously monitoring the process in a system theoretic perspective, enhancing the safety management of the STS.

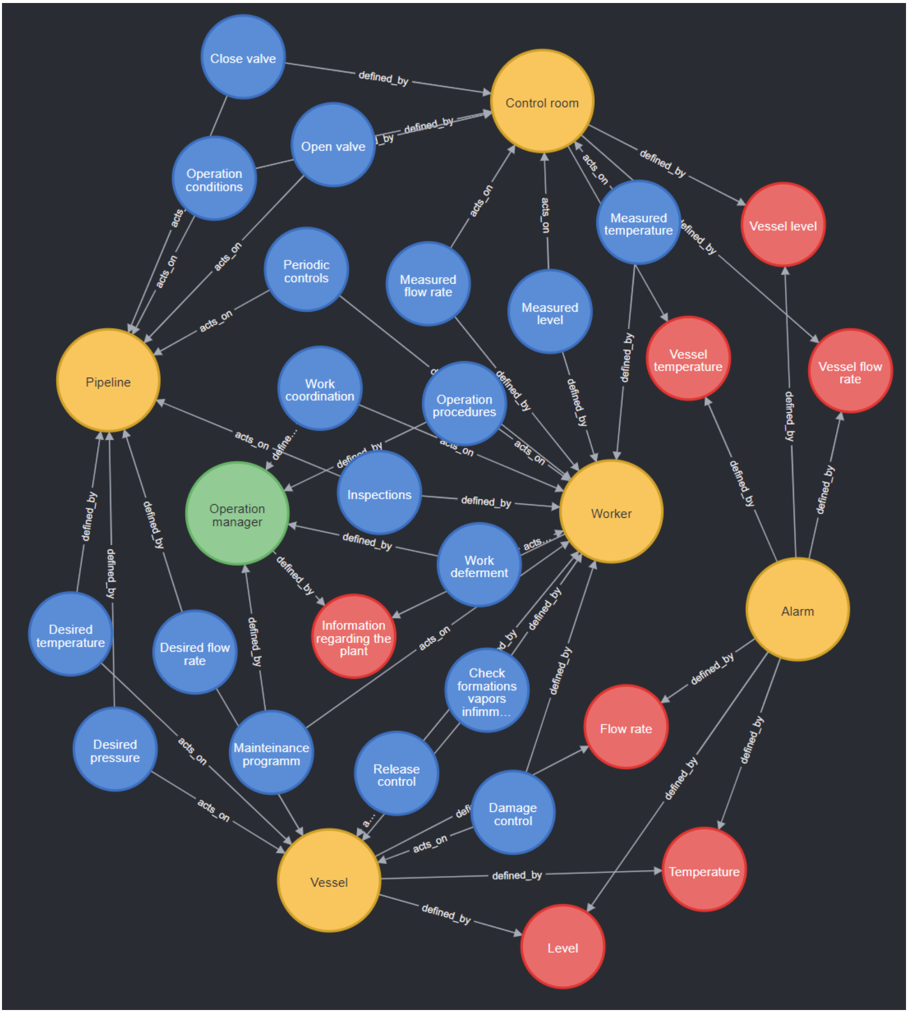


Figure 3. KG representation of the SCS.

Conclusions and implications

This investigation introduces a methodology that combines the principles of system theory to analyse interactions within systems and to translate them into a KG. The integration of the STAMP into a KG enables a structured representation of system knowledge, supporting the analysis and understanding of system behaviours.

The practical implementation of this methodology has been tested in an exemplary organization from the Oil & Gas industry, where effective safety risk assessment and management are critical for ensuring optimal performance and pivotal for humans, facilities, and environment. The KG plays a pivotal role in attaining a shared comprehension of intricate domains, ensuring uniformity in the representation of data gathered in the STAMP model, and facilitating the communication of this information. The proposed approach enables the linkage and analysis of data from multiple sources, thereby unveiling new insights that would otherwise remain challenging to grasp, or even unreachable.

Keywords: socio-technical systems; knowledge graphs; industrial plants; major accidents; knowledge management.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the support of INAIL (National Institute for insurance Against Accidents at Work). This work is funded through the project "RE-SET: Resilience Engineering for Safe Energy Transition" under the INAIL BRIC 2023 funding scheme.

References

Dekker, S., Cilliers, P., & Hofmeyr, J. H. (2011). The complexity of failure: Implications of complexity theory for safety investigations. Safety Science, 49(6), 939–945. https://doi.org/10.1016/j.ssci.2011.01.008

Nakhal A., A. J., Patriarca, R., De Carlo, F., & Leoni, L. (2023). A System-Theoretic Fuzzy Analysis (STheFA) for systemic safety assessment. Process Safety and Environmental Protection, 177, 1181–1196. https://doi.org/10.1016/j.psep.2023.07.014

Newman, M. (2010). Networks: An Introduction. In Networks: An Introduction. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199206650.001.0001

Pasman, H. J. (2009). Learning from the past and knowledge management: Are we making progress? Journal of Loss Prevention in the Process Industries, 22(6), 672–679. https://doi.org/10.1016/J.JLP.2008.07.010

Patriarca, R., Chatzimichailidou, M., Karanikas, N., & Di Gravio, G. (2022). The past and present of System-Theoretic Accident Model And Processes (STAMP) and its associated techniques: A scoping review. Safety Science, 146(105566). https://doi.org/10.1016/j.ssci.2021.105566

Simone, F., Nakhal Akel, A. J., Alvino, A., Ansaldi, S. M., Agnello, P., Milazzo, M. F., Di Gravio, G., & Patriarca, R. (2023). Extending Safety Control Structures: A Knowledge Graph for STAMP. 33rd European Safety and Reliability Conference, 2581–2588. https://www.rpsonline.com.sg/proceedings/esrel2023/html/P568.html

Human-Hardware In the Loop (HHIL) STAMP-based simulations to model cyber-physical complexity in experimental high-risk plants

Francesco Simone[1,12], Antonio Javier Nakhal Akel[1], Manuel Lombardi[1],
Giulio Di Gravio[1], and Riccardo Patriarca[1]
[1] Department of Mechanical and Aerospace Engineering, Sapienza University of Rome, Italy

Purpose

The advent of the fourth industrial revolution drove industrial establishment towards increasing digitalization. Nowadays, industrial plants and their related equipment are recognized within the notion of Cyber Physical System (CPS), i.e., those systems tightly integrating together both physical processes and computation. Even if these systems are meant to improve quality, performance, and operations, they demand for updated approaches for safety management. Such approaches must be capable of dealing with the additional vulnerabilities CPSs bring into play: vulnerabilities at the informative level may have cascading effects on physical processes, too. Recently, with the establishment of the Industry 5.0 paradigm, the role of human in industrial establishments has been formally acknowledged once more. Accordingly, the importance of human-centric approaches and the need for proper workers' up-skilling becomes paramount, yet in a different perspective from traditional industrial operations. Thus, from simple CPS, it is necessary to move towards socio-technical systems, adopting the notion of Cyber-Socio-Technical System (CSTS), which gives emphasis to those systems in which humans and CPSs interact to reach a common goal. The target, for safety managers and practitioners, remains – at least partially – unsolved: it is only of limited benefit to analyse CSTSs operations and their properties with traditional techniques. A systemic approach remains needed. This work aims to evolve this type of investigation with respect to CSTS response to cyber attacks.

Methods

[12] Corresponding author: francesco.simone@uniroma1.it

This research proposes an approach which rely on System-Theoretic Accident Model and Processes (STAMP) to represent the interactions existing between the agents of the CSTS. All the feedback and control actions between human-to-machine, and machine-to-machine must be taken into account. Interactions of type human-to-human are currently out of scope of this research, as being pure social orchestrations. Following STAMP, the Safety Control Structure (SCS) is used to drive Human-Hardware In the Loop (HHIL) simulations to enable gaining quantitative insights on CSTS safety with respect to cyber vulnerabilities. The HHIL technique is here employed to keep track of human and machine actions within the CSTS. The different types of interactions existing in the SCS could lead to three different situations that identify whether the cyber vulnerability can be managed by an automated controller or a human controller, specifically:

- Automated process control (human monitoring): the human worker cannot intervene on process operations, and they may only visualize data from automated controls. The control of the process is fully automated.
- Human indirect process control (human empowering): the human worker can intervene on process operations, but they could only modify the automated control procedure. The process control is still automated, but control actions could be managed by the human worker.
- Human direct process control (human exclusivity): the human worker performs manual control on the process through a direct modification of the actuators. The human is operating on-site and has the possibility to read measurement directly from the equipment.

These situations lead to adverse scenarios when it occurs: (i) a failure of feedback involved in control algorithms, (ii) a failure of control actions, or (iii) any combinations of the two. Accordingly, if F denotes the total number of feedback involved in control algorithms, and C is the total number of control actions, the number of potential loss scenarios S is:

$$S = \sum_{k=1}^{F+C} \frac{(F+C)!}{k!\,(F+C-k)!}$$

The actual number of scenarios to be evaluated in HHIL simulations will be S' ≤ S since some of the combinations may be meaningless from an operational perspective, or prioritization could be performed trough, e.g., System-Theoretic Process Analysis (STPA). The HHIL in the loop testbed must account for the occurrence of meaningful situations and related loss scenarios.

Results

The theoretical approach is instantiated via an application in the Oil and Gas industry, and a physical experimental testbed is used for designing the HHIL model. The testbed simulates the extraction of oil from a pressurized reservoir. The reservoir pressure is higher than the transport pressure, and suction is created using a gas-liquid ejector. This latter is designed to mix two phases at different pressures conveying the necessary transport energy. For safety reasons and in line with the Do No Significant Harm (DNSH) principle, in the experimental testbed, oil and natural gas have been substituted by water and air, respectively. The plant is equipped with electro-valves to control the incoming pressurized water, to regulate the liquid level, and the overall pressure inside the tank. Moreover, a human worker manages the plant. A desktop software and a mobile app are accessible by the human worker. They permit the worker to: (i) visualize process parameters, and (ii) modify control logics. The worker can also intervene on the plant conducting visual inspections and modifying manual valves. An excerpt of the developed SCS is presented in **Figure 1**. The SCS guides the design of the HHIL model architecture, which is sketched in **Figure 2**. Arrows represent exchange of information and possible interactions among different elements of the model. The CPS of the plant is represented by the blocks: “Plant”, “Sensors”, “PLCs” (i.e., Programmable Logic Controllers), and “Actuators”. Dashed blue arrows represent the information exchange in the automated control loop. A “Data center” stores data from “PLCs” (i.e., blue arrow from “PLCs” to “Data center” depicting sensors readings). From the “Data center”, the “PLCs” may receive indications about the control to be performed (i.e., blue arrow from “Data center” to “PLCs” depicting control action imposed by “Human controller”). These latter come from the interaction between the “Human controller” and the “Data center”. Such interactions (i.e., blue arrow from “Data center” to “Human controller”, orange arrow from “Human controller” to “Data center”) are the desktop software and the mobile app, that enable the “Human controller” to read information about the CPS and modify its functioning.

The elements described until now account for the first and second type of scenarios (i.e., human monitoring and human empowering). Additional interactions are added to include the third type (i.e., human exclusivity). Specifically, the “Human controller” could directly read process data from sensors (i.e., orange arrow from “Sensors” to “Human controller”), and they could directly modify the physical process (i.e., orange arrow from “Human controller” to “Actuators”).

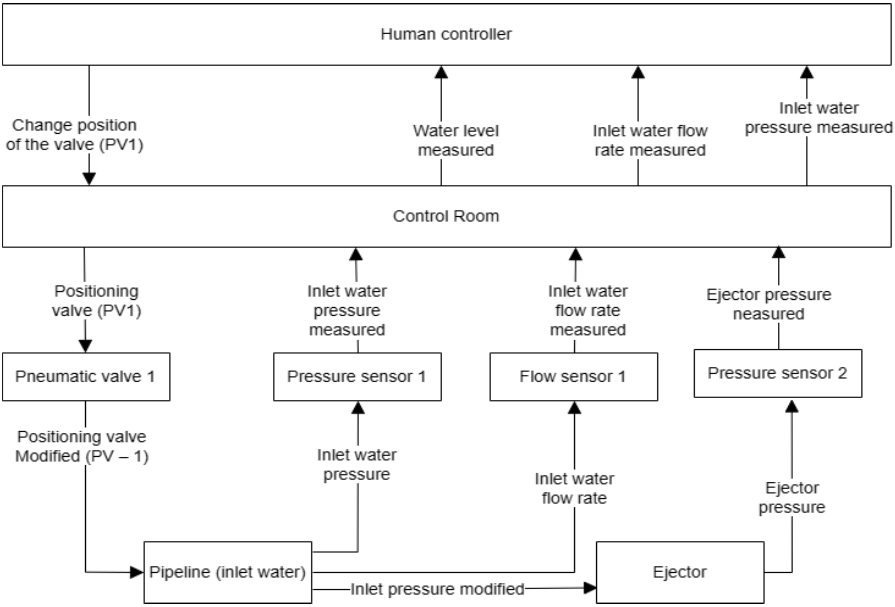


Figure 1. SCS of the CSTS being analysed.

In this way, the HHIL model is capable to simulate every potential loss scenario. However, some of them may lead to dangerous (even destructive) outcomes. To bypass this issue, the “Digital Twin of plant” is added to the model architecture. This element substitutes the physical plant in case of destructive scenario are evaluated. Accordingly, it: (i) receives the control actions from “PLCs” (i.e., light blue arrow from “PLCs” to “Digital Twin of plant”), (ii) simulates the behaviour of the real physical system, and then (iii) returns simulated process parameters (i.e., light blue arrow from “Digital

Twin of plant” to “PLCs”). The “Digital Twin of plant" must be aligned with its physical counterpart, so an exchange of data with the “Data center” is present (i.e., blue arrow from “Data center” to “Digital Twin of plant”).

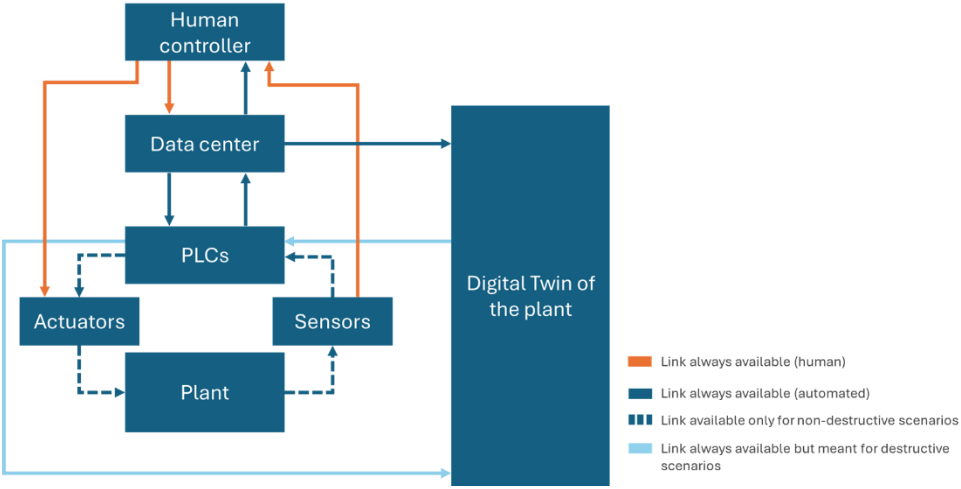

Human controller
Data center
PLCs
Actuators
Sensors
Plant
Digital Twin of the plant
Link always available (human)
Link always available (automated)
Link available only for non-destructive scenarios
Link always available but meant for destructive scenarios

Figure 2. HHIL model architecture as developed by the authors.

The arrows in **Figure 2** distinguish between relationships that always exist (solid arrows), and relationships that are not available in case of destructive scenarios (dashed arrows). The colour code employed differentiates how the information is obtained. Specifically:

- Orange arrows are related to human activities within the CSTS. Information regarding the human worker is collected through a system of motion capture made up of cameras and wearable sensors.
- Blue arrows are related to the CPS. They are already collected during the CPS functioning.
- Light blue arrows are related to the Digital Twin. This information is simulated and collected from the digital model.

Conclusions and implications

The model architecture permits conducting test campaigns systematically through HHIL simulations, making it possible to evaluate the impact of cyber threats on CSTSs. The solution is meant to be a decision support tool to manage CSTSs safety and operations. Moreover, it extends STPA with impact quantification at different level of interactions, enabling the reproducibility of loss scenarios.

Although the implementation of the HHIL testbed could be onerous, the approach favours the knowledge of CSTS, advancing the possibilities of exploring their complexity.

Acknowledgement

This project is funded by the European Union – Next Generation EU under the National Recovery and Resilience Plan (PNRR) – Mission 4 Education and Research – Component 2 From research to business - Investment 1.1, Prin 2022 Notice announced with DD No. 104 of 2/2/2022, entitled RESIST - RESilience management to Industrial Systems Threats, proposal code 2022YSAE2X - CUP B53D23006650006.

Moreover, authors acknowledge Giovanni Mazzuto from Università Politecnica delle Marche for sharing data and information about the experimental plant.

Keywords: stamp; simulation; motion capture; industrial plants; cyber attacks.

Session 6: STAMP in Risk Management and Safety Assessment

Advancing Risk Management in Systems of Systems a Comprehensive Risk Analysis Approach

1 Marjorie Nawila Pettersson (Computer Science and Software Engineering, Mälardalen University, Sweden)
2 Jakob Axelsson (Computer Science and Software Engineering, Mälardalen University, Sweden)
3 Anna Johansson (Economy and Political Science, Mälardalen University, Sweden)
3 Pontus Svenson (RISE Research Institutes of Sweden, Kista Sweden)

ABSTRACT

Systems of systems (SoS) characterized by high degrees of digitization, connectivity, and optimization, are part of modern societies. This study explores the preliminary results of research toward contribution to the holistic analysis of systems of systems (SoS) risks using the STAMP approach. It examines studies on scenarios, including forest fire rescue operations and COVID-19 pandemic management in Sweden. The first study uses STAMP to address unique SoS-specific risk characteristics, while the second study uses it to analyze risk during the pandemic. This highlights the escalating challenges posed by increasing interconnectedness among systems particularly Management of SoS. Consequently, a third study examines existing literature that focuses on management rather than governance, highlighting the need for tailored risk analysis approaches. The study emphasizes the importance of effective governance in SoS management and suggests future research to improve STAMP tools' usability and integrate them with emerging technologies for advanced safety and security analysis in complex systems.

INTRODUCTION

The SoS, consisting of systems referred to as constituent systems (CS), collaborate to achieve a unique capacity that none of them could accomplish individually [1][2]. As the interconnections between CS fluctuate, SoS demonstrates emergent behavior and dynamic characteristics. Yet CS operates and is managed independently. These complex characteristics of the SoS introduce new challenges in analyzing the risks that arise during system interactions in the SoS, necessitating holistic approaches to risk analysis and management. Current risk approaches focus on risk in individual systems whereas SoS risk includes risk across interconnected systems [3]. Hence there is a need to explore more risk analysis approaches for SoS.

PURPOSE

This abstract is about a review of the preliminary results of research exploring new approaches for the holistic analysis of SoS risks. It provides valuable insights from three studies into the risk sources and SoS management, gained by employing the STAMP (System-Theoretic Accident Model and Processes) approach across diverse SoS scenarios, such as forest fire rescue operations and COVID-19 pandemic management in Sweden.

METHODS

This abstract presents a synthesis of preliminary results of research on SoS risk analysis and management. The reviewed studies investigated systems of systems (SoS) using qualitative research methodology with a variety of research methods. In the first study [3], information on the 2014 Västmanland wildfire was gathered using a document review approach. The second research [4], in the meantime, employed a comprehensive literature method, and then the review's findings were thematically analyzed.

Building on this foundation, both studies undertook to assess the applicability of established risk analysis methods within the context of SoS. Utilizing the System-Theoretic Accident Model and Processes (STAMP), they addressed SoS-specific risk characteristics laying groundwork for understanding SoS dynamics and risk factors.

In contrast, the third study [5] focused on synthesizing existing knowledge on SoS management through a literature review. By examining the current state of the art in SoS management and governance, it aimed to provide insights into the evolving complexities of managing interconnected systems.

FINDING AND IMPLICATION

Key sources of risk include unclear roles and latent risk in the first study. This highlights the dynamic character of SoS during crises, illustrating the difficulty of managing systems of systems (SoS) [3]. Further risk analysis indicates the STAMP technique as being useful for determining risk characteristics during the interactions of SoS. However, emergent risks, such as latent risks highlighting hidden dangers that materialize as SoS develops, may require adjustments in the use of the STAMP technique.

The second study finds emergent challenges such as extended SoS structures, uncertainty in decision-making, and the challenge of adapting legislation in a dynamic environment as some of the complexities for SoS. An adjustment of STAMP to include multiple control structures could validate the use of the approach in SoS in capturing additional risks. These findings serve as a basis for practitioners' knowledge base, offering guidance in navigating the complexities of crisis management within SoS.

Finally, the third study explored the complexities of managing SoS, emphasizing the escalating challenges posed by increasing interconnectedness and interdependence among systems. The existing literature leans towards management rather than governance; hence, a research gap remains in comprehensively addressing SoS governance. This study points to the critical role of effective governance in SoS management and identifies avenues for future research to bridge this gap.

CONCLUSION

This abstract synthesis underscores the imperative for tailored risk analysis approaches within socio-technical systems of systems. The synthesis of the studies selected indicates the STAMP technique is highlighted as useful for determining risk in SoS, but adjustments may be needed for emergent risks. Further, the studies reviewed illustrate the dynamic nature of systems of systems (SoS) during crises, emphasizing the difficulty of managing SoS. Identified challenges for SoS management include extended SoS structures, uncertainty in decision-making, and adapting legislation. A review of the state of the art in SoS management underscores the critical role of effective governance in SoS management.

This abstract synthesizes research on the application risk analysis method, STAMP, and the challenges inherent in managing and governing SoS, it contributes to advancing the narratives and practice of SoS risk analysis and management in an increasingly interconnected world. Future research direction on this study will focus on examining the usability of existing

STAMP tools in the context of SoS, as well as exploring their integration with emerging technologies such as artificial intelligence for advanced safety and security analysis in complex systems.

REFERENCES

[1] Maier MW. Architecting principles for systems-of-systems. Systems Engineering: The Journal of the International Council on Systems Engineering. 1998;1(4):267-84.

[2] Axelsson, J. (2019). A refined terminology on system-of-systems substructure and constituent system states. 2019 14th Annual Conference System of Systems Engineering (SoSE), IEEE.

[3] Pinto, C. Ariel, Michael K. McShane, and Ipek Bozkurt. "System of systems perspective on risk: towards a unified concept." International Journal of System of Systems Engineering 3.1 (2012): 33-46.

[3] Pettersson, Marjorie Nawila, et al. "Towards a Risk Analysis Method for Systems of Systems: A Case Study on Wildfire Rescue Operations." 20th Global Information Systems for Crisis Response and Management Conference, ISCRAM 2023; Conference date: 28 May 2023 through 31 May 2023. Information Systems for Crisis Response and Management, ISCRAM, 2023.

[4] M. N. Pettersson, J. Axelsson, P. Svenson, and A. Johansson, “Risk analysis for system of systems management: The swedish covid-19 management case.” Unpublished manuscript , 2024.

[5] M. N. Pettersson, J. Axelsson, P. Svenson, and A. Johansson, “Systems of Systems Management and Governance from a Risk-Handling Perspective.” Unpublished manuscript, 2024.

Standardized safety data and compliance/risk assessment for Occupational Health and Safety surveillance

Antonis Targoutzidis

Planning Manager, Hellenic Institute for Occupational Health and Safety (ELINYAE), GreeceAdjunct Professor, Enterprise Risk Management, Open University of Cyprus, Cyprus

ABSTRACT

STAMP analyses interfaces between all levels of the operational hierarchy. This paper focuses on the top level and more specifically on the interface between Government Regulatory Agencies (GRA) and Company Management (CM), which has several particularities in terms of increased span of control, diversity and autonomy. More specifically, in Occupational Safety and Health (OSH), where regulations include several and detailed technical specifications, many challenges and opportunities for improvement occur.

Generally, the OSH compliance systems consist of two subsystems: the enterprise (CM) and the inspection authorities (GRA). The only specific interaction between them is on-site inspections that are inevitably rare and partial. As both these subsystems interpret legislation, guidelines and know-how, into case-specific controls and measures, independently from each other, inevitably these interpretations differ. Moreover, the picture of authorities about the real safety conditions in each workplace is scarce, partial and non-timely.

A structural change of this system is proposed by creating a direct and standardized channel for OSH data exchange between these two subsystems. Legislation should be centrally interpreted and codified into a single on-line list of specific OSH measures, where enterprises will self-declare compliance to each measure. This will provide clear information to all enterprises about specific requirements and to the authorities about the state of OSH conditions in all enterprises in real-time. The effect of subjective judgements, noise and different interpretations will be reduced, common metrics and benchmarking can be promoted, and on-site inspections can be standardized and prioritized.

The model of this list is based on the codification of Eurostat's European Statistics for Accidents at Work (ESAW), which includes all material factors (infrastructures and materials) and all modes of accidents. For each material factor, possible standardized modes of accidents and relevant preventive measures are identified, along with the relation between them through weighting factors (similarly for health harmful factors). By declaring each material factor and compliance to its relevant prevention measures, a standardized compliance-based risk assessment is automatically calculated, also indicating the missing relevant measures.

This information can be centrally and automatically processed by the system, providing specific alerts to enterprises and authorities, and also prioritizing and guiding on-site inspections that will be conducted on the basis of verification of already stated measures, without requiring reconnaissance.

This universal, standardized, and transparent compliance/risk assessment could be also useful for insurance premium adjustment based on leading (safety), rather than lagging indicators (accidents). Common codification with accident reports (ESAW) allows for machine learning to improve weighting factors.

This complete registration of safety measures requires a different compliance paradigm for the authorities, imposing evaluation of safety measures. Measure's value depends on cumulative reduction of all affected risks, size of affected risks, complementarity/alternation/compatibility to other measures, etc. that cannot fit in the binary paradigm of compliance or non-compliance.

Keywords: Labor Inspection; Compliance; Risk Assessment, Safety Data.

STAMP-ing Out Disaster: A Novel Approach to Preparedness Drill Design and Safety Competency Assessment

Apostolos Zeleskidis, Civil Engineering Department, Democritus University of Thrace, Greece
Stavroula Charalabidou., Civil Engineering Department, Democritus University of Thrace, Greece
Ioannis M. Dokas, Civil Engineering Department, Democritus University of Thrace, Greece

ABSTRACT

This study introduces an innovative methodology for developing operational preparedness drill scenarios coupled with a safety competency evaluation process. The approach leverages the "Engineering for Humans" extension of the STPA (Systems Theoretic Process Analysis) hazard analysis, as proposed by France (2017). This extension is applied to identify causal scenarios that incorporate human behavior and human-computer interaction in relation to unsafe control actions performed by human operators within the Risk and Resilience Assessment Centre of the Region of Eastern Macedonia and Thrace.

The safety requirements identified through the STPA extension serve a dual purpose. Firstly, they are utilized to generate preparedness drill scenarios. Secondly, they form the foundation for implementing the Real-Time Safety Level (RealTSL) calculation methodology, which assesses the safety level of the process during preparedness drills.

This paper presents the outcomes of operational scenarios and demonstrates how these scenarios are integrated into the initial stages of RealTSL. The goal is to effectively apply this methodology in future preparedness drills to evaluate the safety competency of the system under examination.

By combining STAMP-based analysis with preparedness drill design and safety competency assessment, this research offers a holistic approach to enhancing system safety in complex socio-technical environments. The methodology presented has the potential to significantly improve the effectiveness of disaster preparedness training and evaluation.

Keywords: STAMP; Preparedness drills; Safety competency assessment; Human factors; Risk and Resilience Assessment Centre

Session 7: STAMP in Specific Industries and Applications

Harnessing STAMP, STPA, and STECA: A Novel Approach to Safety, Security, and Sustainability in Waste-to-Energy Infrastructure Design

Svana Helen Björnsdóttir, Department of Engineering, Reykjavik University, Iceland
Saemundur E. Thorsteinsson, Department of Engineering, Reykjavik University, Iceland

ABSTRACT

This paper describes a study on how STAMP, STPA and STECA can be applied to meet safety, security and sustainability-based design requirements for a major national infrastructure.

By applying stakeholder theory, it is possible to define and differentiate between actors and stakeholders in a Waste-to-Energy (WtE) system model, a major national project still in the concept phase.

The difference between an actor and a stakeholder lies in the fact that an actor can influence the actions of a system or an organization without directly being a part of the system or in an actual relationship with the organization, while a stakeholder (internal or external) is a defined part of the system or in an actual relationship with the organization. This can depend on, i.a., legal provisions and contractual provisions.

Identifying stakeholders is an important start of modelling a system to capture and analyze the necessary interactions between individual system parts, especially in major national infrastructure projects where strict requirements are made regarding safety, security and sustainability and always provide information regarding status of these elements.

The WtE project chosen for the analysis is at an early stage and a detailed analysis and validation of all aspects is needed, i.a., the scope of the project. However, laws and regulations set a framework for such a project.

The alignment of stakeholders within the system, their role and responsibility in the design and construction phase of the WtE plant, given the sustainability and circular economy restrictions, are addressed in the study. Examples of these restrictions are that the project passes an environmental assessment and that a construction permit is obtained for a suitable location. Also, that only waste is burned that cannot be reused in any way, the incineration value of waste is sufficiently high and stable, toxins do not find their way into the material stream that goes to incineration, the flue gas is cleaned and remains well within the permissible limits according to criteria issued by the EU for WtE incineration plants.

Stakeholders' roles and responsibilities are analyzed, yielding their feedback on potential risks and creating a positive image of the project. Also, suitable ways to enter the project and finance it are devised. In essence, this enables the creation of a safety, security and sustainability-based design approach.

A detailed documentation of the system model development is presented.

The novelty of the study lies in the application of STAMP, STPA, and STECA as a safe, secure and sustainable by design approach for a major infrastructure project. Also, the methods discussed here have not been used in a WtE project as far as known.

Keywords: STAMP; STPA; STECA; Waste-to-Energy; sustainability; project management.

Enhancing collaborative processes in Building Information Modelling with STPA

1. **Ioannis Katranas** Dept. of Civil Engineering, Democritus University of Thrace, Greece, email: ioankatr1@civil.duth.gr,
2. **Georgios Charalampos Kafoutis** Dept. of Civil Engineering, Democritus University of Thrace, Greece and
3. **Ioannis Dokas** Dept. of Civil Engineering, Democritus University of Thrace, Greece

ABSTRACT

This paper explores the utilization of System Theoretic Process Analysis (STPA) into Building Information Modelling (BIM) frameworks to identify potential loss scenarios during collaborative processes such as: The BIM collaborative team fails to deliver high-quality service (resulting in suboptimal project outcomes), budget Overruns (leading to financial difficulties), reduced credibility of the BIM team etc. BIM is widely recognized for enhancing the efficiency and accuracy of construction project management by facilitating multi-disciplinary collaboration and data integration. However, the complexity of interactions within BIM group environments can lead to various loss scenarios that traditional safety analysis methods may overlook. This study demonstrates the application of STPA within a BIM group to systematically identify and mitigate loss scenarios. Through a detailed case study, we outline the steps of integrating STPA into BIM workflows, identifying control actions, and uncovering potential hazards and unsafe interactions. The results highlight the efficacy of STPA in enhancing safety and reliability in BIM-based projects, promoting a proactive approach to risk management in construction. This integration not only improves the identification of loss scenarios but also supports the development of robust mitigation strategies, ultimately contributing to safer and more resilient construction practices.

The methodology involves mapping the BIM collaborative processes onto STPA's hierarchical control structure, encompassing all key stakeholders, information flows, and control actions. By systematically analysing these elements, we identify critical points where inadequate control or erroneous information transfer could lead to hazardous conditions. The case study further illustrates how specific BIM tools and protocols can be adjusted or redesigned to address these vulnerabilities. Key findings reveal that the utilization of STPA into BIM enhances the detection of complex, emergent hazardous system states. For instance, it uncovers scenarios where miscommunication between architects and engineers could lead to structural design flaws, or where data incompatibility between BIM models could result in incorrect construction execution. Additionally, the study highlights the importance of continuous monitoring and feedback loops within the BIM environment to ensure ongoing risk mitigation throughout the project lifecycle.

Indicative examples of hazards and unsafe control actions (UCA) are listed below:

Hazards:

H1: the BIM team lacks a consistent shared understanding of the project at all times,

H2: BIM System fails to maintain model integrity across multiple project phases,

H3: BIM team violates the minimum time for deadline.

Indicative Unsafe Control Actions:

Control Action	Provided	Not Provided	Too late	Stopped too soon, applied too long
Share the latest model updates	When the BIM team has not finished its updated work	When there is a deadline for the BIM team to complete the essential tasks	When the latest model is used as a foundation by another subgroup	When a governing authority updates a rule that influences the project
Establish work status	When the project's scope is undefined	When labour costs need to be estimated	When a sub-team decides to exit the BIM team	When the project's conditions are altered

This pioneering integration of STPA into BIM lays the foundation of more safe collaborative processes during construction safety practices, enabling stakeholders of a new perspective to address potential issues in collaborative processes and ensure the integrity and success of construction projects before they escalate into costly and dangerous incidents. This proactive approach may enhance project outcomes but also may build trust among project participants and clients by demonstrating a commitment to safety and quality. This research underscores the potential for STPA to become a standard practice in BIM-integrated construction projects, fostering a culture of safety and proactive risk management in the industry.

Keywords: STPA; BIM; Collaborative Processes;

Analysis of Fire Protection Regulation for Properties within or near Forest Areas in Greece using Systems Theoretic Early Concept Analysis (STECA)

1. **Georgios Charalampos Kafoutis** Dept. of civil Engineering, Democritus University of Thrace, Greece, email: gekafout@civil.duth.gr
2. **John Dokas** Dept. of civil Engineering, Democritus University of Thrace, Greece
3. **Ioannis Katranas** Dept. of Civil Engineering, Democritus University of Thrace, Greece

ABSTRACT

The increasing frequency and severity of wildfires in forested regions in Greece necessitate robust regulatory frameworks to mitigate risks and increase the safety level of properties and inhabitants against wildfires. In March 2023, Greece introduced a new law aimed at enhancing fire protection measures for properties situated within or near forested areas. This paper employs Systems Theoretic Early Concept Analysis (STECA) to comprehensively evaluate the effectiveness and potential shortcomings of this regulatory intervention.

STECA offers a systematic approach to understanding complex systems by examining interactions, dependencies, and feedback loops at an early stage of the regulatory process. By applying STECA to the fire protection regulation, this study seeks to identify key factors influencing its implementation, assess its impact on stakeholders, and anticipate potential unintended consequences. The analysis encompasses multiple dimensions, including regulatory enforcement mechanisms, stakeholder engagement, resource allocation, and resilience to changing environmental conditions. Through the lens of STECA, the interplay between policy objectives, institutional capacities, and socio-economic factors is examined to uncover potential vulnerabilities and areas for improvement.

Preliminary findings suggest that while the new regulation represents a significant step forward in enhancing fire protection measures, several challenges remain. The analysis conducted with STECA method has revealed multiple gaps, particularly in the areas of vegetation management, structural fire protection, storage restrictions, evacuation preparedness,

compliance and enforcement capacity, community awareness and the integration of scientific knowledge into policy-making processes.

The regulation mandates the creation of protection zones around buildings to mitigate fire risks in an effort to address vegetation management. However, if vegetation within these zones is not properly managed, it can lead to the accumulation of combustible materials, thereby increasing the fire hazard. Proper maintenance of these zones is crucial to reducing the likelihood of fires spreading to structures and this is not sufficiently ensured by the regulation. Another area of concern is structural fire protection. The regulation requires compliance with stringent fire resistance standards for building materials. Yet, due to economic constraints, some property owners may fail to meet these standards, thereby compromising the structural integrity of buildings during a wildfire. This economic barrier poses a significant risk to the overall effectiveness of fire protection measures. Storage restrictions also present a challenge. The regulation stipulates that flammable materials, such as firewood, should not be stored near buildings. Non-compliance with these storage restrictions (firewood is a necessity during the winter in rural areas) can lead to the accumulation of flammable materials, which significantly increases the fire hazard. Evacuation preparedness is critical for safeguarding lives during wildfire events. The development of effective evacuation plans and ensuring that occupants are well-prepared to evacuate safely is paramount. However, if evacuation routes are inadequate or if occupants are not sufficiently informed or trained in evacuation procedures, these plans may prove ineffective. Proper training and clear communication are vital components of successful evacuation strategies. Finally, compliance and enforcement of the regulation pose significant challenges. Inadequate enforcement mechanisms, such as audit committees comprising untrained officials and limited control over a small percentage of properties, undermine the regulation's effectiveness. Furthermore, if property owners do not adhere to fire protection requirements, the likelihood of fire protection measures failing increases substantially. Strengthening enforcement mechanisms and ensuring comprehensive compliance are crucial to the regulation's success.

Addressing these gaps requires a multi-faceted approach involving regulatory oversight, public education and outreach, infrastructure improvements, and community engagement. By identifying and addressing these gaps, stakeholders can enhance the resilience of properties within or near forest areas to wildfire threats, reducing the potential for loss of life and property damage. This paper highlights the utility of STECA in analysing and enhancing the effectiveness of fire protection regulations in or near forested areas by systematically identifying and addressing underlying systemic vulnerabilities (gaps of the regulation). Then policymakers can better safeguard properties and communities from the growing threat of wildfires, contributing to greater resilience and sustainability in forest management practices. The analysis can inform future policy decisions for fire safety in Greek forest areas.

Keywords: STECA; Fire Protection Regulation; Forest fires

Session 8: STAMP in Emerging Technologies

SAISec: STPA in Artificial Intelligence Systems of Airport Security

Anastasia Giamali[1,13] and Andreas Maniatopoulos[2]

[1]Democritus University of Thrace, Department of Civil Engineering, Greece

[2] Democritus University of Thrace, Department of Electrical & Computer Engineering, Greece

ABSTRACT

While airports implement strict security protocols to detect and prevent illegal activities, incidents still occur. Hence why airport authorities continuously strive to enhance security measures and implement innovative technologies to mitigate security risks and address emerging threats effectively. The large crowds that are simultaneously present in the facilities, particularly in check-in, security monitors and luggage collection, along with the time sensitive procedures and stress that everyone is under, make staff and travelers focus on individual tasks one at a time, thus providing opportunity for thefts, disorderly behavior and attempts to access restricted areas. At the same time, airports offer passage to other countries, which is of interest to individuals who attempt to smuggle items such as drugs, weapons, or counterfeit goods through the airport's security checkpoints or cargo facilities. Lastly, airports are potential targets of terrorist activities, such as hijackings and bombings, which pose a significant threat to public safety. To address this issue, we propose a system that salvages the capabilities of Artificial Intelligence and STPA analysis. System-Theoretic Process Analysis (STPA), is a hazard analysis technique used to identify and mitigate risks in complex systems, by considering not only individual components but also their interactions within the system. It is based on systems theory, which views systems as interconnected entities, where

[13] Corresponding author: anastasiayiamali@outlook.com

changes in one part can affect the entire system and thus, is able to uncover potential hazards that may arise from interactions between system components, rather than just focusing on individual failures. The approach it offers can be particularly useful for a dynamic system such as an airport, because by identifying these systemic risks in the design of the security systems, STPA enables engineers to uncover more potential needs, implement effective safeguards and design features to prevent unsafe scenarios. STPA also emphasizes the importance of understanding the underlying goals and objectives of the system, as well as the broader socio-technical context in which it operates. This helps in identifying not only technical failures but also human and organizational factors that could contribute to unsafe incidents, which is particularly useful in the context of a facility whose main purpose is to provide the means to fulfill people's need for long distance transportation. Our proposed AI system for airport security is designed to fundamentally change the way airports detect and respond to potential threats, while prioritizing passenger safety and privacy, by leveraging cutting-edge technologies such as computer vision and physiological analysis to provide a comprehensive and proactive approach to security screening.

After conducting a thorough STPA analysis of the airport security system as a whole, meaning both the theoretical needs and the hardware used, we utilize the results of the report as training data for Artificial Intelligence systems. The rich dataset that STPA can provide, through in depth analysis of the system, can serve as valuable input for training AI models to identify the patterns and relationships which are deemed as unsafe in the analysis, enabling them to recognize potential hazards and deviations from safety norms more effectively, leading to improved predictive capabilities and proactive risk management. Furthermore, integrating STPA results into AI training can enhance the adaptability and robustness of AI systems in dynamic environments with the holistic perspective provided by STPA allowing AI models to account for various system interactions and dependencies, making them better equipped to handle unforeseen circumstances and changes in operating conditions. Moreover, using STPA results as training data can facilitate the development of AI-driven decision support systems for safety-critical applications. By incorporating the knowledge gained from STPA analysis, these AI systems can provide real-time guidance and recommendations to people in charge of security monitoring, helping them make informed decisions to prevent illegal activities.

Regarding its architecture, the first component of our AI system involves the deployment of advanced computer vision algorithms integrated into existing CCTV camera networks, with the algorithms continuously analyzing video feeds in real-time, detecting and identifying suspicious activities or behaviors. Whether it's unauthorized access, erratic movements, or abandoned items, our AI-powered computer vision system swiftly alerts security personnel, enabling rapid response to potential threats. The major benefit of this system is that it can analyze the video feed from all the cameras of the airport simultaneously, as opposed to people whose attention span is limited and they are subjected to physical toll. Note, however, that the system's purpose is to draw the attention of security personnel to the incident, not to act on its own. It will do that by highlighting with flashing red borders the screen in which a potentially hazardous activity is taking place along with a corresponding title.

Complementing the computer vision system is our innovative use of high refresh rate cameras equipped with AI with physiological analysis capabilities, strategically positioned at key checkpoints like passport control, capturing subtle physiological cues, such as facial expressions, heart rate, and blood pressure variations by motion amplification. By analyzing these cues, our AI system can assess individuals' emotional states, detect signs of nervousness, and even evaluate the veracity of statements, providing security personnel with invaluable insights into passenger behavior, allowing for targeted interventions when necessary. Our AI systems prioritize both effectiveness and ethics. We are committed to ensuring that the implementation of these technologies complies with privacy regulations and respects passengers' rights. In an effort to make this system as fair as possible, the authors have taken action against AI discrimination by extensive research in AI and Ethics, providing the algorithm in question with a fair and representative dataset. Furthermore, the research team invested significant hours studying behavioral psychology, emotion recognition, and human nature to ensure the AI system accurately identifies emotions, as well as finds the correlation with subtle physical signs and emotional state such as the increase of the pupil to iris ratio, which despite being barely perceivable, it conveys important information about the psychological state of the target.

Airport security is essential for safeguarding passengers, crew, and aircraft from terrorism, violence, and other illegal activities. A state-of-the-art security system, enhanced by AI trained with scenarios generated through STPA analysis, can significantly bolster security measures and prevent a wide range of illegal activities. Those scenarios can help the AI identify the unsafe actions. Moreover, by continuously analyzing new scenarios and updating their algorithms, AI systems can stay ahead of threats and provide airports with dynamic security solutions.

Keywords: STPA; Artificial Intelligence; Computer Vision; Airport Security System

Towards a STAMP-Based Safety Metric in Mixed Human-AI Squadron Missions

1. **Nikolaos Vasiliadis** STS's Deputy Commander (Synthetic Training Squadron, HAF)
2. **John Dokas** Dept. of civil Engineering, Democritus University of Thrace, Greece

1. Introduction

As the landscape of modern warfare evolves with the advent of sophisticated technologies, there is an increasing trend toward integrating Unmanned Combat Aerial Vehicles (UCAVs) into traditional squadrons. This shift brings unique challenges and necessitates a comprehensive reevaluation of safety protocols. Our research, which is novel in its focus on mixed human-AI squadron missions, aims to develop enhanced ORM practices tailored for these missions, addressing the emerging risks and operational dynamics of such integrations.

2. Objectives

The research aims to achieve several critical objectives:

1. Develop and validate new STAMP-based safety metrics for mixed human-AI squadron operations.

2. Identify and mitigate potential risks arising from the interaction between human pilots and AI-controlled UCAVs.

3. Improve decision-making processes and operational effectiveness within mixed squadrons.

4. Ensure the seamless integration of UCAVs into traditional squadrons without compromising mission safety or performance.

By accomplishing these objectives, the research seeks to provide a robust framework that enhances current ORM practices, making them more suitable for the complexities of modern warfare involving both human and AI elements.

3. Methodology

The research will combine system-theoretic process analysis (STPA) and simulation techniques. These methodologies are selected for their unique ability to handle complex systems and interactions, making them ideal for analyzing the intricate dynamics of mixed human-AI squadron missions.

STPA will be employed to:

1. Identify potential hazards in mixed human-AI squadron operations.

2. Analyze the interactions between human pilots and AI-controlled UCAVs to determine where and how risks may arise.

3. Develop control strategies to mitigate identified risks and ensure safe operation.

3.1 Simulation

Simulations will be utilized to model various mixed squadron scenarios, providing a controlled environment to test and refine the proposed safety metrics. These simulations will incorporate both human pilots and AI-controlled UCAVs, allowing for the manipulation of critical variables such as mission complexity, environmental conditions, and human-AI communication.

Simulations will be conducted to:

1. Validate the proposed safety metrics under different operational conditions.

2. Assess the impact of mission complexity and environmental factors on safety and effectiveness.

3. Refine control measures and decision-making processes to enhance mission safety.

4. Expected Outcomes

The research is expected to yield several significant outcomes:

1. **Validated Safety Metrics**: A set of validated safety metrics designed explicitly for mixed human-AI squadron missions, addressing these operations' unique risks and challenges.

2. **Enhanced ORM Framework**: A comprehensive framework for integrating the new safety metrics into existing ORM practices, ensuring they are seamlessly incorporated into the Hellenic Air Force's safety protocols.

3. **Operational Insights**: Detailed insights into the operational dynamics of mixed human-AI squadrons, including potential safety pitfalls and strategies for effective integration.

4. **Recommendations for Implementation**: Practical recommendations for implementing the enhanced ORM practices, including changes to training programs, operational procedures, and system design.

These outcomes will provide a robust foundation for ensuring the safe and effective operation of mixed human-AI squadrons, contributing to the broader field of military aviation safety.

5. References

1. Leveson, Nancy G. *Engineering a Safer World: Systems Thinking Applied to Safety*. Cambridge: MIT Press, 2011.
2. Hellenic Air Force. "Operational Risk Management." Accessed May 25, 2024. https://www.haf.gr/.

ESWC

European STAMP Workshop and Conference

YEARS
1973-2023

DEMOCRITUS
UNIVERSITY OF THRACE

THANKS TO OUR SPONSORS

VWAY

V WAY Co Ltd

ΕΛΙΝΥΑΕ

ΕΛΛΗΝΙΚΟ ΙΝΣΤΙΤΟΥΤΟ ΥΓΕΙΑΣ ΚΑΙ ΑΣΦΑΛΕΙΑΣ ΣΤΗΝ ΕΡΓΑΣΙΑ