# Safety Improvements for Laboratory Handling of Energetic Materials Applying System -Theoretic Process Analysis

STAMP Workshop 2023 - MIT

**KARENS. ANDRADE**, ANTONIO V. DINIZ MERLADET, THOMAZ M. KLAPÖTKE, CHIARA MANFLETTI

**LUDWIG-MAXIMILIAN UNIVERSITY MUNICH – TECHNICAL UNIVERSITY OF MUNICH**

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# Karen S. de Andrade

Captain **ANDRADE -** BRAZILIAN AIR FORCE

- Chemical Engineer - Master in Polymers (UFMG)
- Ongoing: PhD Chemistry – Energetic Materials (LMU)

## Institute of Aeronautics and Space

- ✓ 16 years laboratory work
- ✓ Solid propulsion
- ✓ Synthesis (bounding agents, catalysts, binders, oxidizers)
- ✓ Analysis – Quality control
- ✓ Technical Evaluation - Acquisitions

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# OBJECTIVE

Model the hazards of **handling energetic materials in research laboratories** and analyze the scenarios applying STPA (System-Theoretic Process Analysis) to **minimize the effects of unsafe events or mitigate their consequences**.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# SUMARY

1. Introduction
2. Motivation
3. STPA Application
4. Main Results from Unsafe Control Actions, Safety Constraints and Loss Scenarios
5. Applicability of the Analysis
6. Benefits for Research Centers
7. Conclusion
8. References

# INTRODUCTION

## Laboratories

- Good Laboratory Practice

### Analysis

- Defined process → Operational Procedures
- Quality System → ISO/IEC 17025 – ISO 9001
- Operator with experience

### Synthesis

### Research

- New process
- No Quality System
- Operator with less experience

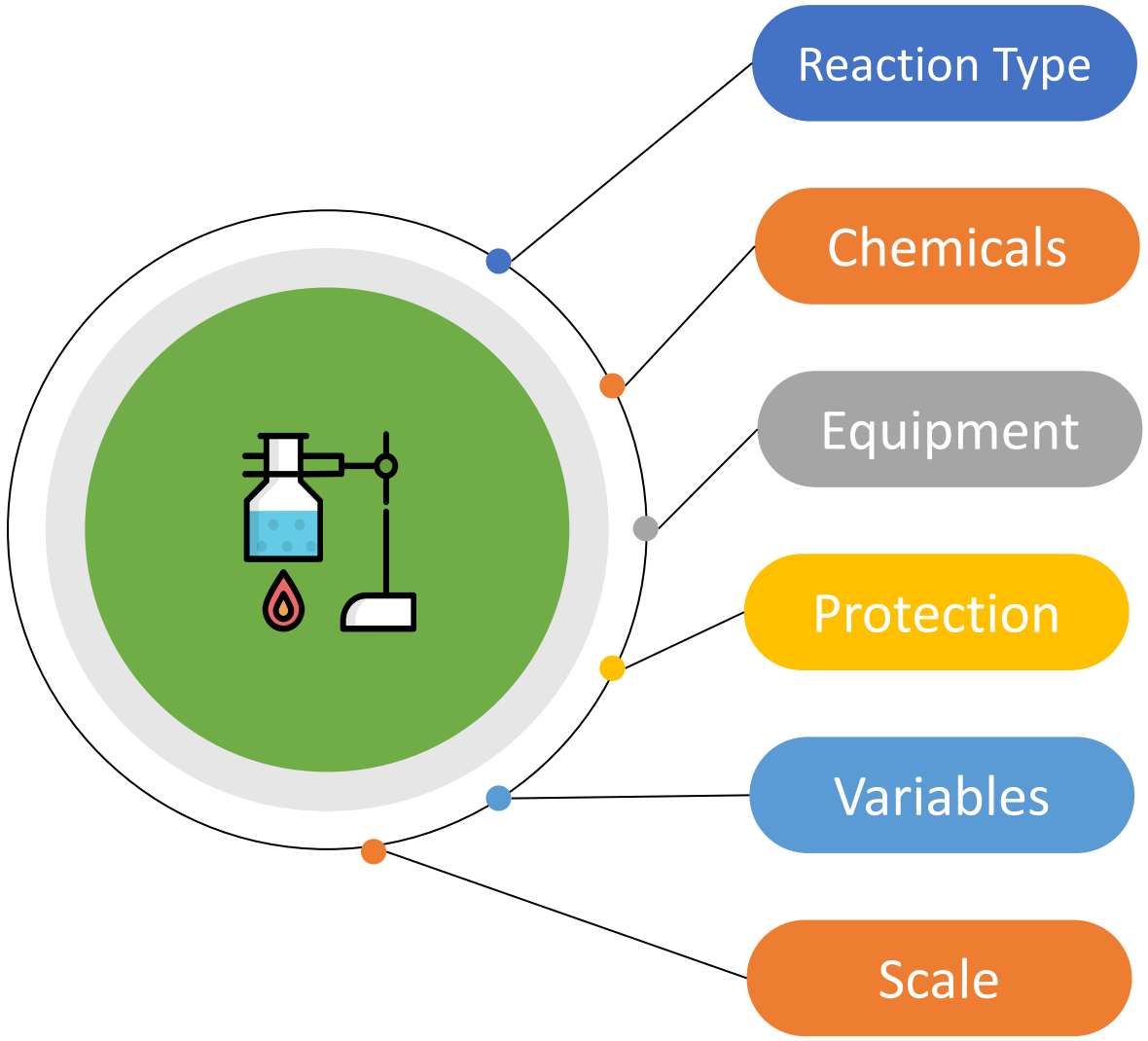
LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# MOTIVATION

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# BEFORE STPA

The chemical reaction/analysis as protagonist



LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

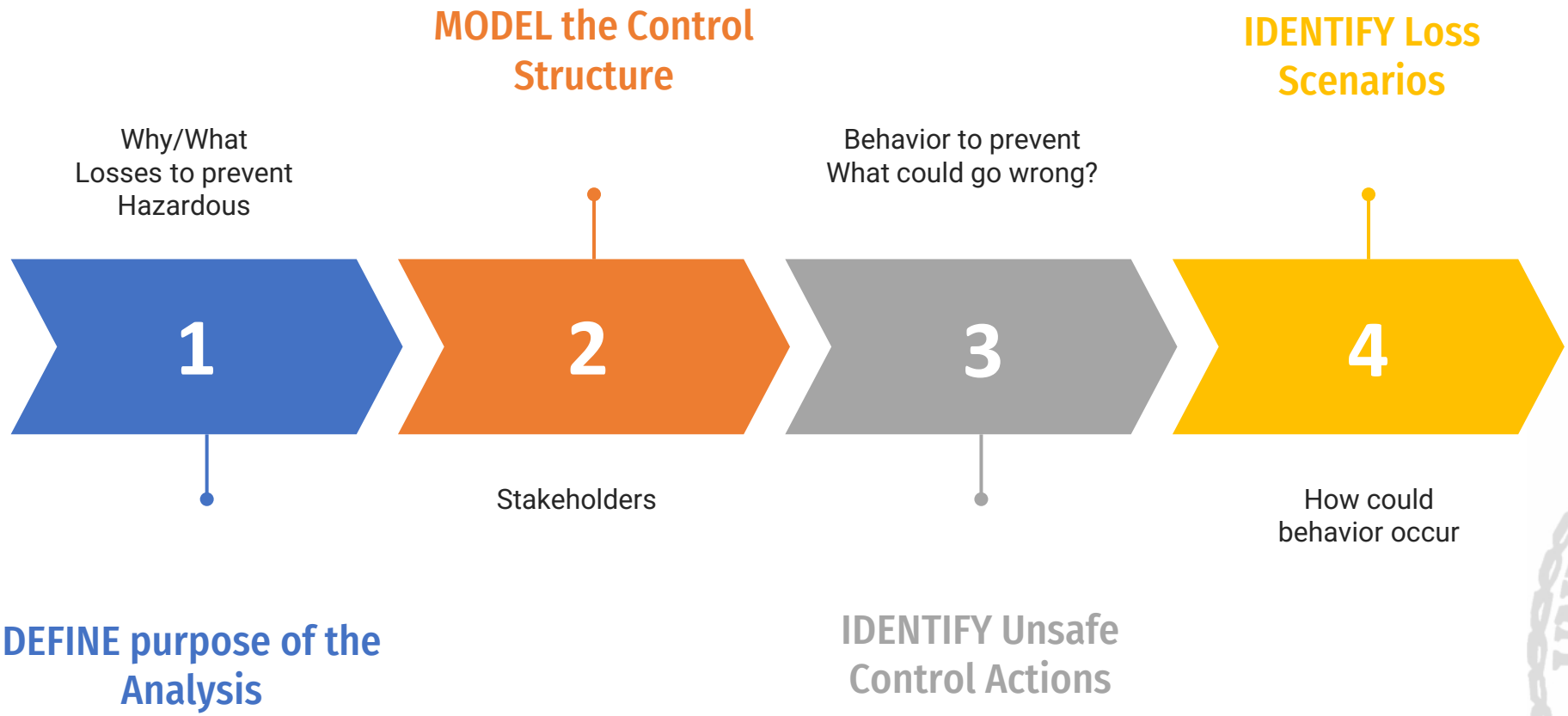
# AFTER STPA

The chemical handling of energetic materials as protagonist

Emergency mode

Made **complex** things
**less complicated**

# STPA APPLICATION




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

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# STPA APPLICATION

## Main Losses (L) for Energetic Materials Handling in Research Laboratories

| | |
|---|---|
| L-1 | Loss of human life or human injury of laboratory-related personnel. |
| L-2 | Loss of produced energetic material. |
| L-3 | Damage to the Laboratorial Facility or the laboratory equipment. |
| L-4 | Rework and project schedule timeline losses. |
| L-5 | Financial losses. |
| L-6 | Environmental losses. |
| L-7 | Loss of human life or human injury of personnel external to the laboratory facilities. |

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# IDENTIFYING SYSTEM-LEVEL HAZARDS

| | System-level Hazards (H) | Associated Losses |
|---|---|---|
| H-1 | **The system process variables violate the minimum safety acceptable standards conditions for energetic materials.** | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |
| H-2 | Personal and Collective Protective Equipment not used for laboratory activities. | **[L-1]** |
| H-3 | Laboratory equipment out of calibration standards. | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6]** |
| H-4 | **Energetic Materials usage out of the prescribed.** | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |
| H-5 | Laboratory Procedures or Manuals not including essential safety protocols. | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6]** |
| H-6 | Materials, tools, infrastructure, or equipment damaged or unavailable to the operator proceed with the laboratory activities. | **[L-4], [L-5]** |
| H-7 | Laboratorial Equipment or Energetic Materials are not adequately identified and stored. | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |
| H-8 | Laboratory facilities not appropriated for the current activities. | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |
| H-9 | **Energetic Materials are handled without operational training.** | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |

# IDENTIFYING SAFETY CONSTRAINTS


| | System-level Hazard | Associated Losses |
|---|---|---|
| H-1 | The system **process variables** violate the minimum safety acceptable standards conditions for energetic materials. | **[L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7]** |

| | System-level Safety Constraints |
|---|---|
| SC-1.1 | The **energetic material state** must not differ from the safety **acceptable conditions** to be handled. |
| SC-1.2 | Laboratory Operators must **verify the safety acceptable environmental conditions and the restrictions** for handling energetic materials. |
| SC-1.3 | Laboratories that handle energetic materials must have laboratory environmental **control equipment.** |
| SC-1.4 | Laboratory Operators must **set the laboratory process variables conditions in accordance with the limitations** for handling the energetic materials under manipulation (analysis/syntheses). |
| SC-1.5 | The laboratory supervisor must **supervise the laboratory activities** to verify the safety standards for handling energetic materials. |
| SC-1.6 | During laboratory handling and experiments with Energetic Materials, the Laboratory Operators must **measure and receive data of the synthesis** process variables conditions. |
| SC-1.7 | Laboratory Operators **must be able to stop the synthesis** once it is detected that the process variables conditions are out of the safety acceptable states for handling. |

# IDENTIFYING SAFETY CONSTRAINTS

| | System-level Hazard | Associated Losses |
|---|---|---|
| H-4 | Energetic Materials usage out of the prescribed. | [L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7] |

## System-level Safety Constraints

| | |
|---|---|
| SC-4.1 | Energetic materials must be **used as prescribed**. |
| SC-4.2 | Energetic materials must be **identified** as to the **synthesis date, expiration date** when industrialized, or **revalidation date**. |
| SC-4.3 | A **storage method** for using chemicals, such as FIFO (First-In, First-Out), should be adopted. |
| SC-4.4 | Laboratory Operators must be **trained** to manipulate energetic materials correctly. |
| SC-4.5 | Expired materials must be revalidated before use. |
| SC-4.6 | Energetic materials must be **identified** as to the particular **danger of handling**. |
| SC-4.7 | The Laboratory Supervisors must be a part of the **scale of the energetic material manipulated**, if the authorizations are correct, and if the work is conducted at the **appropriate time** with people to provide **first aid** or **trigger emergency mode** if necessary. |

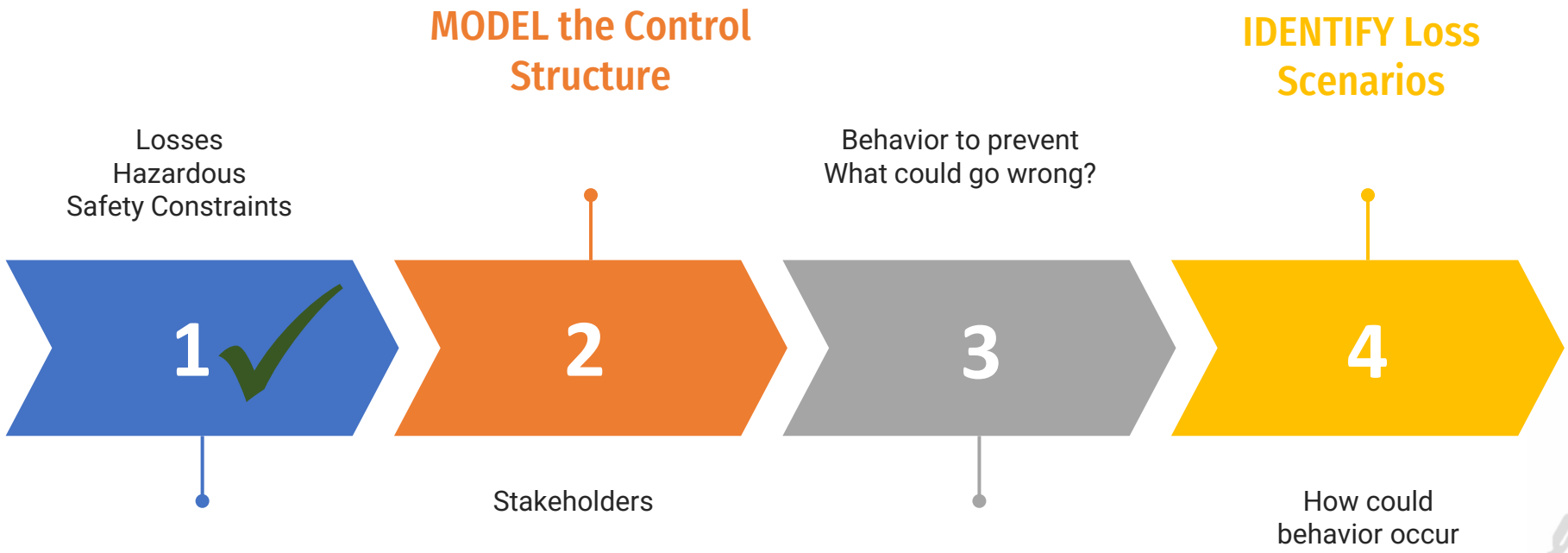
# IDENTIFYING SAFETY CONSTRAINTS

| | System-level Hazard | Associated Losses |
|---|---|---|
| H-9 | Energetic Materials are handled without **operational training**. | [L-1],[L-2], [L-3], [L-4], [L-5], [L-6], [L-7] |

## System-level Safety Constraints

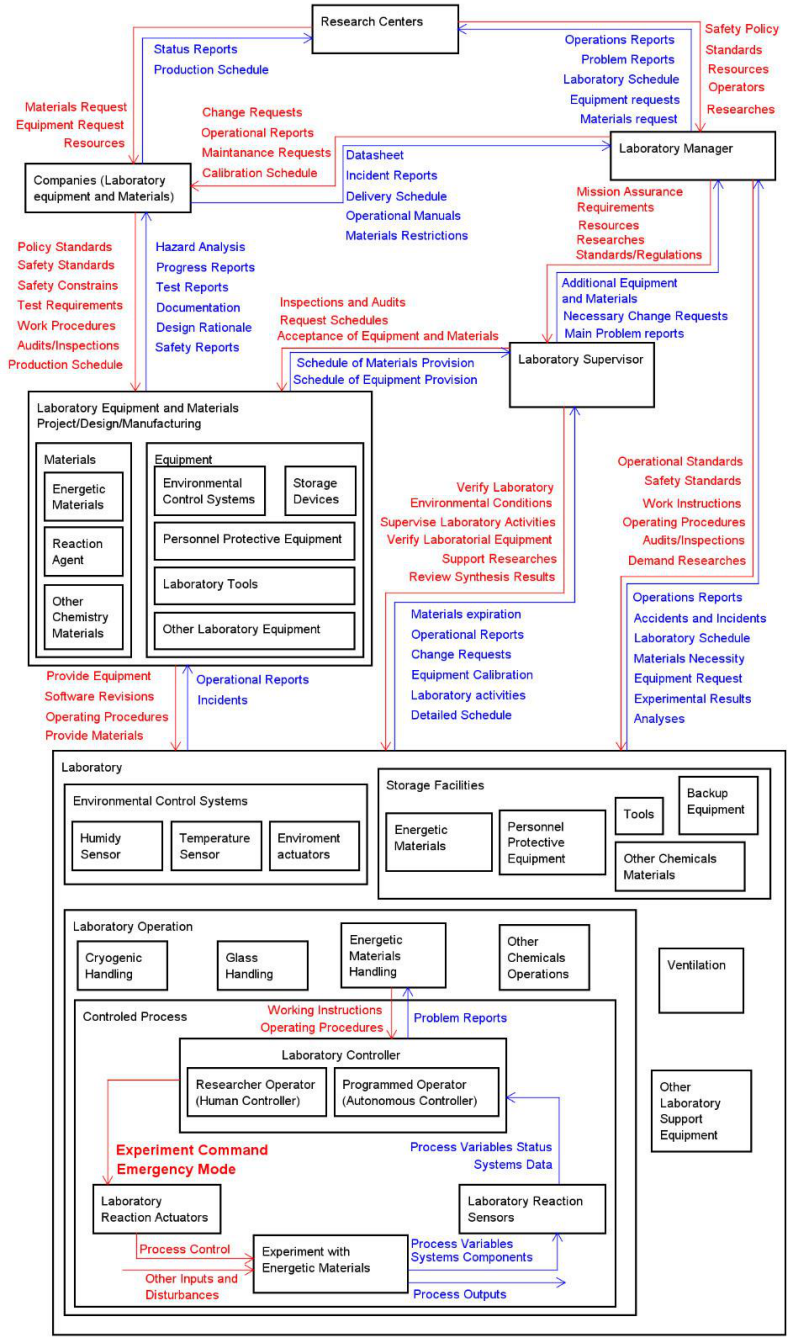
| | |
|---|---|
| SC-9.1 | Operators must **conclude operational laboratory training** for handling Energetic Materials. |
| SC-9.2 | Operational laboratory trainings must **approach the safety constraints and guidelines** on handling Energetic Materials. |
| SC-9.3 | The Laboratory Managers must **periodically implement training** for safely handling Energetic Materials to the Laboratory Supervisors and Operators. |
| SC-9.4 | Laboratory Supervisors must **verify if the Operators have concluded the training** for safely handling Energetic Materials before authorizing the activities. |

# STPA APPLICATION



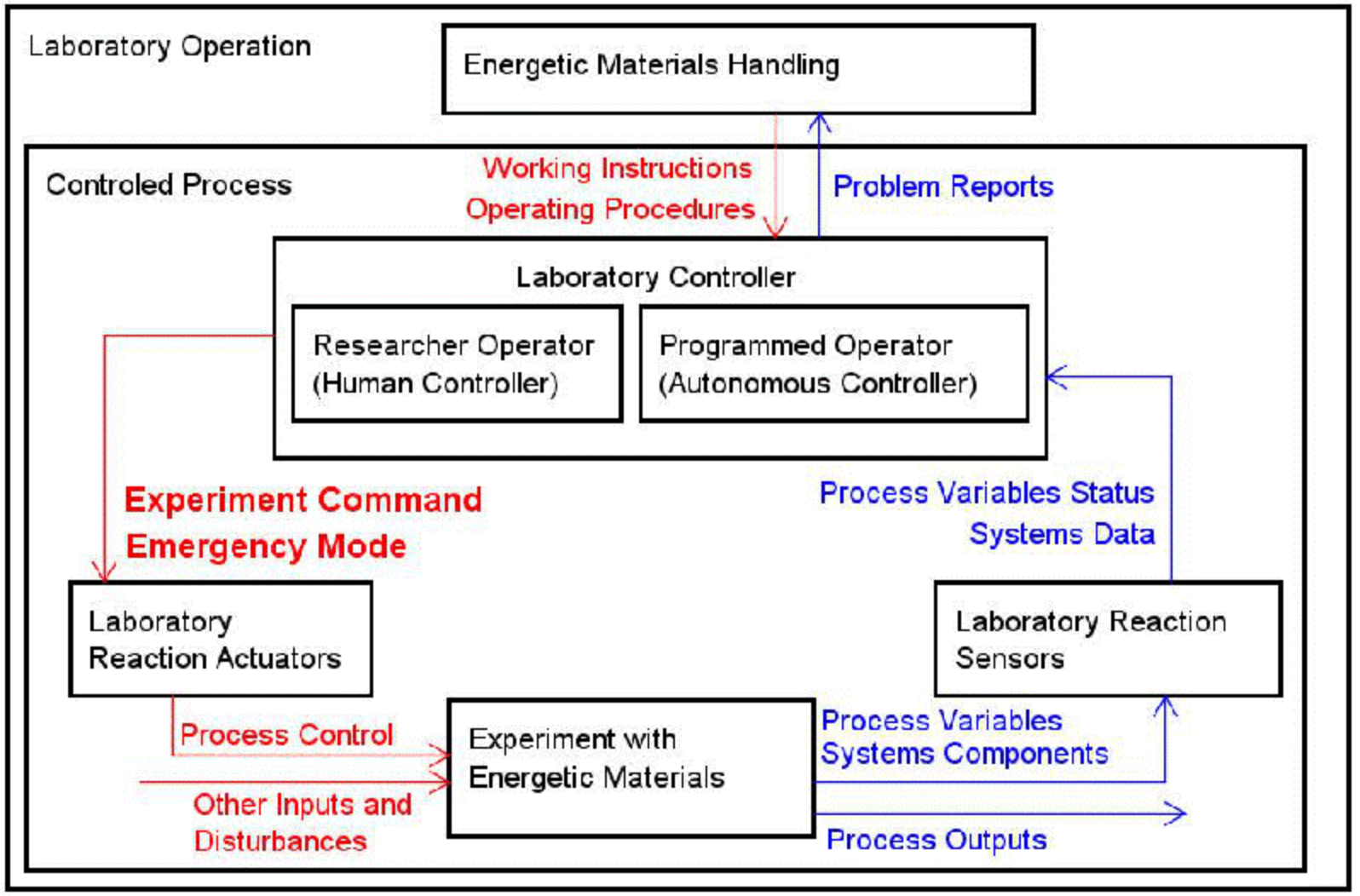

Leveson, N. G., Thomas, J. P. STPA Handbook. USA, **2018**.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN



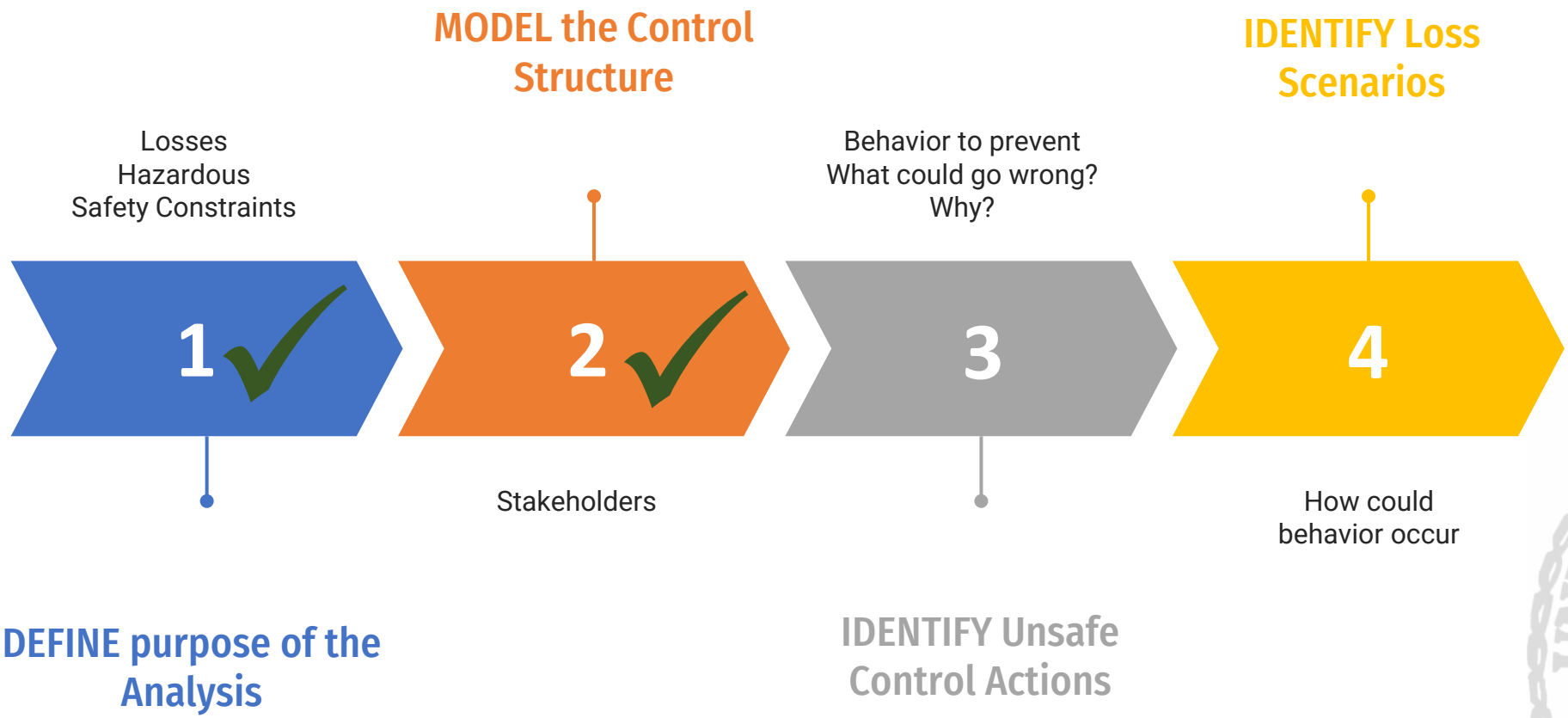

Hierarchical Control Structures

# Research Centers
# Companies
# Laboratory Manager
# Laboratory Supervisor
# Operator




Analyzed Process

# STPA APPLICATION




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

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# UNSAFE CONTROL ACTIONS

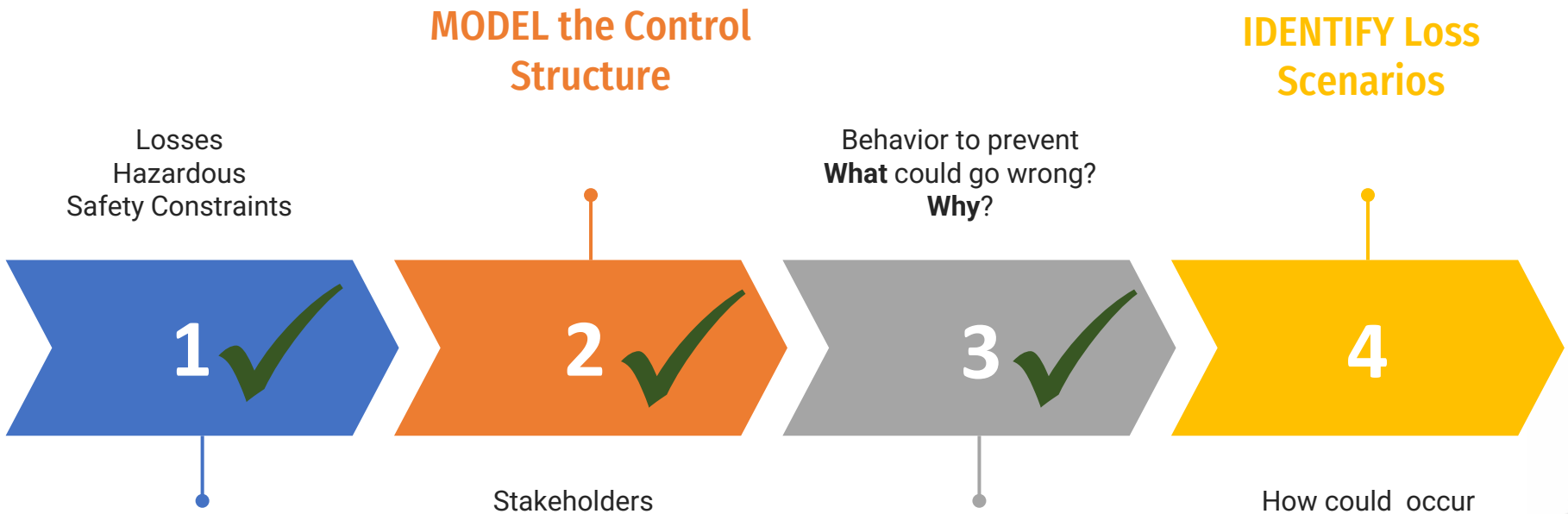
What?
Why?

| Control Action | Not providing causes hazard | Providing causes hazard | Too early, too late, out of order | Stopped too soon, applied too long |
|---|---|---|---|---|
| Command Experiments with Energetic Materials | UCA-2: The operator does not provide Experiment Command when the system has acceptable Process Variables.<br>[H-3] [H-5] [H-6] [H-8] [H-9] | UCA-3: The operator provides Experiment Commands when the Laboratory is not in the correct Environmental Condition for Energetic Materials handling.<br>[H-3] [H-5] [H-6] [H-8] [H-9] | UCA-11: The operator provides Experiment Commands out of order and not in accordance with the operational procedures.<br>[H-1] [H-3] [H-5] [H-6] [H-9] | UCA-13: The operator applied too long the Experiment Commands, changing the expected system components.<br>[H-1] [H-3] [H-5] [H-6] [H-9] |
| Provide Emergency Mode | UCA-16: The operator does not provide Emergency Mode when the Systems Components are out of the safety or experimental limits.<br>[H-1] [H-3] [H-5] [H-6] [H-7] [H-8] [H-9] | UCA-17: The operator provides Emergency Mode when the system is inside predefined conditions for Energetic Materials handling.<br>[H-3] [H-5] [H-6] [H-7] [H-9] | UCA-19: The operator provides Emergency Mode too late after the system achieves critical safety or experimental conditions.<br>[H-1] [H-3] [H-5] [H-6] [H-7] [H-9] | UCA-21: The operator stopped too soon to provide Emergency Mode before the system conditions achieved safety or acceptable experimental limits.<br>[H-3] [H-5] [H-6] [H-9] |

H-3 Laboratory equipment out of calibration standards.

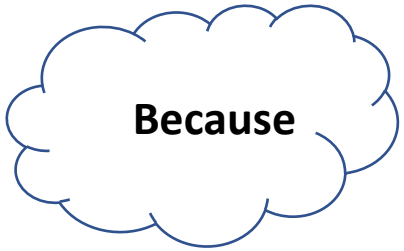
H-9 Energetic Materials are handled without operational training.

# STPA APPLICATION




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

# LOSS SCENARIOS

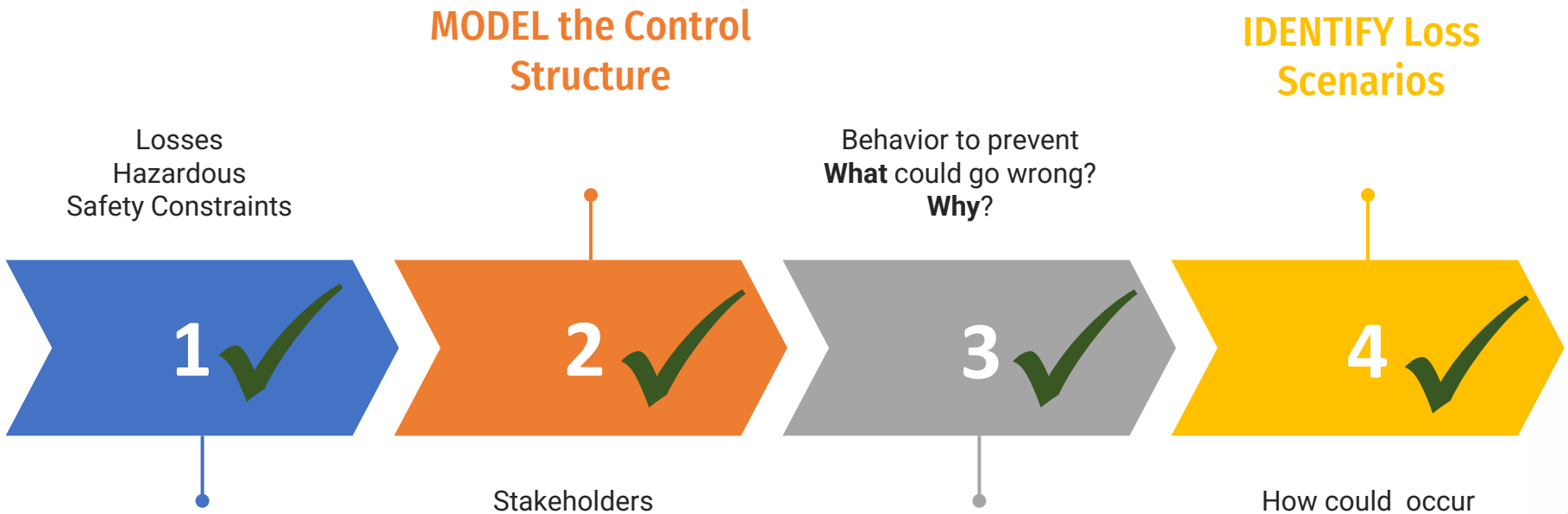



| UCA | Loss Scenarios | Associated Causal Factors and mitigation constraints |
|---|---|---|
| UCA-3 | **Causal Scenario 5:** Experiment command **is provided** **in incorrect Environmental Conditions** for Energetic Materials handling **because** of **errors in the operational procedure** resulting in incorrect analytical data or accidents. | • Operational procedures do **not inform about the setting** for Environmental Conditions.<br>• Operational **procedures are incomplete**, not detailing the process to set the correct Environmental Conditions for each Energetic Materials handling. (**Room temperature**)<br>• Operational **procedures were incorrectly defined**, informing wrong values.<br>• Operational **procedures were not updated** after process changes.<br>• Operational **procedures were incorrectly updated** after process changes. |
| UCA-16 | **Causal Scenario 6:** Emergency mode **is not provided** when the **Systems Components are out of the safety or experimental limits** **because** of a **lack of** Laboratorial facilities, Equipment, Materials, hardware, or tools to execute the procedure for Emergency mode. | • Laboratory facilities, equipment, materials, hardware, or tools are **improperly stored or not identified**.<br>• Laboratory facilities, equipment, materials, hardware, or tools are **unavailable**.<br>• Laboratory facilities, equipment, materials, hardware, or tools are **not operational.**<br>• Laboratory equipment, materials, hardware, or tools are **not correctly calibrated. (Thermometer – Synthesis)** |

# LOSS SCENARIOS


| UCA | Loss Scenarios | Associated Causal Factors and mitigation constraints |
|---|---|---|
| **Provide Experiment Commands with Energetic Materials in correct conditions.** | **Causal Scenario 1:** Laboratorial equipment actuators **execute unproper Experiment commands** due to **calibration flaws**. Resulting in incorrect analytical data or accidents. | • Laboratorial equipment **actuator was not calibrated**.<br>• Laboratorial equipment actuator is with **calibration out of expiration date**. |
| **OR** | **Ambient moisture – FT-IR** | |
| **Provide Emergency Mode when Process Variable Status or Systems Data is out of acceptable conditions.** | **Causal Scenario 2:** Laboratory equipment **actuators execute unproper Experiment commands** due to **operational malfunction**. Resulting in incorrect analytical data or accidents. | • Laboratorial equipment actuator is **out of nominal specification**, needing maintenance or substitution.<br>• Laboratorial equipment **actuator is not operational**.<br>• Laboratorial equipment **actuator was not updated** after process changes.<br>• Laboratorial equipment actuator was **incorrected updated** after process changes. |
| | **Causal Scenario 3:** Laboratorial equipment actuators **does not execute Experiment commands** due to **operational failures.** Resulting in incorrect analytical data or accidents. | |

# STPA APPLICATION




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

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# STPA APPLICATION

- 07 Losses
- 09 System-level Hazards
- 39 Safety Constraints
- 53 Controller Responsibilities
- 22 Unsafe Control Actions from 2 Control Actions analyzed
- 14 Loss Scenarios with Associated Causal Factors and Rationales.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# APPLICABILITY OF THE ANALYSIS

- Any research laboratory that handle Energetic Materials.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# BENEFITS FOR THE RESEARCH CENTERS

- Avoid loss scenarios
- Mitigate the consequence of laboratory hazards
- Reduce experimental rework
- Decrease waste of chemicals

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# CONCLUSION

STPA applied to:

- **Avoid undesired events or to mitigate their consequences** during the Energetic Material Handling in research centers.
- **Propose improvements** for research laboratories and **exemplify benefits for increasing safety** in handling energetic materials.

- Supervisor paper **“Discipline precedes spontaneity”**
- **Why? Prevent** Loss of human life or human injury of laboratory-related personnel.

# CONCLUSION

- **Why? Prevent** Loss of human life or human injury of laboratory-related personnel.

## VLS-1 V03 (São Luis Launch Operation)

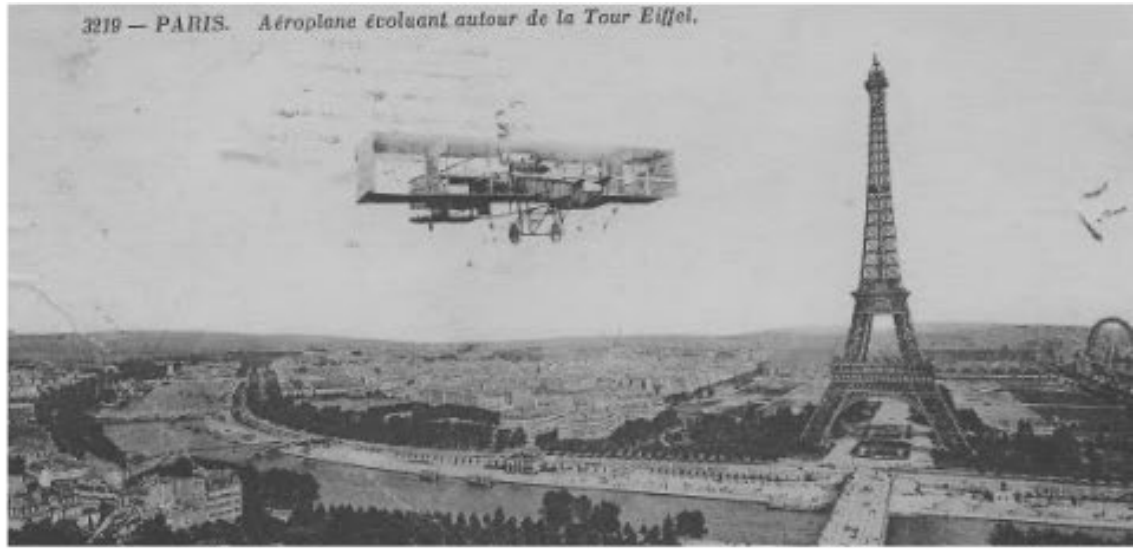

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# REFERENCES


1. Klapötke, Thomas M.. Chemistry of High-Energy Materials. Berlin, Boston: De Gruyter, 2022.
2. Leveson, N. G., Thomas, J. P. STPA Handbook. USA, 2018.
3. Young, W. & Leveson, N. Inside Risks: An Integrated Approach to Safety and Security Based on Systems Theory. Proceedings of the ACM, 2014, Vol 57 no 2, p. 35
4. Leveson, N. G.; Stephanopoulos, G. A system-theoretic, control-inspired view and approach to process safety. AIChE Journal, v. 60, n. 1, 2014, p. 13.
5. Leveson, N. G.; Thomas, J. STPA Primer. USA, 2013.
6. Leveson, N. G. A new accident model for engineering safer systems. Safety Science, v. 42, n. 4, 2004, p. 1-2.
7. Leveson, N. G. Engineering a Safer World: Systems Thinking Applied to Safety, Cambridge, Mass.: The MIT Press, 2012.
8. Walls, L., Revie, M., Bedford, T. Risk, Reliability and Safety: Innovating Theory and Practice. 26th ESREL. Glasgow, Scotland, 2016, p. 129.
9. DCA 800-2/2016: Quality and Safety of Systems and Products at COMAER.
10. Brazilian Technical Standards Association NBR ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories. Rio de Janeiro, 2017.
11. IAE LASI 2013: Safety Code of Laboratory Practice.
12. STAMP Workbench version 2.0.0/ece626, developed by Apache Software Foundation. Copyright (C) 2018 Information-technology Promotion Agency, Japan (IPA).

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# Thank you


"Invent is to imagine what nobody thought; it is to believe what no one has sworn; it is to risk what no one dared; is to accomplish what no one has tried. Invent is transcend."

**Alberto Santos Dumont**

andradeksa@fab.mil.br

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# UNSAFE CONTROL ACTIONS

| Control Action | Not providing causes hazard | Providing causes hazard | Too early, too late, out of order | Stopped too soon, applied too long |
|---|---|---|---|---|
| **Command experiments with Energetic Materials from Operator (Human Controller)**<br><br>**or**<br><br>**Programmed Controller (Autonomous)** | UCA-1: The operator does not provide Experiment Command when the Laboratory is in the correct Environmental Conditions for experiments with Energetic Materials.<br><br>[H-3] [H-5] [H-6] [H-8] [H-9]<br><br>UCA-2: The operator does not provide Experiment Command when the system has acceptable Process Variables.<br><br>[H-3] [H-5] [H-6] [H-8] [H-9] | UCA-3: The operator provides Experiment Commands when the Laboratory is not in the correct Environmental Condition for Energetic Materials handling.<br><br>[H-3] [H-5] [H-6] [H-8] [H-9]<br><br>UCA-4: The operator provides Experiment Commands when Laboratory Equipment or Materials used in the system are with expiration out of date. [H-1] [H-2] [H-3] [H-4] [H-5] [H-7] [H-9]<br><br>UCA-5: The operator provides Experiment Commands when the amount of Energetic Materials is outside of the acceptable range of laboratory safety constraints.<br><br>[H-1] [H-2] [H-3] [H-4] [H-5] [H-9]<br><br>UCA-6: The operator provides Experiment Commands without using proper Personal or Collective Protective Equipment. [H-2] [H-3] [H-5] [H-6] [H-9]<br><br>UCA-7: The operator provides additional Experiment Commands when the Process Variables, system components, and operational procedures indicate that the experiment has finished.<br><br>[H-3] [H-5] [H-9] | UCA-8: The operator provides Experiment Commands too early before the system Process Variables have achieved the indicated values established in the operational procedures for energetic materials handling.<br><br>[H-1] [H-3] [H-5] [H-6] [H-9]<br><br>UCA-9: The operator provides Experiment Commands too early before the laboratory environment conditions are in the acceptable range for energetic materials handling.<br><br>[H-3] [H-5] [H-6] [H-8] [H-9]<br><br>UCA-10: The operator provides Experiment Commands too late, after the prescribed time established in the operational procedures.<br><br>[H-1] [H-3] [H-5] [H-6] [H-9]<br><br>UCA-11: The operator provides Experiment Commands out of order and not in accordance with the operational procedures.<br><br>[H-1] [H-3] [H-5] [H-6] [H-9] | UCA-12: The operator stopped too soon to provide Experiment Commands before the system had achieved the expected Process Variable conditions.<br><br>[H-1] [H-3] [H-5] [H-6] [H-9]<br><br>UCA-13: The operator applied too long the Experiment Commands, changing the expected system components.<br><br>[H-1] [H-3] [H-5] [H-6] [H-9] |

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

# UNSAFE CONTROL ACTIONS

| Control Action | Not providing causes hazard | Providing causes hazard | Too early, too late, out of order | Stopped too soon, applied too long |
|---|---|---|---|---|
| **Provide Emergency Mode from EMH Operator (Human Controller)**<br><br>**or**<br><br>**Programmed Controller (Autonomous)** | UCA-14: The operator does not provide Emergency Mode when the Reaction/Analysis Sensors (Process Variable Status or Systems Data) indicate that the Energetic Materials handling is out of acceptable conditions.<br><br>[H-1] [H-5] [H-6] [H-7] [H-8] [H-9]<br><br>UCA-15: The operator does not provide Emergency Mode when the feedback of the Reaction/Analysis Sensors (Process Variable Status or Systems Data) is uncertain/unknown. [H-1] [H-3] [H-5] [H-6] [H-7] [H-8] [H-9]<br><br>UCA-16: The operator does not provide Emergency Mode when the Systems Components are out of the safety or experimental limits. [H-1] [H-3] [H-5] [H-6] [H-7] [H-8] [H-9] | UCA-17: The operator provides Emergency Mode when the system is inside predefined conditions for Energetic Materials handling.<br><br>[H-3] [H-5] [H-6] [H-7] [H-9] | UCA-18: The operator provides Emergency Mode too early, while the experimental Process Variables Status is in a transient state. [H-3]<br><br>[H-4] [H-5] [H-6] [H-7] [H-9]<br><br>UCA-19: The operator provides Emergency Mode too late after the system achieves critical safety or experimental conditions. [H-1] [H-3] [H-5] [H-6] [H-7] [H-9]<br><br>UCA-20: The operator provides Emergency Mode out of order, not in accordance with work instructions.<br><br>[H-1] [H-5] [H-9] | UCA-21: The operator stopped too soon to provide Emergency Mode before the system conditions achieved safety or acceptable experimental limits. [H-3] [H-5] [H-6] [H-9]<br><br>UCA-22: The operator applied for too long provision of Emergency Mode, achieving sensors inoperative status.<br><br>[H-3] [H-5] [H-9] |