System Theoretic Process Analysis (STPA) / System Theoretic Accident Model and Processes (STAMP) as Acceptable Means of Compliance for Hazard Analysis

Military Airworthiness Conference

MAC2018

María Molina Martinez

Safety Section, Airworthiness Area - INTA

Madrid, 26/09/18

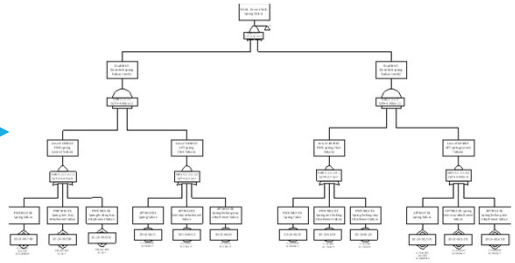
Outline

- Possible areas for improvement for Hazard Analysis
- STAMP/STPA
- STPA as an acceptable mean for compliance
- CAST
- Conclusions

Accident Causality Model

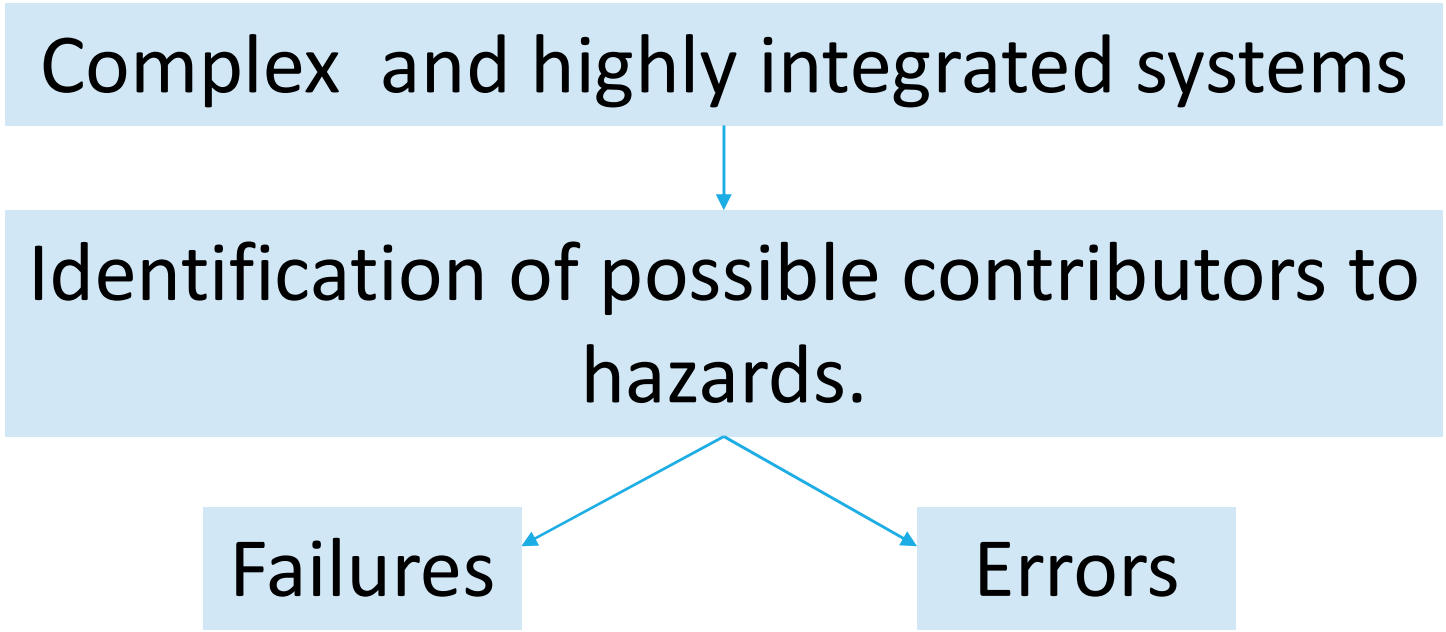
All hazard analysis is based on some conception by the analyst (and built into the analysis technique) of how and why accidents occur. (Nancy Leveson, STPA Primer)

Hazard analysis →based on an accident model.

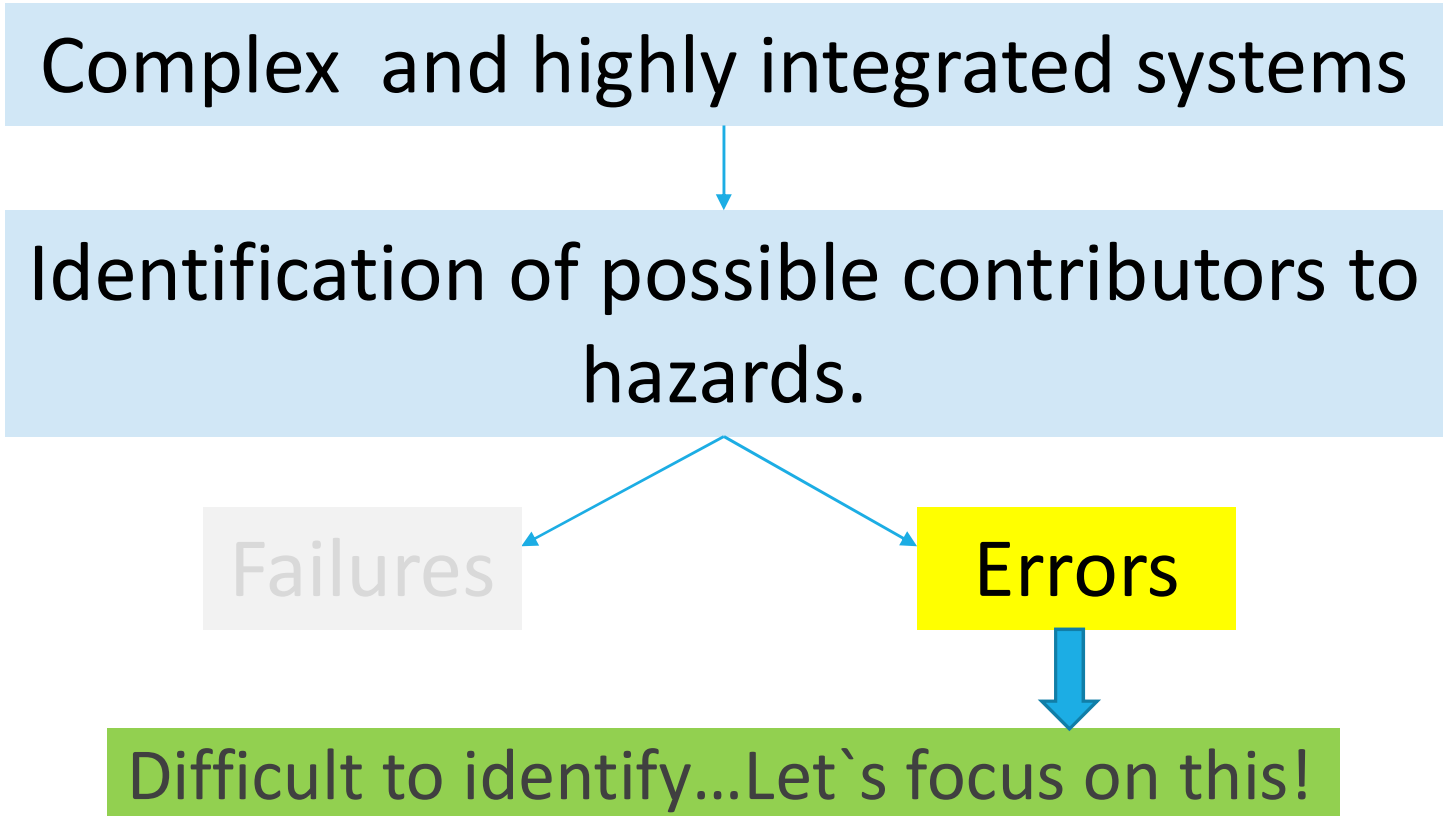


Let`s look for areas of improvement!

Thinking of possible areas of improvement…



Thinking of possible areas of improvement…



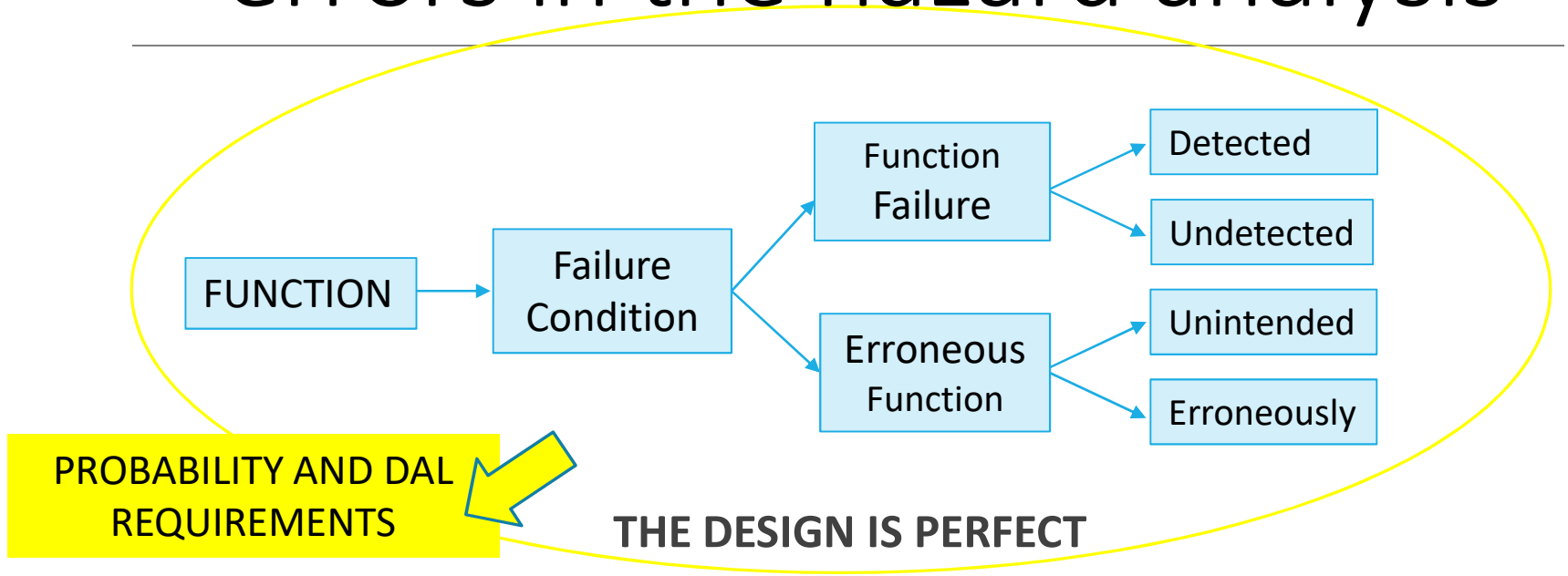
Thinking of possible areas of improvement…

Complexity → **Design errors**

1. ~~Situational Awareness errors?~~
2. ~~High level software requirements errors?~~
3. ~~Component interaction design errors?~~

Hazard Analysis → Requirements

1.Situational Awareness Human errors in the hazard analysis



…Nothing failed…

Design was just not adequate

2. Software requirements errors

- SW vs Requirements Errors
- Requirements, design or implementation errors→ development assurance processes.

ARP 4754A → requirements correct & complete →SW and AEH

- DO-178C & DO-254 asumption

- Correct: unambiguous, verifiable, and consistent with other requirements.
- Completeness: degree to which the requirement satisfies users, maintainers, and certifiers needs.

Can the requirements still be unsafe?

Tools →  → Safe SW requirements

Designer

3. Component interaction design errors

- Can an accident be caused by interactions among several components in complex systems?
  - Without component failures
  - All components operating as designed

- Can the requirements be flawed?

Complexity of interactions leads to unexpected system behavior difficult to anticipate.

STAMP (Systems Theoretic Accident Model and Process)

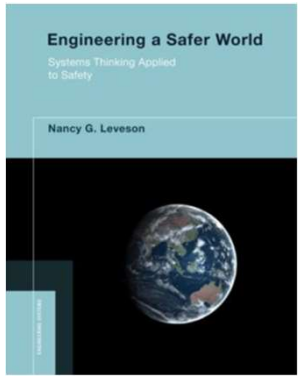
STAMP →accident model →based on System Theory

STPA→hazard analysis method

Both developed at MIT by prof. Nancy Leveson and her team.

For complex, sociotechnical systems

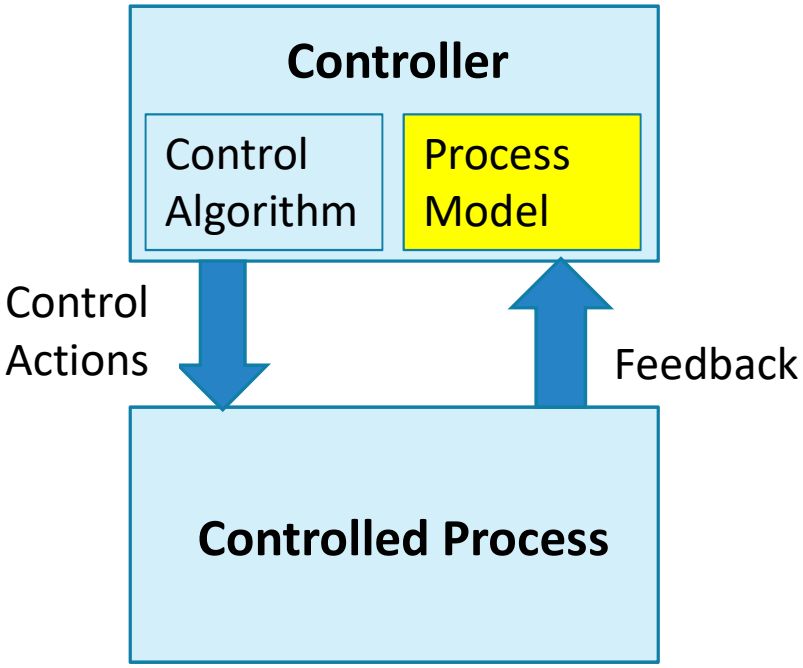
Main principle: **Safety is a control problem**



Accidents results from inadequate control, not from chains of failure events

Free download at: https://mitpress.mit.edu/books/engineering-safer-world

STAMP (Systems Theoretic Accident Model and Process)

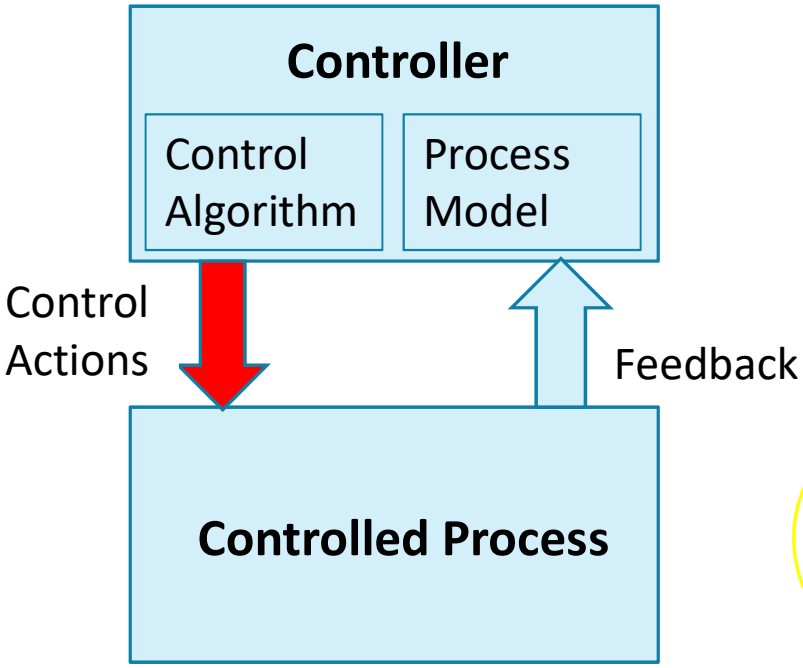


Process model (beliefs) formed based on feedback and other information

Control algorithm determines appropriate control actions given current beliefs

Author: Nancy Leveson- Engineering a Safer World

STAMP (Systems Theoretic Accident Model and Process)



Four types of **unsafe control actions**:

1)Control actions required for safety are not given

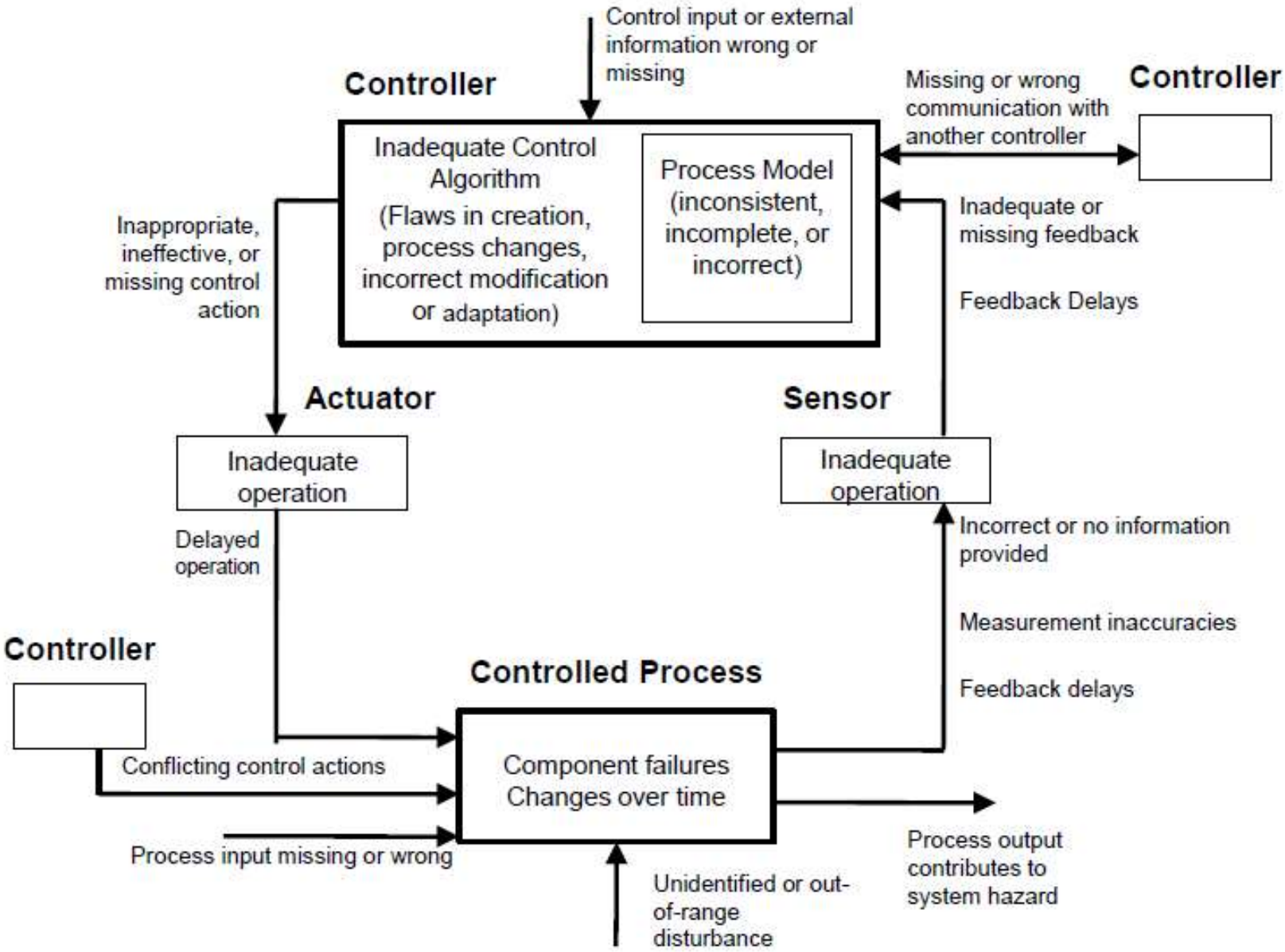
FUNCTION FAILURE

2)Unsafe ones are given

3)Potentially safe control actions but given too early, too late

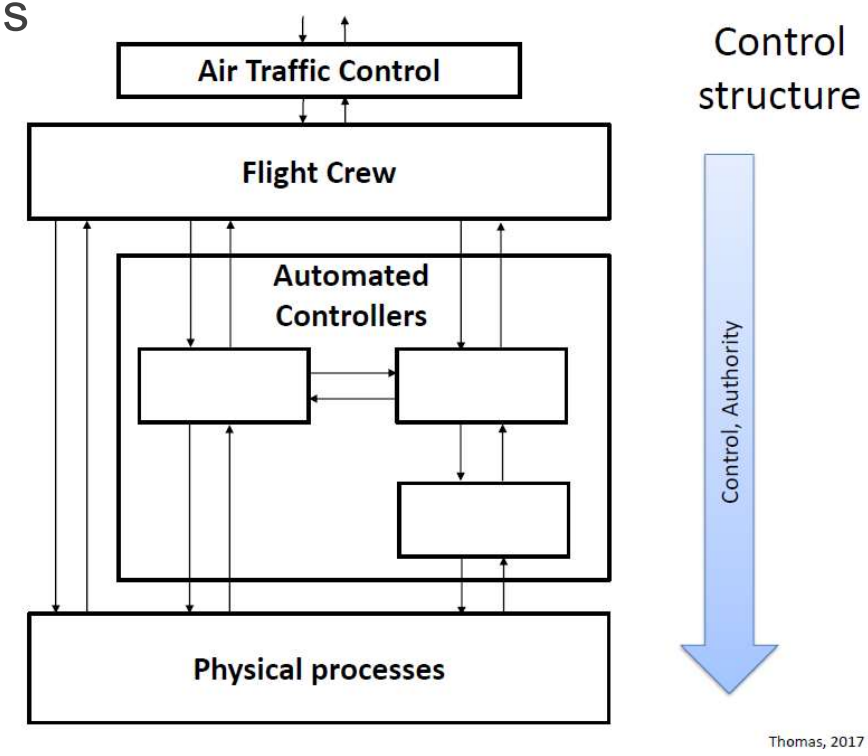
4)Control action stops too soon or applied too long

ERRONEOUS FUNCTION


Control input or external information wrong or missing
Controller
Inadequate Control Algorithm
(Flaws in creation, process changes, incorrect modification or adaptation)
Process Model (inconsistent, incomplete, or incorrect)
Missing or wrong communication with another controller
Controller
Inappropriate, ineffective, or missing control action
Inadequate or missing feedback
Feedback Delays
Actuator
Sensor
Inadequate operation
Inadequate operation
Delayed operation
Incorrect or no information provided
Measurement inaccuracies
Feedback delays
Controller
Controlled Process
Conflicting control actions
Component failures
Changes over time
Process input missing or wrong
Unidentified or out-of-range disturbance
Process output contributes to system hazard

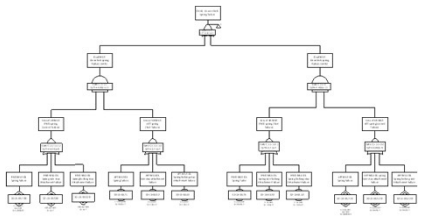
STPA (System-Theoretic Process Analysis)

- Identify system accidents, hazards
- Draw functional control structure
- Identify unsafe control actions
- Identify accident scenarios

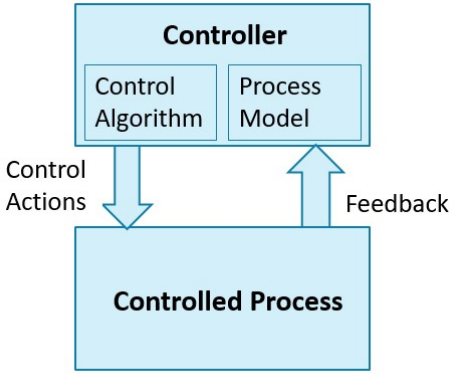


Thomas, 2017

STPA as an aceptable mean for compliance



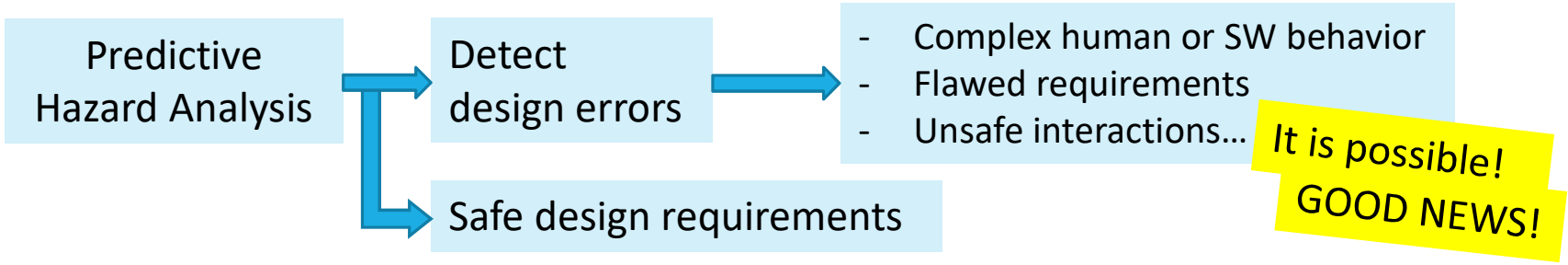
FUNCTION FAILURE → COMPONENT FAILURES



Control Actions required for safety are not given

- COMPONENT FAILURES → Possible failures identified. No data: redundancy, probability?
- Wrong process model → High level SW requirements
- Wrong algorithm
- Wrong feedback → Design requirements

STPA as an aceptable mean for compliance



Failure of components identified, but no data available for redundancy or minimum reliability.

WAY AHEAD:

- Let´s determine how STPA could be used in combination with other existing traditional techniques and guidance material
- Let´s look for international consensus on the use of STPA

FOR THAT REASON: It is strongly recommended to include implementation of STPA on a pilot certification project

CAST-Causal Analysis using System Theory

How do we find inadequate control that caused the accident?

Investigation reports should explain

- **Why it made sense for people to do what they did** rather than judging them for what they allegedly did wrong, and
- What **changes** will reduce likelihood of accident happening again

Basic Process:

- Identify **system hazard** violated and **system safety design constraints**.
- Construct **safety control structure** as it was designed to work.
- For each component, determine if it **fulfilled its responsibilities** or provided **inadequate control**.

Conclusions

- Hazard Analysis could include more design errors as possible contributors to accidents.
- It is strongly recommended to include implementation of STPA on a pilot certification program, so further studies are accomplished to integrate STPA with traditional techniques.
- For accident investigation, it is recommended the use of CAST.
- For concrete event analysis or critical processes, STPA could also be really useful and easy to implement.

Thank you!

Bibliography

- FAR/CS: Parts 23/25/27/29. 1309 /AC_AMC_GM
- ARP 4761
- ARP 4754A
- MIL-STD-882E
- Engineering a Safer World (Leveson, 2011)
- STPA Handbook. https://psas.scripts.mit.edu/home/

Recognition:

- Dr. Nancy Leveson, MIT
- Dr. John Thomas, MIT

Contact

- molinamm@inta.es
- +34915201622