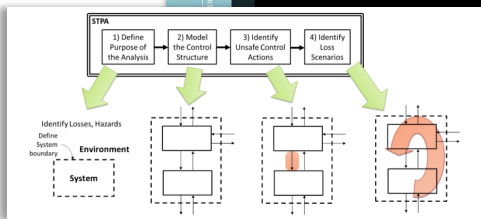
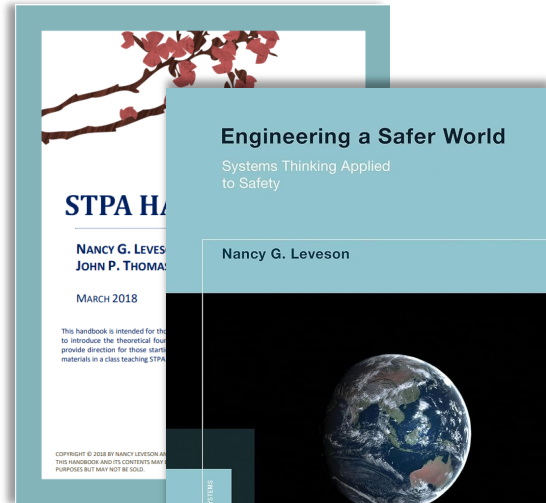


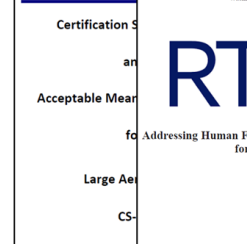
➔ **STPA loss scenarios for human-systems integration**

2025 MIT STAMP Workshop

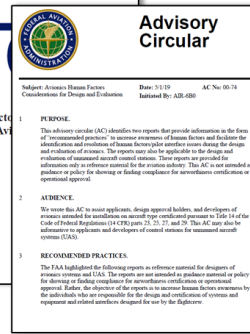
Embraer methodology to conduct the discussions on this topic includes previous experiences and the following reference:



AMC 25.1302 - Installed Systems and Equipment for Use by the Flight Crew (2007)



DO-372 - Addressing Human Factors / Pilot Interface Issues for Avionics (2017)



AC 00-74 Avionics Human Factors Considerations for Design and Evaluation (2019)

An Improved Design Process for Complex, Control-Based Systems Using STPA and a Conceptual Architecture¹

Nancy Leveson
 Engineering Systems Lab
 Aeronautics and Astronautics Dept.
 MIT
 January 11, 2020

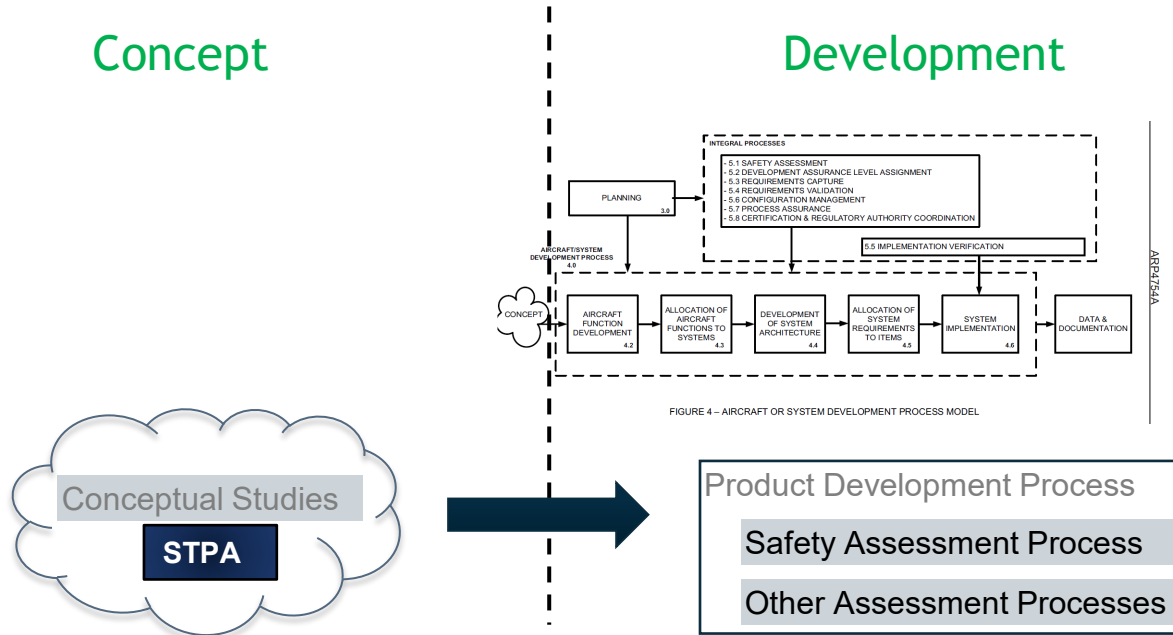
Considering our practice, the STAMP approach enriches the discussion between the specialists from distinct domains, such as safety, supportability, security and **human factors** to determine the adequate decision-making that will influence the design of the system



In that context, this discussion will complement the **coverage of human-systems integration analysis** for Systems Engineering trade-off to create **recommendations and flowing-down** through requirements during the development and subsequent stages.

Concept

Development



Conceptual Studies

STPA

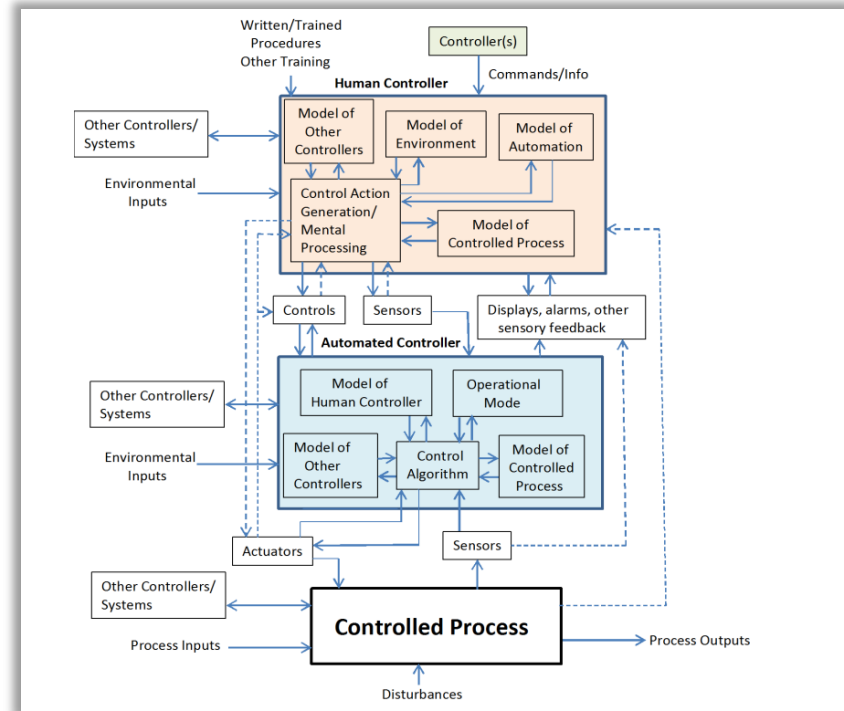
Product Development Process

Safety Assessment Process

Other Assessment Processes

How to extend a STPA analysis considering human-system integration aspects?

- 1) Establish the generic conceptual architecture as reference
- 2) Define which conceptual control model elements are going to be considered at the extended analysis
- 3) Analyze with Human Factors specialist in which interactions the human controller we could have an impact coming from contextual elements
- 4) Evaluate the impact of aspects that could influence actions such as System Context, human beliefs, behaviors, and thought process.



Leveson, N. "An Improved Design Process for Complex, Control-Based Systems". Engineering Systems Lab, MIT, 2020

By following these steps, the conceptual control model elements were associated with aspects that could influence actions. Thus, the result is the “relationship matrix”.

Conceptual Control Model Elements

- *Model of Other Controllers*
- *Model of Environment*
- *Model of Automation*
- *Control Action Generation/ Mental Processing*
- *Model of Controlled Process*

Categories

- *Excessive Workload*
- *Low Workload*
- *Fatigue*
- *Training (Tech Info)*
- *Training (Procedure)*
- *Mental Model*
- *Security*
- *Interface*
- *Situation Awareness*
- *Complacency*
- *Incapacitation*

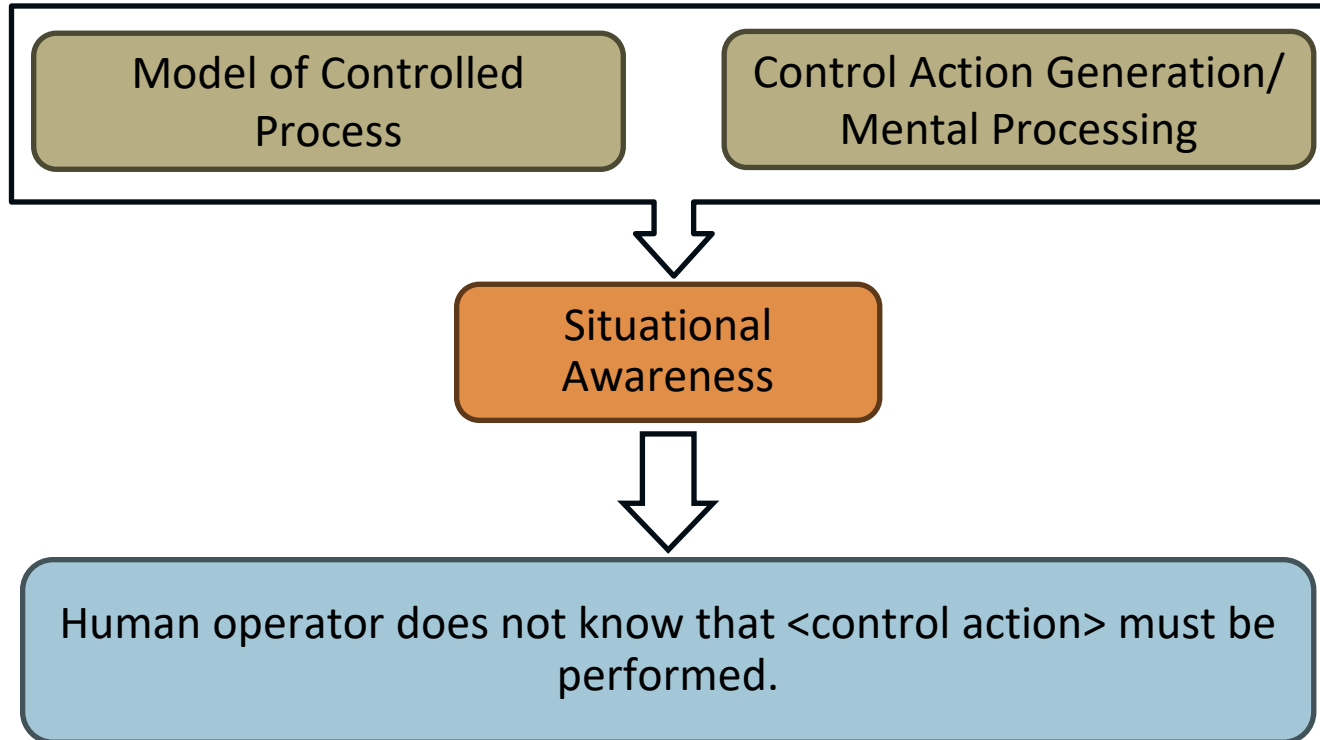
Relationship between Conceptual Control Model Elements and Categories

	EW	LW	FAT	T(TI)	T(P)	MM	SEC	INT	SA	COM	INC
Model of Other Controllers				X	X	X		X			
Model of Environment						X		X			
Model of Automation				X	X			X		X	
Control Action Generation/ Mental Processing	X	X	X	X	X	X	X	X	X	X	X
Model of Controlled Process				X	X				X	X	

Relationship between Conceptual Control Model Elements and Categories

	EW	LW	FAT	T(TI)	T(P)	MM	SEC	INT	SA	COM	INC
Model of Other Controllers				X	X	X		X			
Model of Environment						X		X			
Model of Automation				X	X			X		X	
Control Action Generation/ Mental Processing	X	X	X	X	X	X	X	X	X	X	X
Model of Controlled Process				X	X				X	X	

Scenario analysis considering the Situational Awareness influence:



Situational
Awareness

```
graph TD; SA[Situational Awareness] --> SD[Scenario Description: Human operator does not know that <control action> must be performed.]; SD --> RE[Recommendation Example: The training system should inform when the <control action> must be performed, including: - during upon TBS conditions];
```

Scenario Description

Human operator does not know that <control action> must be performed.

Recommendation Example

The training system should inform when the <control action> must be performed, including:

- during upon TBS conditions

Human Scenario Type	Scenario Description	Recommendations examples
Excessive Workload	Excessive workload performing tasks leads to human operator performing hazardous control action.	The system should provide a work environment that maintains an adequate human operator workload including tasks: - control action
	Low workload performing tasks leads to low attention (distractions) and human operator performing hazardous control action.	The system should provide a work environment that maintains adequate human operator engagement, and minimizes the negative impact of extended periods of low workload, including tasks: - control action
Fatigue	Fatigue interferes with human operator's capability to perform control action.	The system should provide a work environment that allows the human operator to perform her/his duties without unreasonable concentration or fatigue including tasks: - control action
Training (Technical Information)	Human operator performs hazardous control action based on wrong/unclear technical information from system.	The Training Material should contain system technical information necessary for the human operator to perform control action.
Training (Procedure)	Human operator does not know how to perform control action.	The training system should qualify human operator to perform control action procedure.
	Human operator receives correct feedback/information but does not interpret it correctly	
Mental Model	Human operator believes she/he knows how to perform control action based on previous experience.	The required skill for the human operator profile should include proficiency to perform control action for this specific system.

Human Scenario Type	Scenario Description	Recommendations examples
Security	Unauthorized person acting as a human operator performs hazardous control action.	The system should ensure authentication of human operator identity.
	Interface with human operator to input control action facilitates hazardous control action.	The system should provide an interface to input control action that allows the human operator to safely accomplish this task.
Situational Awareness	Human operator does not know that control action must be performed.	The training system should inform when the control action must be performed, including: - during upon TBS conditions
	Human operator does not know that hazardous control action was performed (correctly/incorrectly).	The system should inform the human operator if control action was performed (incorrectly OR correctly).
Complacency	Human operator believes that automation will perform control action.	The system should inform the human operator about the automation status (availability, modes).
		The system should inform the human operator when an intervention action is required.
Incapacitation	Human operator is unable to perform the control actions.	The training system should orient the human operator with the capabilities designed for the automation.
		The system should monitor human operator incapacitation. The system should initiate emergency procedure for safe operation.

Conclusion

- *Categories of Human Factors Aspects can improve human system integration analysis through STPA*
- *This strategy does not aim to limit the scope of the STPA analysis, but to support it*
- *A clear process to structure the categorization is essential to obtain results that will extend the STPA analysis regarding human-controller perspective.*
- *The application of this process enables early discussions regarding the Human factors influence at the system requirements being an opportunity for a more integrated development*

➔ STPA loss scenarios for human-systems integration

Bruna Silva Queiroz

Chief Engineer Office
EMBRAER

São José dos Campos, Brazil
bruna.queiroz@embraer.com.br

Thiago Rodrigues da Costa

Chief Engineer Office
EMBRAER

São José dos Campos, Brazil
thiago.rodrigues@embraer.com.br

Carina Carla Silva

Chief Engineer Office
EMBRAER

São José dos Campos, Brazil
carina.silva@embraer.com.br

Marcelo de Lima B. Moreira

Chief Engineer Office
EMBRAER

São José dos Campos, Brazil
marcelo.moreira@embraer.com.br

➤ STPA loss scenarios for human-systems integration

- [1] Leveson, Nancy G. Engineering a safer world: Systems thinking applied to safety. The MIT Press, 2016.
- [2] Leveson, Nancy G., and John P. Thomas. "STPA handbook." Cambridge, MA, USA (2018).
- [3] Leveson, N. "An Improved Design Process for Complex, Control-Based Systems". Engineering Systems Lab, MIT, 2020.
- [4] AMC 25.1302 - Installed Systems and Equipment for Use by the Flight Crew (2007)
- [5] DO-372 - Addressing Human Factors / Pilot Interface Issues for Avionics (2017)
- [6] AC 00-74 Avionics Human Factors Considerations for Design and Evaluation (2019)