STAMP CONSIDERATIONS AT EMBRAER

June 2023

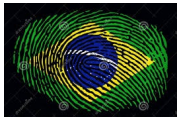
THE CONTENT PRESENTED HERE CONTAINS THE VISION OF STAMP APPLICATION THAT FITS THE CONTEXT OF EMBRAER

SECTION 1: *Timeline and Embraer Context*

SECTION 2*: Knowledge Foundation*

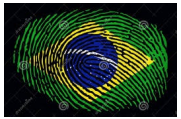
SECTION 3: *Formalization at Embraer Systems Engineering Process*

SECTION 4*: Perceived Gains*

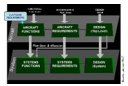


STAMP AT EMBRAER: TIMELINE AND CONTEXT

The first contact with STAMP methodology was in 2011 with Professor Nancy and led to a relevant work few years later in applying STPA on a subsystem of our E2 aircraft. The results of this work served a lot as a consistent step in industry learning from academy and feedbacking knowledge gained. In parallel we invested even more intensely on the conceptual basis for the methodology which is the same for Systems Engineering.



EMBRAER



Scott Jackson

S7VEN

S7VEN Formation

FAA SW Conference

Nancy Levenson

Workshop STAMP/STPA at ITA

Nancy Levenson

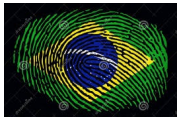
STPA Application AMS E2 Andrea

2011

2023

STAMP AT EMBRAER: TIMELINE AND CONTEXT

There was a very important contribution from Embraer in formalizing the use of the methodology as a Mean Of Compliance for Cybersecurity Assessment on Commercial Aviation. Subsequent work in different contexts, business units, and for different purposes, led to the advancements in our understanding of the benefits of using the methodology considering Embraer context and what works for us.



2011

Scott Jackson

FAA SW Conference

Nancy Levenson

S7VEN Formation

Nancy Levenson

Workshop STAMP/STPA at ITA

Nancy Levenson

STPA Application AMS E2 Andrea

STPA-Sec Application

STPA-Sec CyberSecurity MOC

Visit from Varun from FAA STPA-Sec

DLR AGILE

Invitation for Agile Open Day

S7VEN migration to GSW

STPA Application - Landing Gear, External Lights

STPA Application
- UAS Operation
- SKY
- Autonomous flight
- Phenom 300 Avionics

Internship Program

STPA tool study development

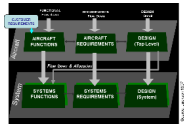
Invitation for STPA Liason Recommendation Pratics Task Force Felipe

STPA Application for Supportability

STPA Application
- C390
- RPAS Operation
- eVTOL
- SuperTucano

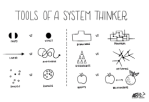
2023

STAMP AT EMBRAER: KNOWLEDGE FOUNDATION

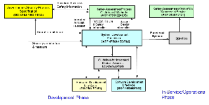


Systems Engineering

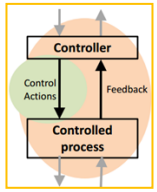
STAMP



Systems Thinking



Certification Framework

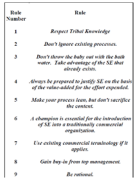


Nancy Leveson

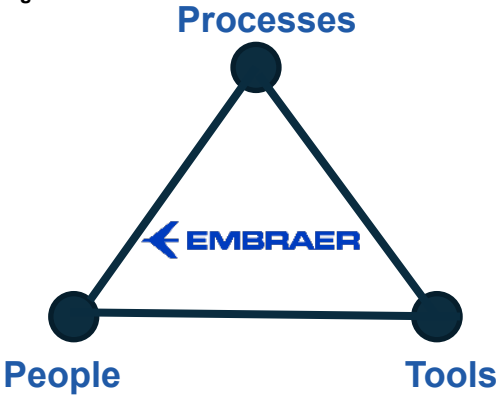
Critical Behavior

Gentry Lee

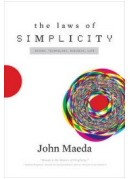
Rules



Scott Jackson

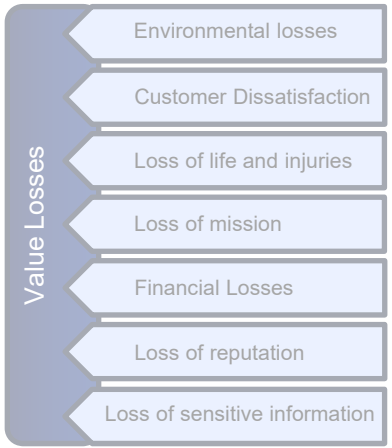


STPA



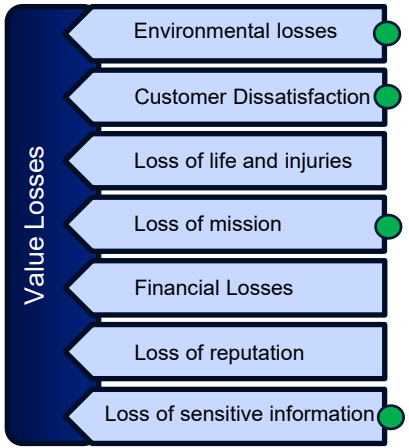
The STAMP Team at Embraer is part of the Systems Engineering group at the Chief Engineer Office to assure consistency in the analysis considering required qualification and vision.

Considering our practice, the methodology was proven to provide good results in supporting the requirements engineering process in formalizing concerns of distinct system emergencies such as safety, security, supportability in an integrative manner facilitating trade-offs.



STAMP AT EMBRAER: FORMALIZATION AT OUR SYSTEMS ENGINEERING PROCESS

Used to assess losses beyond traditional safety focus, but also relevant to business in a structured manner. The coverage enriches completeness of the first system requirements set including measures to treat mapped hazardous scenarios.



The application of STAMP methodology is used at Embraer to complement well established traditional analyzes

In that context of Requirements Engineering, the result of the analysis conducted during the concept stage will reflect in the design, operations of the systems by flowing-down the requirements during the development and subsequent stages.

Concept

Development

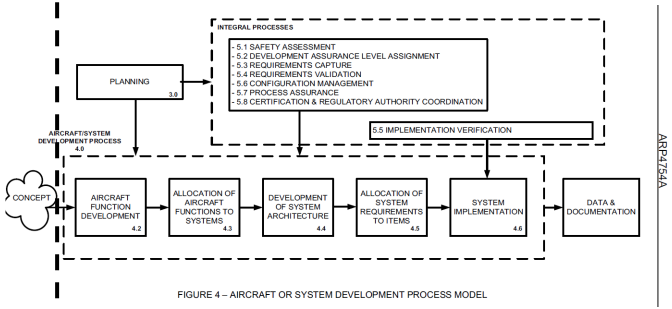


FIGURE 4 – AIRCRAFT OR SYSTEM DEVELOPMENT PROCESS MODEL

Conceptual Studies

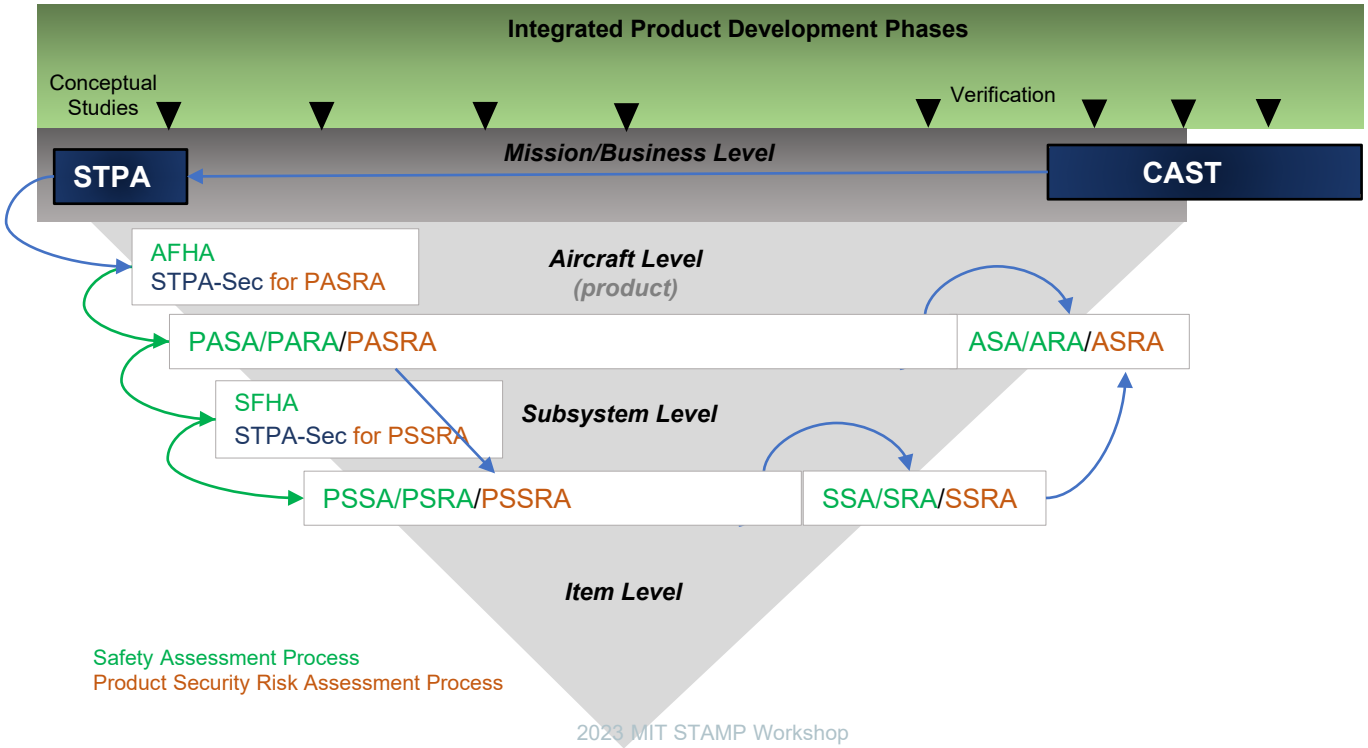
STPA

Product Development Process

Safety Assessment Process

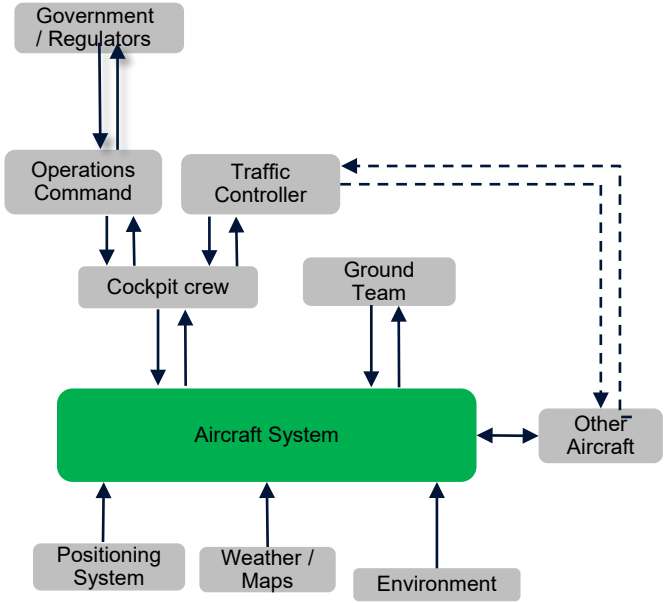
Other Assessment Processes

The analyses are conducted at the “mission-level” or “product system-level” free from design specifications in order to focus on the operations and on its inherent hazardous contexts and interactions.



STPA AS A PRELIMINARY HAZARD ANALYSIS TO COMPLEMENT (SAFETY AND OTHER) ANALYZES

i. Structure the understanding of the operation from a control perspective

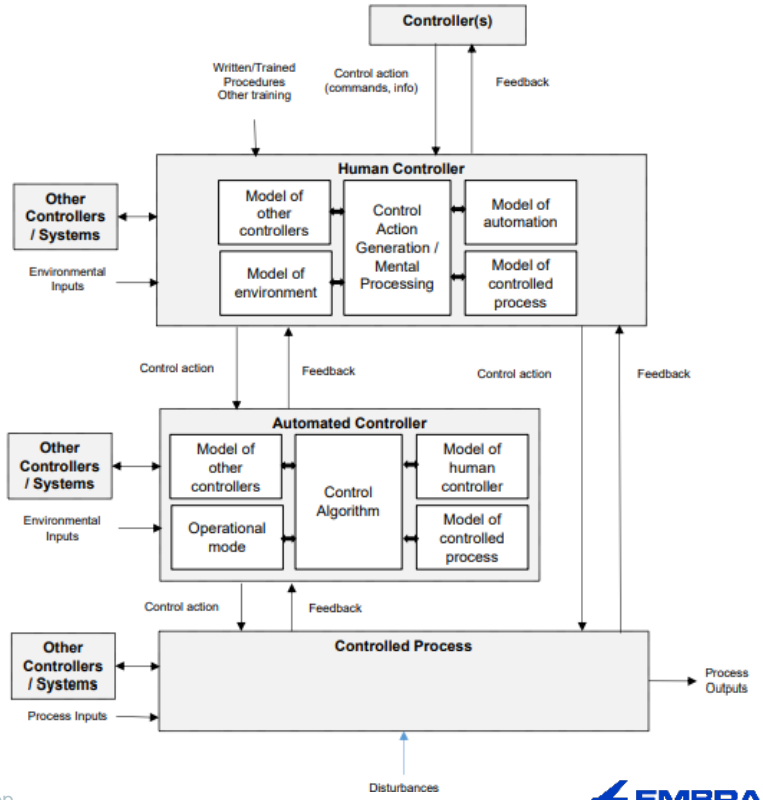


STPA AS A PRELIMINARY HAZARD ANALYSIS TO COMPLEMENT (SAFETY AND OTHER) ANALYZES

i. Structure the understanding of the operation from a control perspective

ii. More comprehensive context scenarios including Human Interaction

iii. More comprehensive context scenarios considering software intensive systems



STPA AS A PRELIMINARY HAZARD ANALYSIS TO COMPLEMENT (SAFETY AND OTHER) ANALYZES

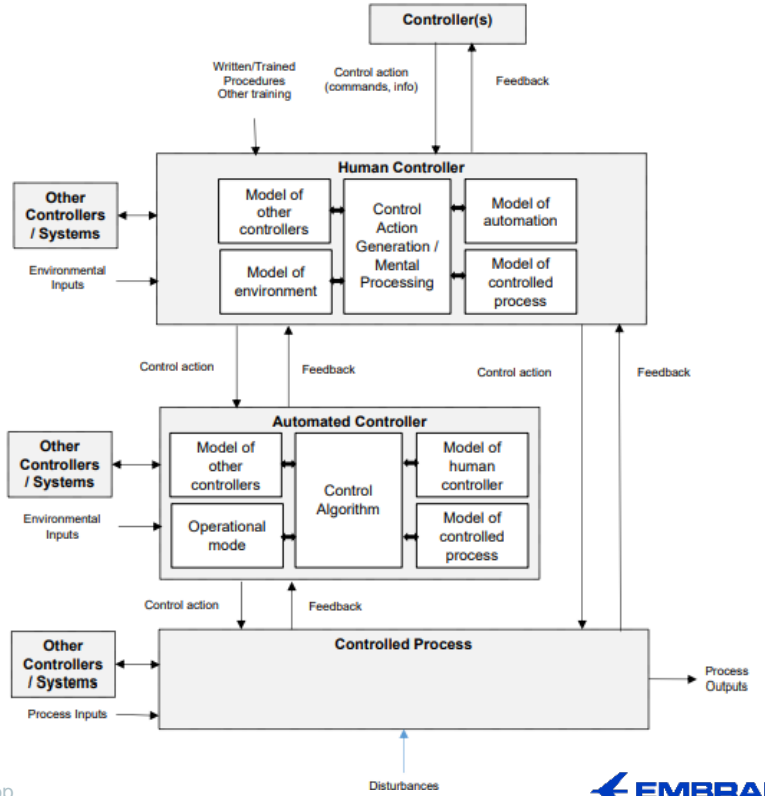
i. Structure the understanding of the operation from a control perspective as input for subsequent safety analysis

ii. More comprehensive context scenarios including Human Interaction

iii. More comprehensive context scenarios considering software intensive systems

iv. Traceability from operational recommendations, system requirements to hazards

v. Subsequent traditional analysis for design the product proceeds as we know it



EMBRAER

Carina Carla Silva
carina.silva@embraer.com.br
SYSTEMS ENGINEERING TEAM