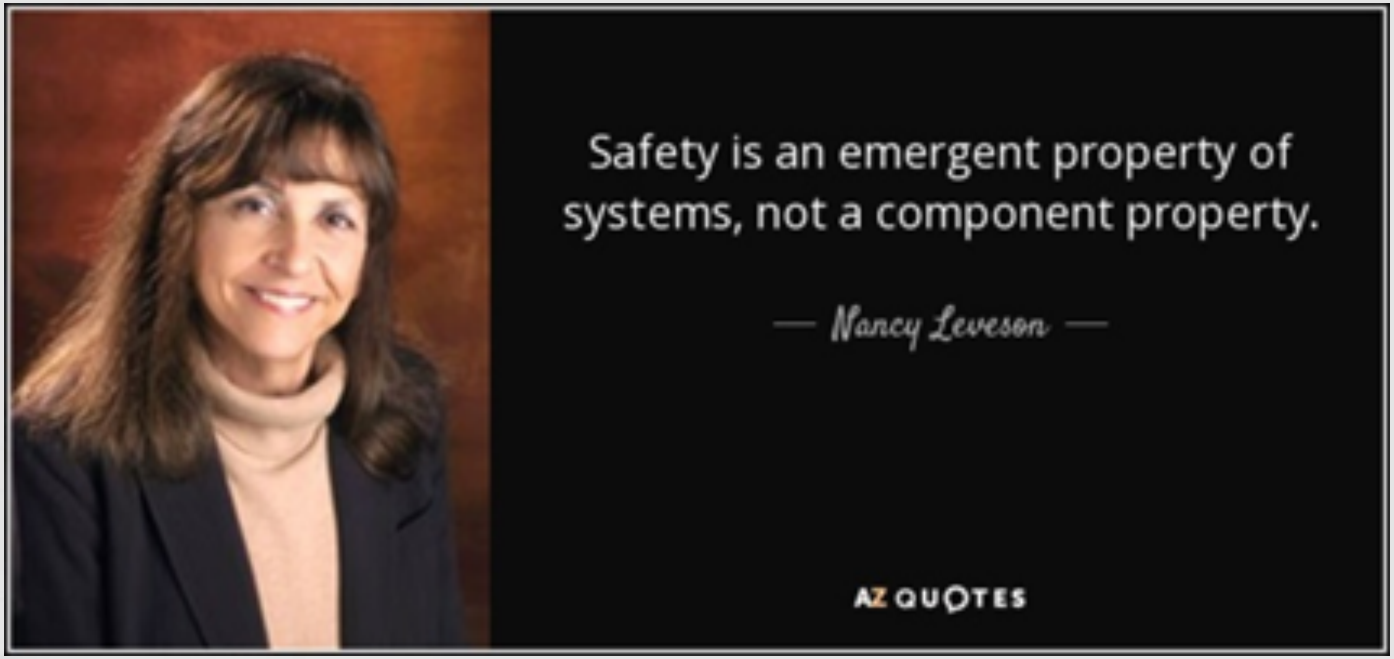
EMBRAER

Challenges for Introducing STAMP/ STPA

Marcos Antonio Viana Tavares
Systems Engineering and Software Manager
Chief Engineer Office

Mar/27/2018

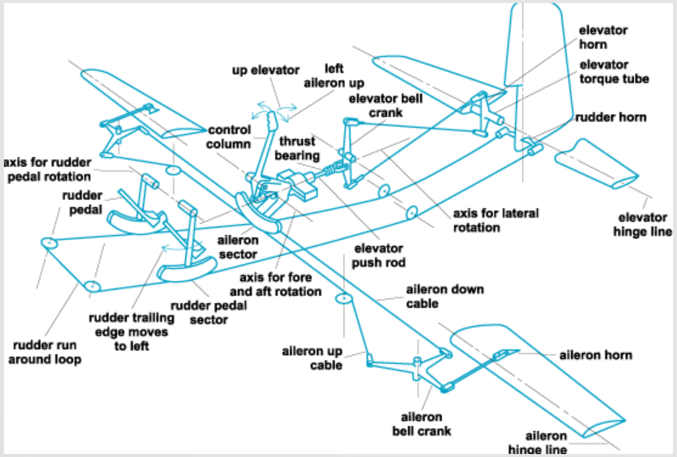


Safety is an emergent property of systems, not a component property.

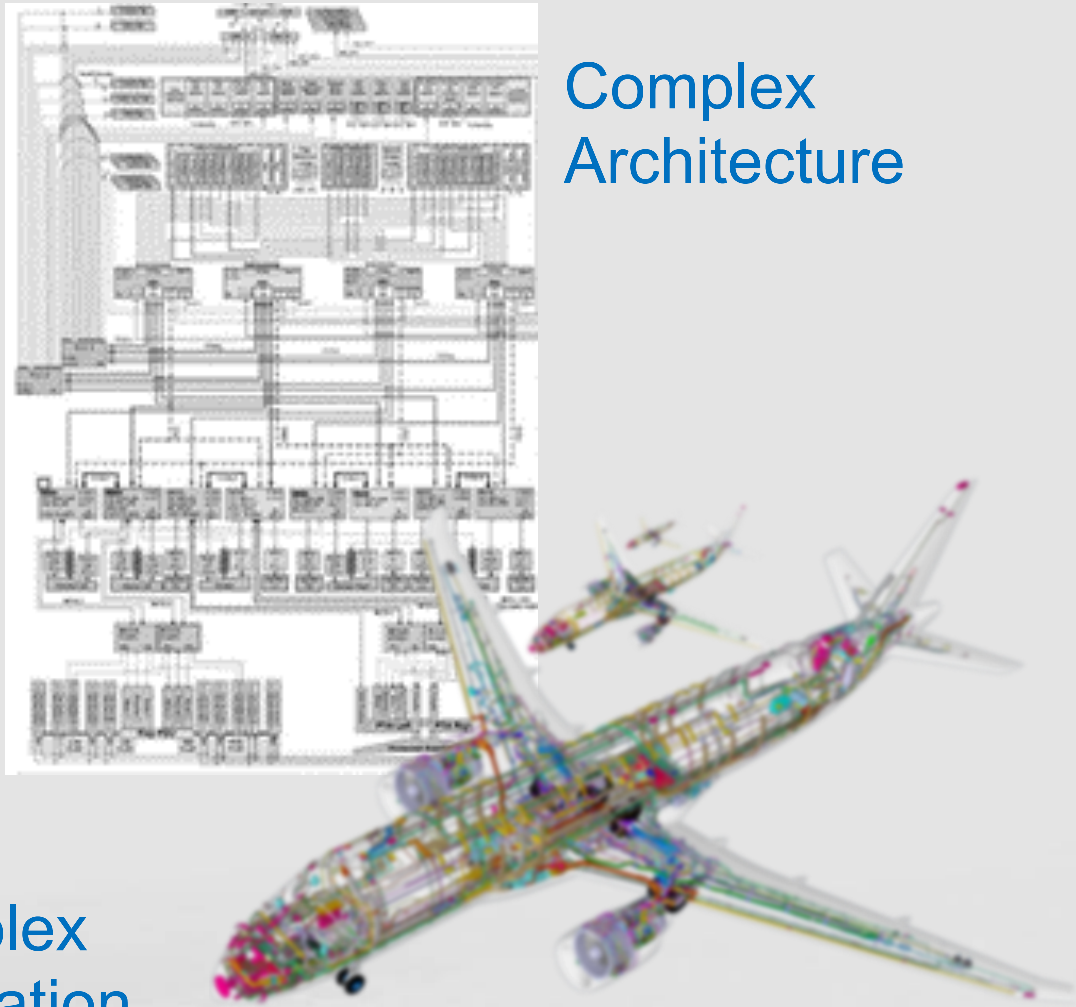
— Nancy Leveson —

Context

Systems Evolution



Simple system

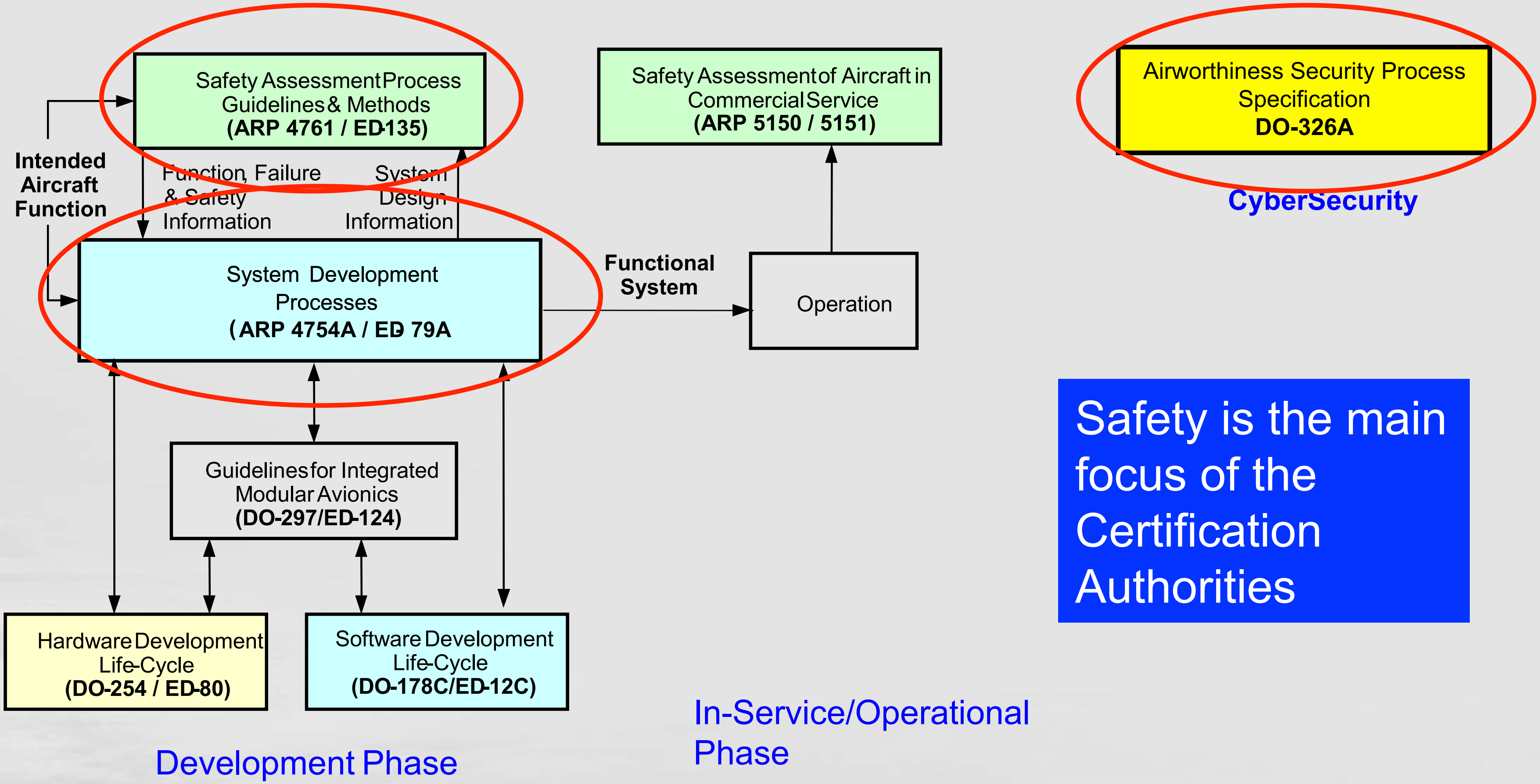


Complex Architecture

Complex Installation

Context

Certification Framework

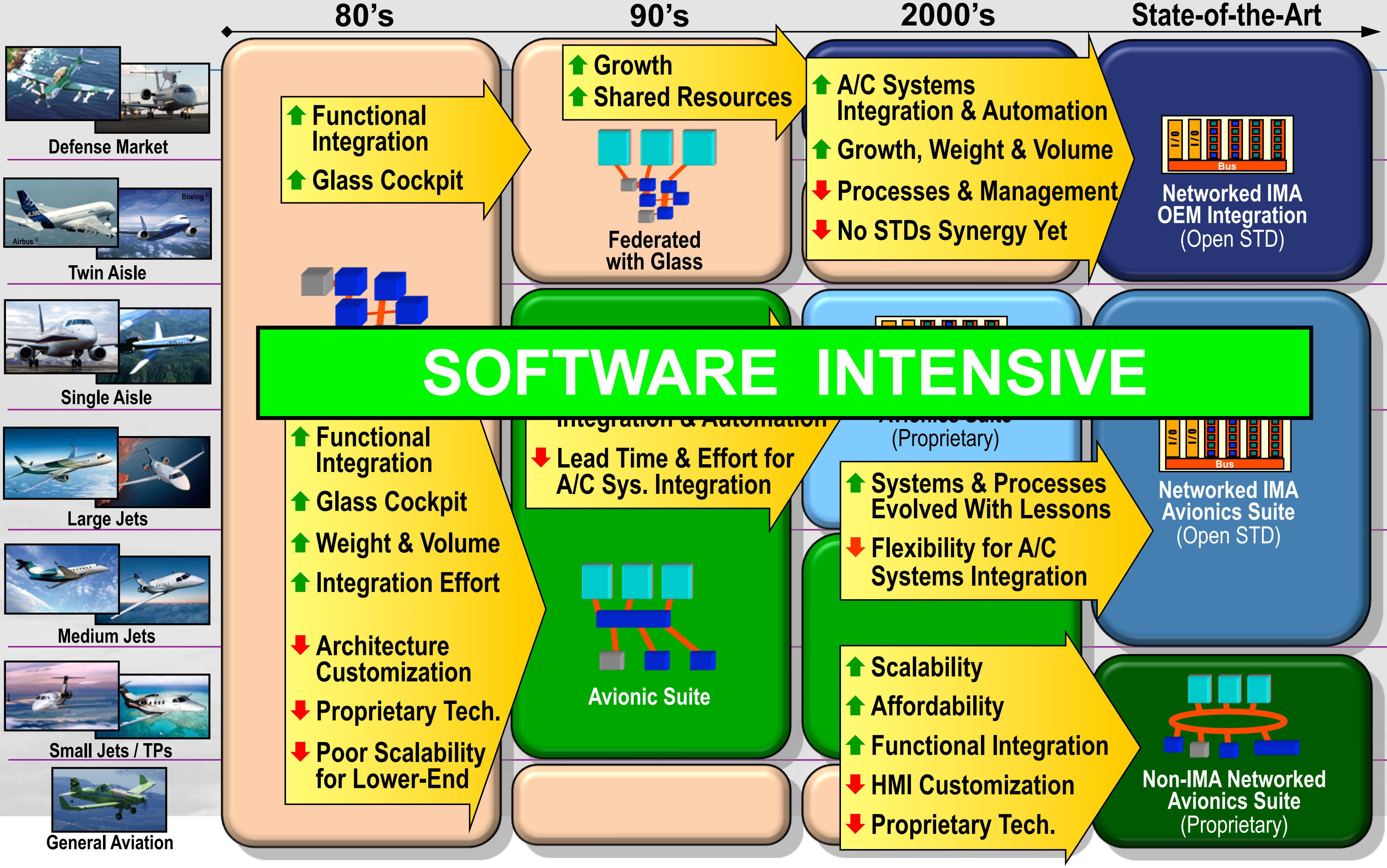


Safety Assessment Process Guidelines & Methods (ARP 4761 / ED135)
Safety Assessment of Aircraft in Commercial Service (ARP 5150 / 5151)
Airworthiness Security Process Specification DO-326A
CyberSecurity
Intended Aircraft Function
Function, Failure & Safety Information
System Design Information
System Development Processes (ARP 4754A / ED 79A
Functional System
Operation
Guidelines for Integrated Modular Avionics (DO-297/ED-124)
Hardware Development Life-Cycle (DO-254 / ED-80)
Software Development Life-Cycle (DO-178C/ED-12C)
Development Phase
In-Service/Operational Phase

Safety is the main focus of the Certification Authorities

Context

Complexity and Highly Integrated Systems



80’s

90’s

2000’s

State-of-the-Art

Defense Market

Twin Aisle

Single Aisle

Large Jets

Medium Jets

Small Jets / TPs

General Aviation

⬆ Functional Integration

⬆ Glass Cockpit

⬆ Growth

⬆ Shared Resources

Federated with Glass

⬆ A/C Systems Integration & Automation

⬆ Growth, Weight & Volume

⬇ Processes & Management

⬇ No STDs Synergy Yet

Networked IMA OEM Integration (Open STD)

SOFTWARE INTENSIVE

⬆ Functional Integration

⬆ Glass Cockpit

⬆ Weight & Volume

⬆ Integration Effort

⬇ Architecture Customization

⬇ Proprietary Tech.

⬇ Poor Scalability for Lower-End

Integration & Automation

⬇ Lead Time & Effort for A/C Sys. Integration

Avionic Suite

(Proprietary)

⬆ Systems & Processes Evolved With Lessons

⬇ Flexibility for A/C Systems Integration

Networked IMA Avionics Suite (Open STD)

⬆ Scalability

⬆ Affordability

⬆ Functional Integration

⬇ HMI Customization

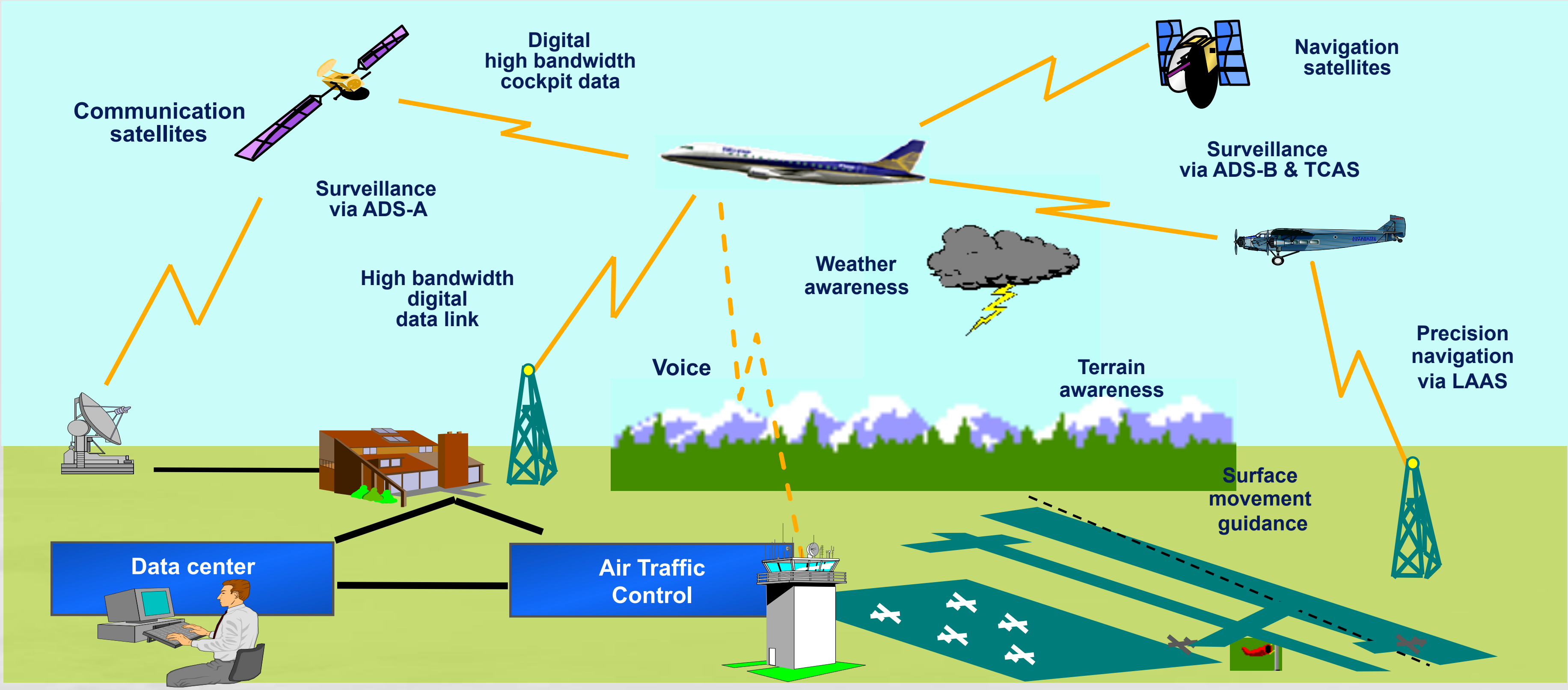
⬇ Proprietary Tech.

Non-IMA Networked Avionics Suite (Proprietary)

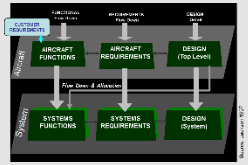
This chart is notional and does not refer to any industry milestones such as aircraft launch, certification or entry into service dates. It’s only intended to provide a big picture of the avionics evolution.

Context

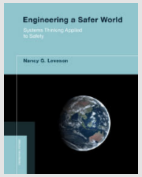
CNS-ATM


Communication satellites
Digital high bandwidth cockpit data
Navigation satellites
Surveillance via ADS-A
Surveillance via ADS-B & TCAS
High bandwidth digital data link
Weather awareness
Voice
Terrain awareness
Precision navigation via LAAS
Surface movement guidance
Data center
Air Traffic Control

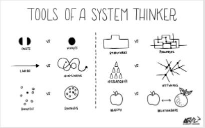
Knowledgment Foundation



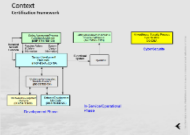
Systems Engineering



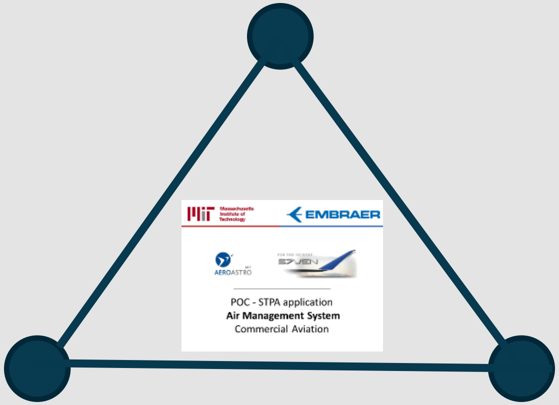
STAMP



Systems Thinking



Certification Framework



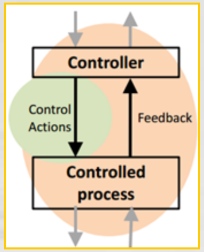
POC - STPA application
Air Management System
Commercial Aviation

Processes

People

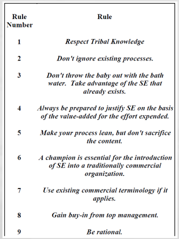
Critical Behaviors

Gentry Lee



Nancy Leveson

Rules

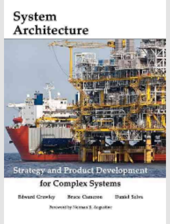


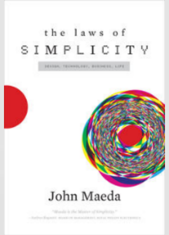
Rule Number	Rule
1	*Respect Tribal Knowledge*
2	*Don't ignore existing processes.*
3	*Don't throw the baby out with the bath water. Take advantage of the SE that already exists.*
4	*Always be prepared to justify SE on the basis of the value-added for the effort expended.*
5	*Make your process lean, but don't sacrifice the content.*
6	*A champion is essential for the introduction of SE into a traditionally commercial organization.*
7	*Use existing commercial terminology if it applies.*
8	*Gain buy-in from top management.*
9	*Be rational.*

Scott Jackson

Tools

STPA





Summary

- The STAMP/STPA shall be considered in the context of Systems Engineering and Systems Thinking for Architecting Complex and Highly Integrated Systems
- Its potential is increased if applied since the initial phases of the development (SE lifecycle)
- It requires a cultural change in the majority of the organizations
- It is important to influence the Certification Authorities to include the STAMP/STPA as a complementary and/or alternative means of compliance
    - CyberSecurity: Embraer submitted and White Paper incorporated in the ED-203A
    - ASTM: Embraer/MIT are submitting a Standard Guide for Part 23
    - S-18: Boeing/Embraer/MIT are developing and AIR (Aerospace Information Report)
- Identifying, selecting and training the appropriate persons in the organization to apply this methodology is a key point

EMBRAER

Thank you!

Viana
mtavares@embraer.com.br

Q.J.A

POC – AMS STPA Application

Massachusetts Institute of Technology
EMBRAER
MIT AEROASTRO
FOR THE JOURNEY
S7VEN

STPA application

Air Management System

Commercial Aviation

Systems Engineering Culture Change
Scott Jackson Rules

1. Respect Tribal knowledge.
2. Don’t ignore existing processes.
3. Don’t throw the baby out with the bath water. Take advantage of the SE that already exists.
4. Always be prepared to justify SE on the basis of the value-added for the effort expended.
5. Make your process lean, but don’t sacrifice the content.
6. A champion is essential for the introduction of SE into a traditionally commercial organization.
7. Use existing commercial terminology if it applies.

Jackson, Scott – Introducing Systems Engineering into a Traditionally Comercial Organization

Systems Engineering Culture Change

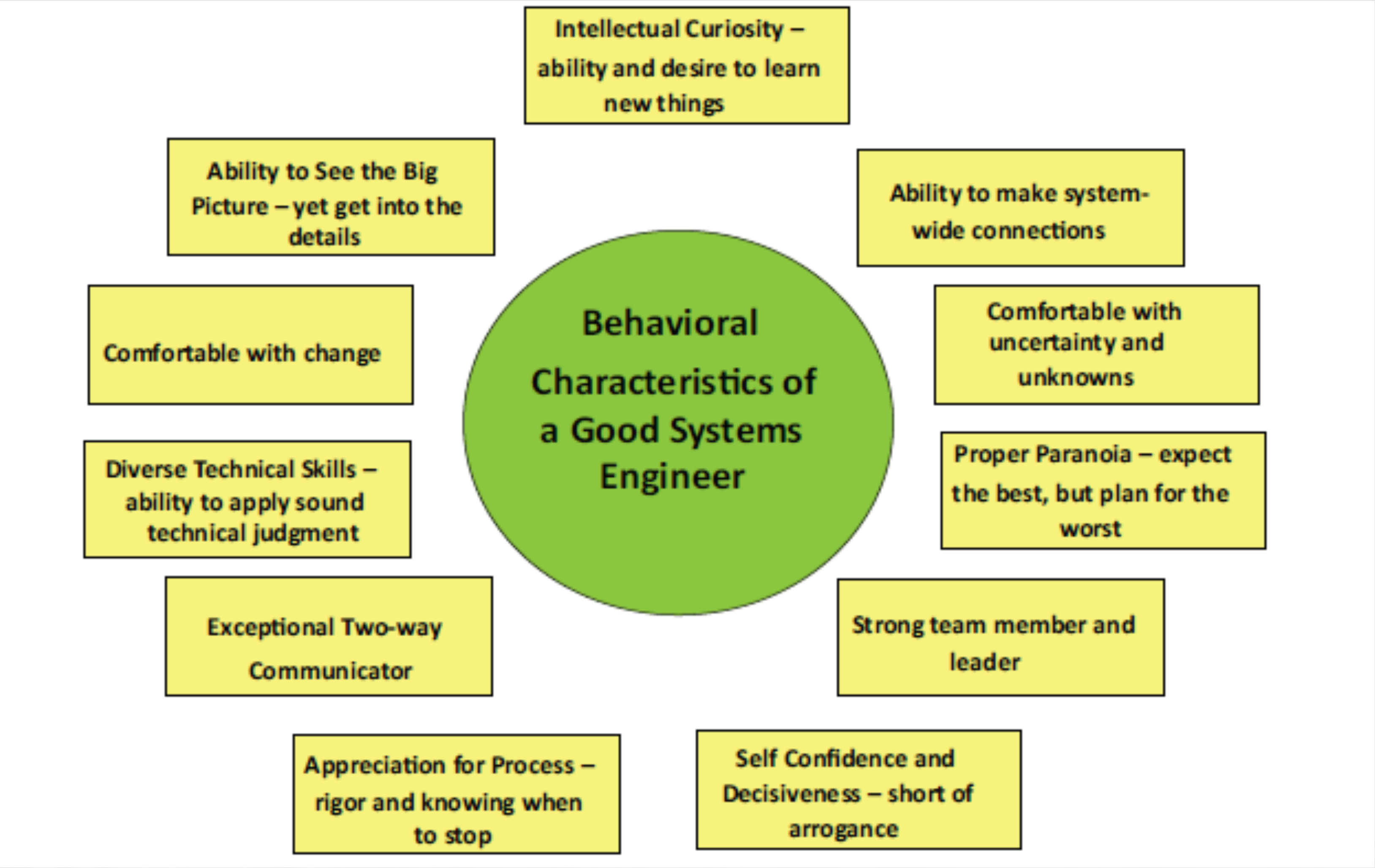
Scott Jackson Rules

8. Gain buy-in from top management.
9. Be rational.
10. Be satisfied with incremental progress.
11. Train, train, train.
12. Take advantage of IPD both for its own qualities and for the introduction of SE.
13. Stand firm.

Jackson, Scott – Introducing Systems Engineering into a Traditionally Comercial Organization

Systems Engineering Culture Change

Gentry Lee´s Critical Behaviors



Behavioral Characteristics of a Good Systems Engineer

Intellectual Curiosity – ability and desire to learn new things

Ability to make system-wide connections

Comfortable with uncertainty and unknowns

Proper Paranoia – expect the best, but plan for the worst

Strong team member and leader

Self Confidence and Decisiveness – short of arrogance

Appreciation for Process – rigor and knowing when to stop

Exceptional Two-way Communicator

Diverse Technical Skills – ability to apply sound technical judgment

Comfortable with change

Ability to See the Big Picture – yet get into the details

NASA – The Art and Science of Systems Engineering