PRODUCT DEVELOPMENT

STPA at Boeing
Driving Safety Requirements for Future Aircraft Design

Verdiana Ciriello, Systems Integration PD
Paul Lambertson, Modeling and Simulation lead PD

Agenda

- Why use STPA
- Team Effort
- Control Structure
- Requirements
  - Analysis
  - Sample
- Conclusion

Why use STPA?

Nasa 2004

Space Shuttle
500,000 lines of code

Boeing 2022

Boeing 787
6.7 million lines of code

Edmonds.com 2018

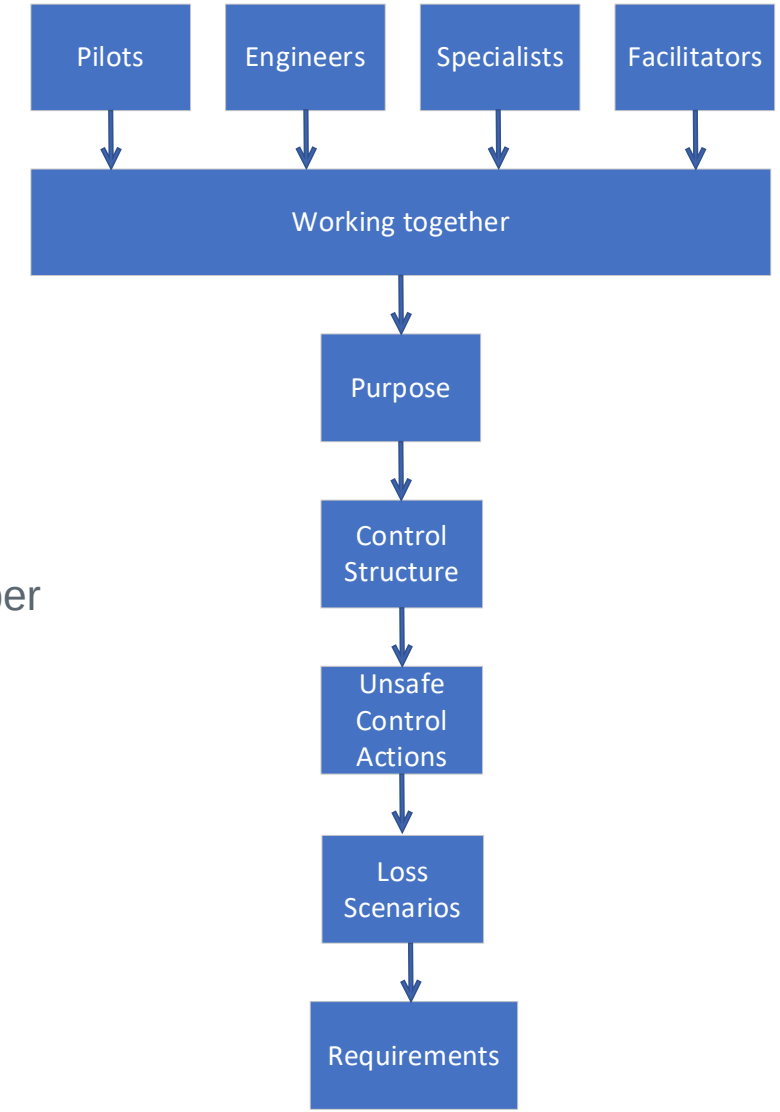
Ford Taurus
50 + million lines of code

Next new aircraft?

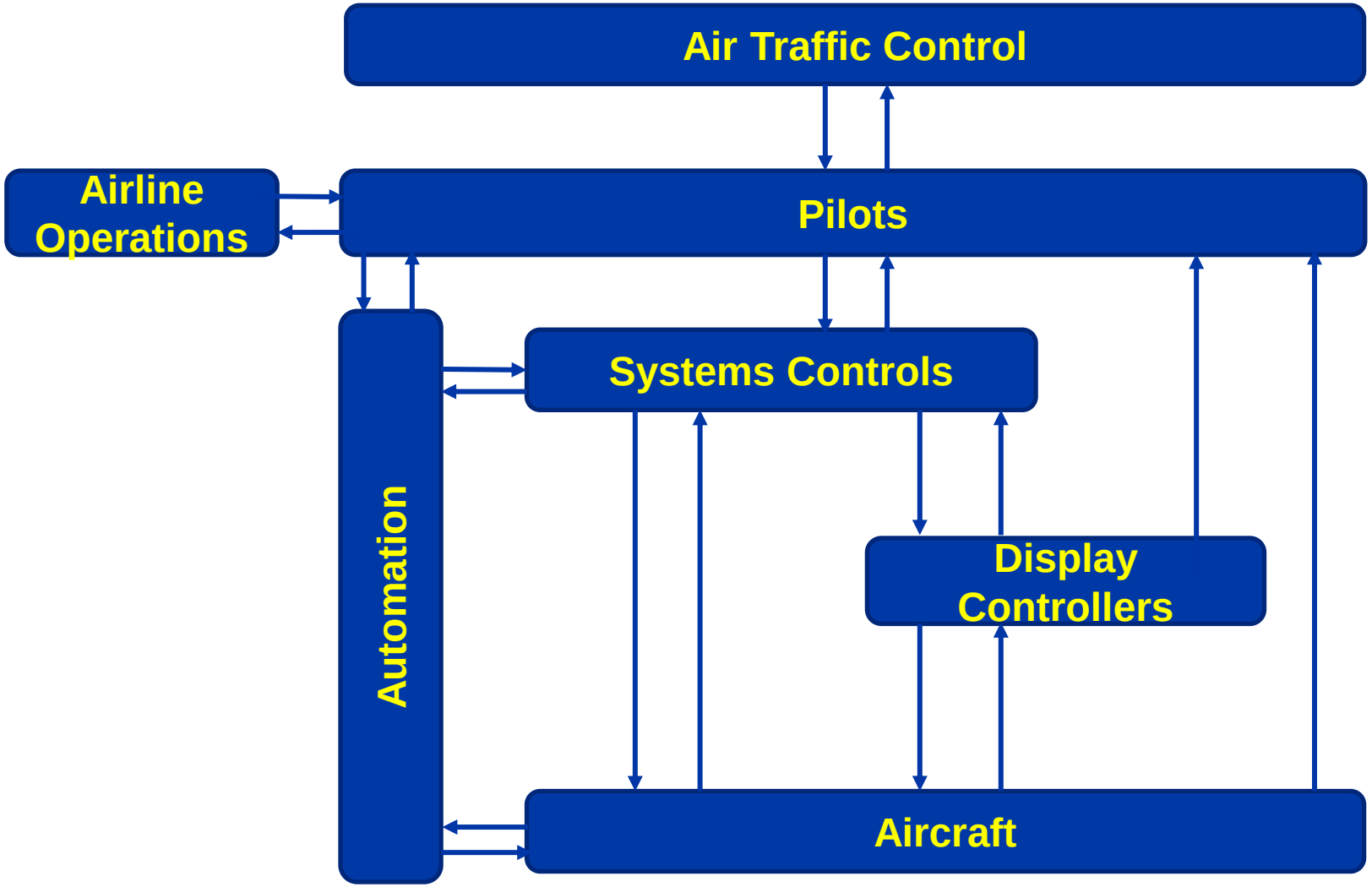
STPA Enables Engineers to Manage Complexity

Benefits of cross functional teaming for STPA

- Encourages inclusive teamwork
  - Including key stakeholders
  - Open communication
  - Joint purpose
- Enables productive reviews
  - The knowledge of the team is more than the knowledge of any one member
  - Higher ability to assess completeness
  - Communication to non-engineers, common language
  - Assistance for understanding despite complexity



Control Structure



Comparing two methods for development of requirements

Boeing 2022

Traditional

- Design objectives created
- Architecture is necessary (use cases, functional architecture etc.)
- Requirements driven from the architecture

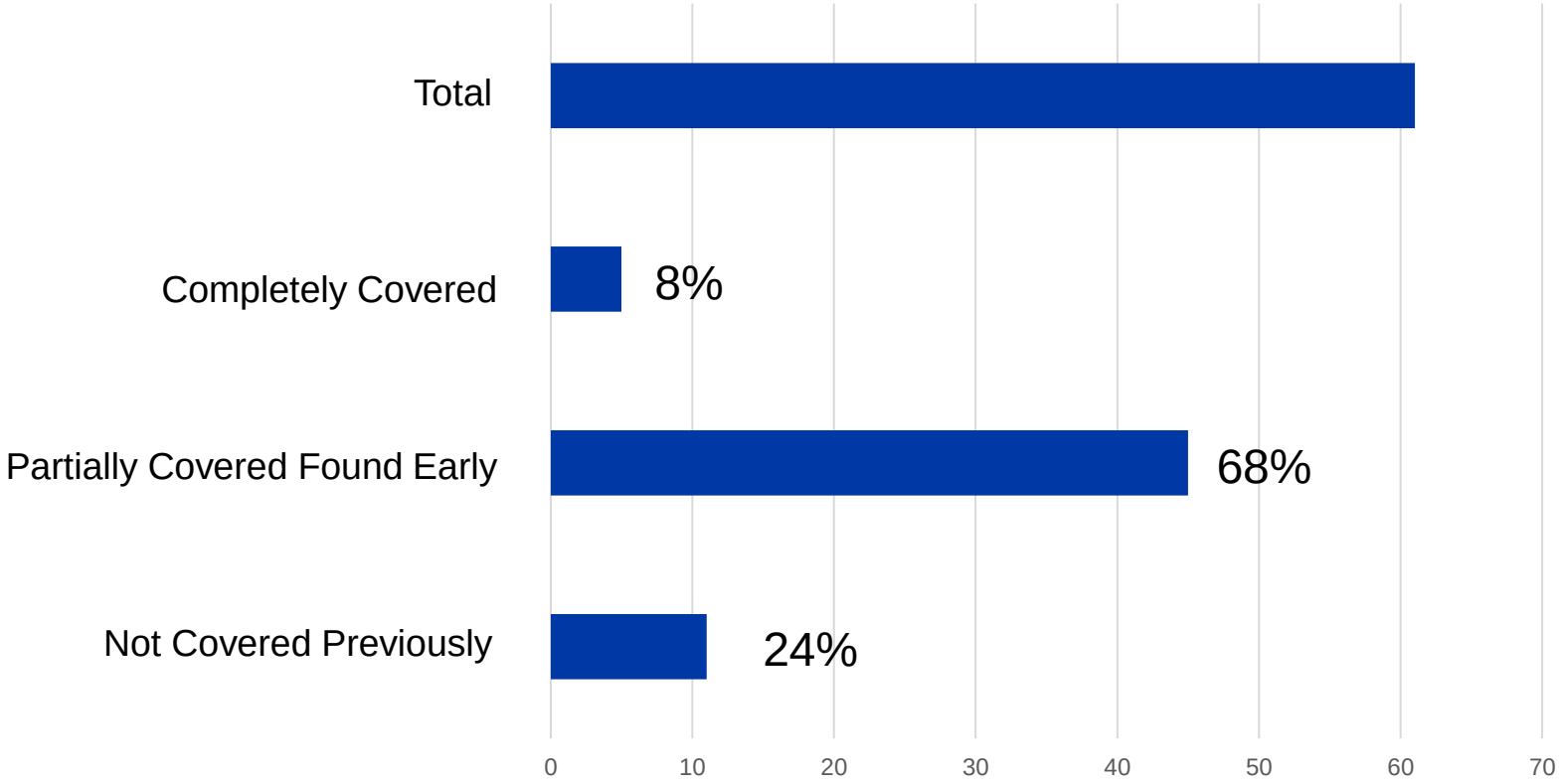
Requirements Improvement

STPA

- Design objectives created
- Control structure created
- Driving requirements from the control structure
- Can be used as the basis for development of a system architecture

Safety Requirements Driving the Architecture and Design

Requirements analysis



92% of STPA Requirements were improvements over Traditional Requirements

Example: Thrust during ground operations

STPA Requirement

The design of the system must ensure the pilots have an accurate mental/process model to make sure ground instructions are interpreted correctly, to prevent an engine blast that will damage other aircraft, structures as well as injure people, create foreign objects and debris, etc.

High level (system level) safety requirement

New Requirement

Traditional Requirement

No equivalent requirement was created

How would this fit into a more traditional Engineering requirement system:

Traditional Example:
The aircraft shall have a systems interface that prevents engine blasts from causing damage.

Rationale: The requirement is Intended to prevent an engine blast that will damage other aircraft and provide the pilots an interface that allow ground instructions to be interpreted correctly

Example: Thrust command for stall STPA analysis compared to traditional requirement

STPA Requirement:

The design of the system must ensure thrust is commanded when the A/C speed is less than the necessary speed to maintain lift, to eliminate the possibility of a stall condition that may damage the aircraft or injury people.

High level safety requirement

Enhanced Previous Traditional Requirement

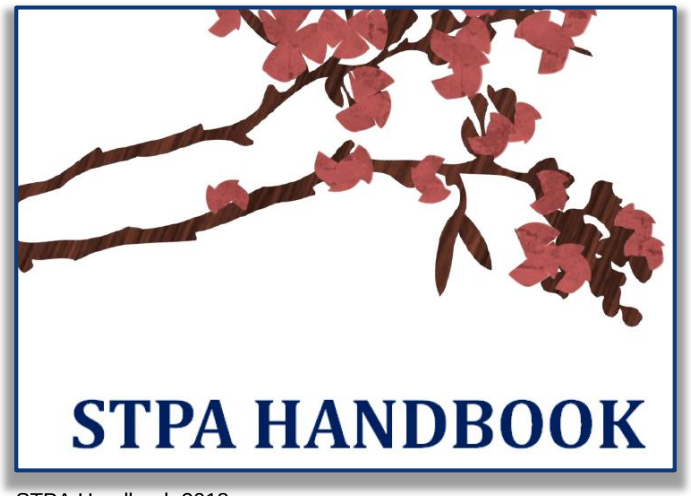
Traditional Requirements:

The aircraft shall be designed such that no single failure, regardless of probability, leads to loss of stall envelope protection or associated functions in combination with stall warning, during impending stall, preventing continued safe flight and landing.

How would STPA enhance the traditional requirement?

Conclusion

- STPA has the ability to identify potential safety issues before a design or architecture exists
- Complexity is increasing
- Teamwork is a necessity for completeness
- A representative control structure is vital for the completion of STPA



STPA Handbook 2018

Boeing BCA 2022