Consideration of STAMP-STPA in Civil Aviation

2021 STAMP Workshop

By: Linh Le & Eric M. Peterson

Date: June 28, 2021
Presentation Objectives

• Summarize safety process improvement recommendations

• Request commercial aviation industry’s experience in using STPA (or other tools/methods) in product development and system safety assessments
  – Voluntary
  – All information will be treated as confidential
  – All information will be ‘sanitized’ if used by FAA in future guidance materials
Safety Process Recommendations / Mandate Summary

• Multiple independent accident safety reviews, mandates, and recommendations
  – Common themes
    • System Safety Process
    • Human Factors – Safety Integration
    • Guidance Material
    • Certification Processes
    • FAA Oversight
Recommendations Summary

• System Safety Process
  – Develop, validate, and implement design and analysis models, methodologies, and approaches capable of identifying interactions among complex systems

• Human Factors – Safety Integration
  – Develop methods/tools - validating assumptions about pilot recognition and response to safety-significant failure conditions
    • Working together with industry
  – Promote consistent use of systematic analysis of Human Performance and Error Assessments to compliment System Safety Assessments
Noted Common Deficiencies from “Reviews”

• Inadequate analysis of failure scenarios which result in multiple flight deck effects
  – Cascading effects of a single failure

• Incomplete understanding of automated systems effects on human performance

• Functional Hazard Assessment
  – Identified assumptions of flight/ground crew actions not comprehensively validated in operational environments
    • Awareness of system behaviors
    • Pilot training
    • Pilot skills
    • Maintenance process
  – Potential incomplete functional hazard lists
Industry Outreach

• What are current industry best practices for evaluation of complex systems and human factors that can be used in conjunction with system safety process?

• Does industry have recommendations to close gaps identified by independent safety process reviews?
Industry Outreach

• What methods, processes, tools will address human-factor analysis gaps?

• Are there complementary human factor methods /tools /processes which may be integrated into the safety assessment continuum?

• What methods, processes, tools will enhance complex system analyses?
STPA Encouraging Constructs

• Complex systems can be analyzed
• Includes planned implementation and human operators in the analysis
• Easily integrated into system engineering / model-based system engineering development strategies
FAA Outreach

• Seeking innovations in system safety analysis techniques and testing methods for human / machine interface and integrated or automated (i.e. complex) systems
  – Evaluate new techniques (e.g. MIT’s System-Theoretic Process Analysis (STPA)) that can augment/improve current System Safety methods, particularly in the effort to understand the role of human performance / human errors
  – Identifying methods for defining mission-representative test conditions to uncover workload and integration issues when the aircraft operates with normal/full-up configurations and when in failed conditions
STPA Consideration by Industry

- Encourage wider application and evaluation of the STAMP-STPA methodology
  - Apply to new projects (TC, STC)
  - Expand applications in civil aviation
  - Provide FAA feedback on lessons learned
    - What works well, what doesn’t
    - Both good & bad lessons important

- Establish a basis for FAA consideration of the technique for certification
Conclusion

• Civil aviation needs an integrated human factor – safety assessment analytical methodology in addition to traditional pilot-in-the-loop evaluation / testing

• STPA may be an one approach to address the method / tool needs
  – Need experienced, empirical data to accomplish
Thank You for your attention

Contacts:
Linh.Le@faa.gov
Eric.M.Peterson@faa.gov