A STRUCTURED AND COMPREHENSIVE AIR VEHICLE RISK ASSESSMENT

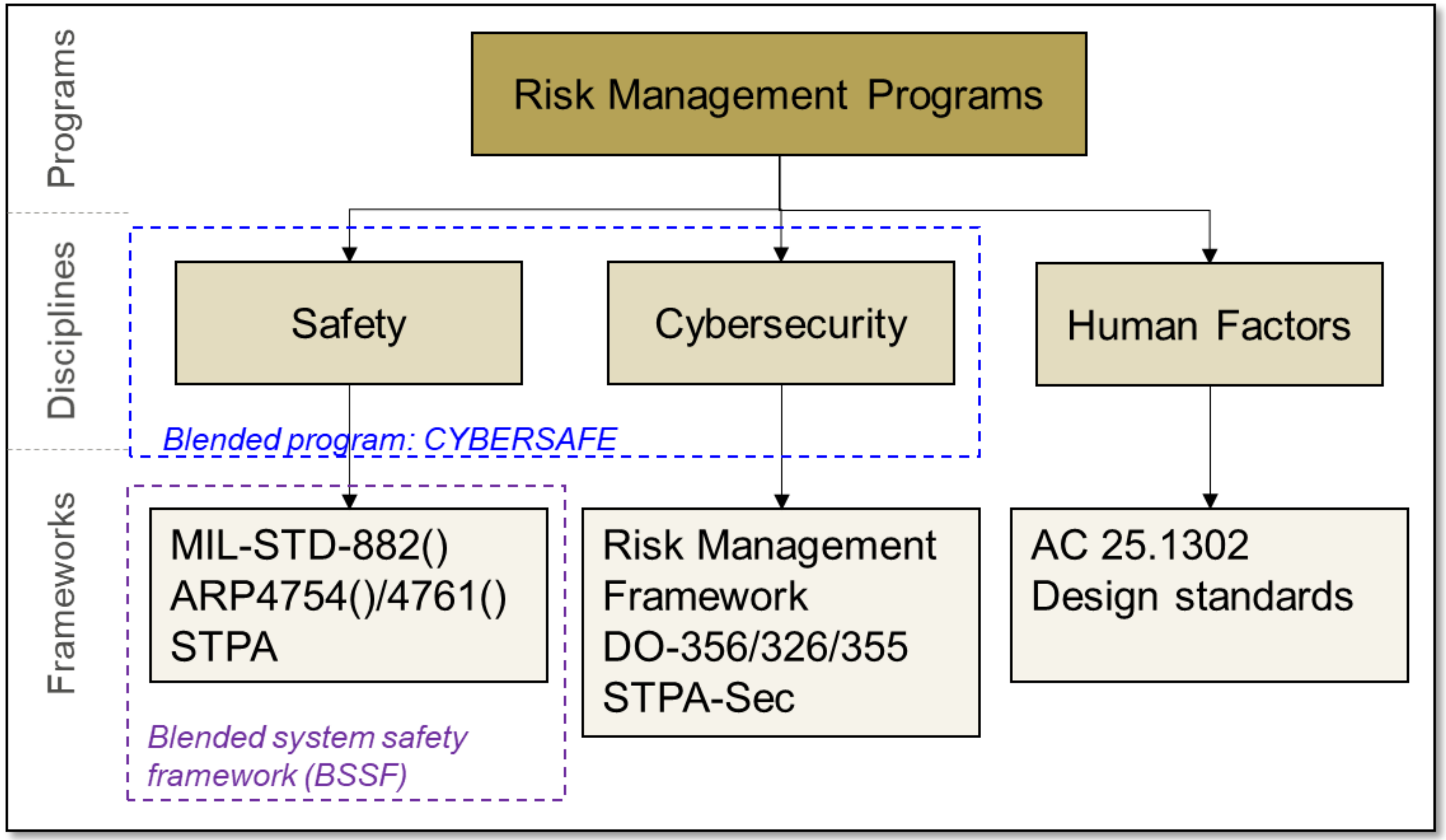
Dr. Laurence H. Mutuel

MIT STAMP WORKSHOP, 9 June 2022

Risk Management Frameworks

System Safety Program Objectives

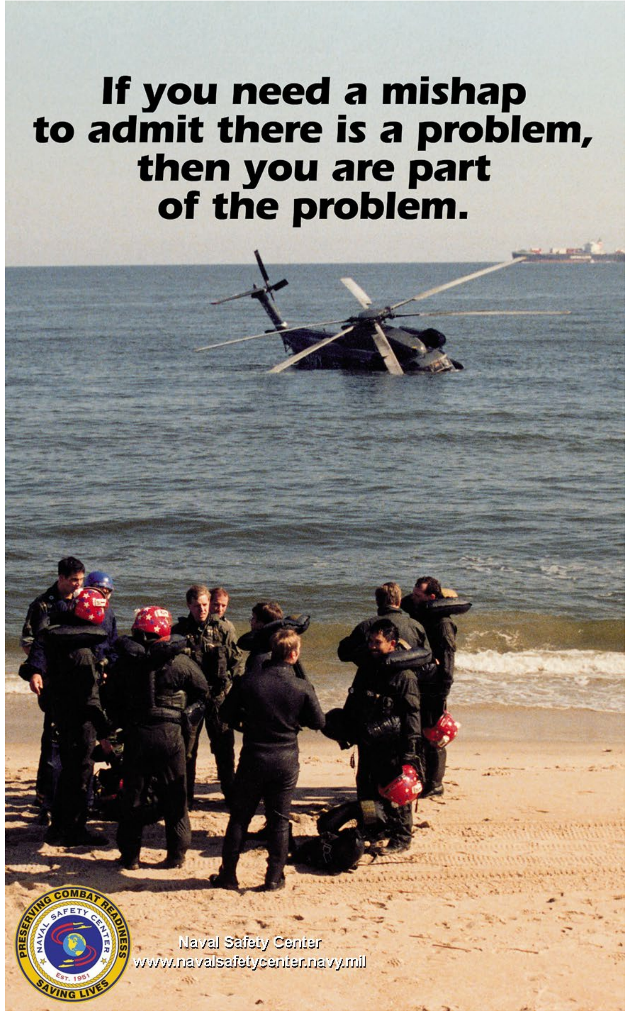
- During development, blend
  - MIL-STD-882E
  - SAE ARP4754A and ARP4761
  - System Theoretic Process Analysis (STPA)
- Plan for fielded system
  - MIL-STD-882E



Blended Framework for System Safety that Extends to Cybersecurity and Human Factors via STPA

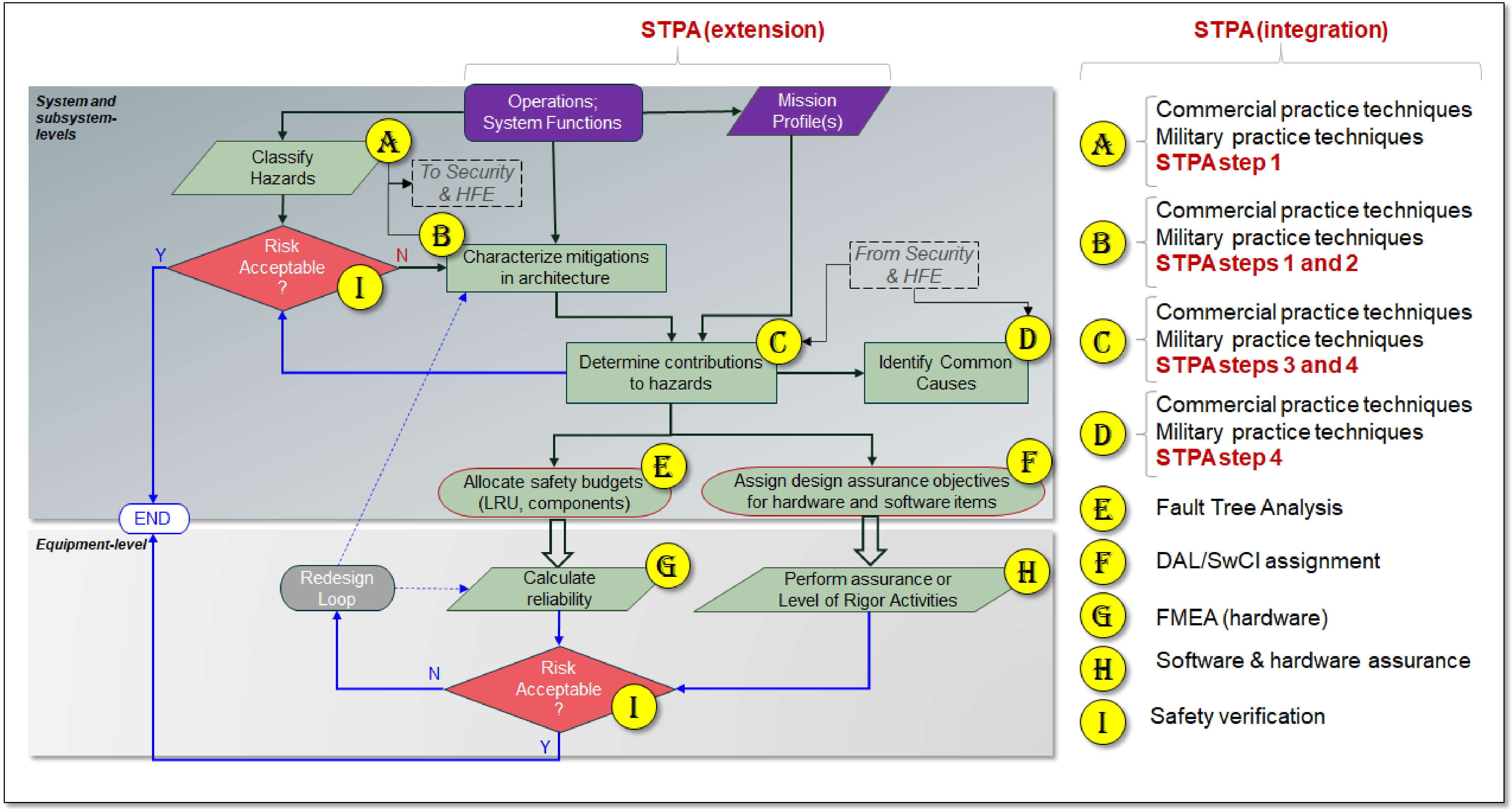
STPA Use in Key Safety Processes

- ❑ Hazard Identification
  - Aircraft level analyses primarily draw from Step 1
  - System level analyses primarily draw from Steps 2 and 3
- ❑ Risk Assessment
  - Steps 3 and Step 4 provide complementary content
- ❑ Risk Mitigation
  - Deriving requirements from Step 4
- ❑ Safety Verification
  - STPA supports developing Test Cases



All top-level Safety Processes Benefit from STPA Integration

STPA in Key System Safety Activities



STPA both Extends and Integrates with System Safety Activities

Lessons Learned from Concurrently Using Multiple Techniques

Each framework carries implicit context that could derail the approach if ignored:

- ✓ Capture assumptions that became implicit with more traditional practices
- ✓ Documenting assumptions is necessary to revisit analysis when design matures
- ✓ Splitting hairs may be needed, or results of analysis may be misleading

Safety techniques need be applied to the aircraft or system design in context:

- Historical: objective criteria were developed with a dated templated aircraft architecture
- Baseline: subjective criteria assumed baseline risk that may not always be transferable
- Development Assurance is tied to severity criteria derived from commercial practice

Consider this additional scope for meaningful blending:

- A portion of the risk may be carried at airspace level, tied to societal benefits
- Effects on the crew may be defined in context of cockpit configuration

Specific to use of STPA:

- STPA is most powerful where traditional practices are weakened by context (e.g., maturity, complexity of interactions), do review up front to apply STPA tactically

Safety Planning sets the stage for meaningful blending and robust safety statements

Conclusion

Blended System Safety Framework improves Safety performance by:

- Applying distinct techniques that support common risk management processes
- Understanding and using the techniques’ complementarity

Bell deployed the blended approach on FARA using a combination of theory and trial-and-error

- Starting at the aircraft level to capture relevant Doctrine and operational context
- Deep diving into armament to address human interactions, cyber-survivability and maturing concepts

Bell’s implementation of Blended Framework includes closed loop learning

- Capture of lessons learned after pilot program and after each major process step
- Traceability and measurement of safety process improvement