# Leveraging STPA to Create an Improved Risk Matrix

CPT(P) Sam Yoo
Instructor
Department Systems Engineering
West Point, NY

LCDR Dro Gregorian
Flight Instructor, US Navy
San Diego, CA


https://en.wikipedia.org/wiki/Leonardo_Next-Generation_Civil_Tiltrotor


https://www.japcc.org/wp-content/uploads/JAPCC_FBRC_screen.pdf

**STAMP Workshop**
June 2021



This research is based upon work supported by the US Army Combat Capabilities Development Command (CCDC) Aviation & Missile Center (AvMC) under Air Force Contract No. FA8702-15-D-0001. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of CCDC AvMC.

# Why do we care about improving the risk matrix?

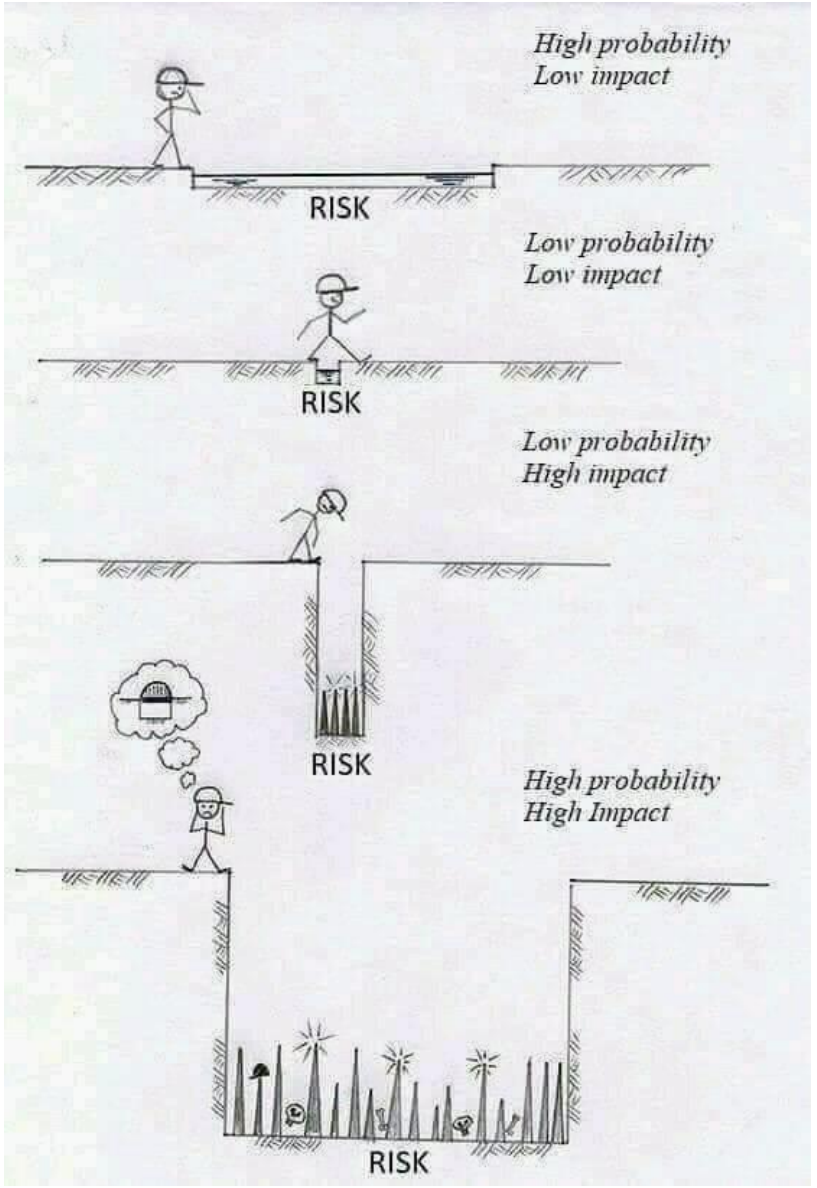
1. The risk matrix is a **widespread assessment tool**
2. **Overly rely upon probability** and reliability theory
3. **STPA** can greatly improve risk assessment
   - Identifies hazards not found by traditional methods
   - Replaces probability estimation with the concept of **mitigation effectiveness**
4. Use of STPA and mitigation effectiveness leads to a **new STPA-Informed Risk Matrix** (SRM)
5. Critical problems are **identified early** in the design

| RISK ASSESSMENT MATRIX | | | | |
|---|---|---|---|---|
| SEVERITY / PROBABILITY | Catastrophic (1) | Critical (2) | Marginal (3) | Negligible (4) |
| Frequent (A) | High | High | Serious | Medium |
| Probable (B) | High | High | Serious | Medium |
| Occasional (C) | High | Serious | Medium | Low |
| Remote (D) | Serious | Medium | Medium | Low |
| Improbable (E) | Medium | Medium | Medium | Low |
| Eliminated (F) | Eliminated | | | |

https://acqnotes.com/wp-content/uploads/2014/09/Risk-Assessment-Matrix.png

# What is Risk?

- "potential future event or condition that may have a negative effect on achieving program objectives for cost, schedule, and performance; defined by the **probability** of an undesired event or condition and the consequences, impact, or **severity** of the undesired event, were it to occur." (DoD Risk, Issue, Opportunity Management Guide)
- Often conveyed in "if-then" statements



# Strengths of the Risk Matrix Make them Highly Used in Industry

- **Simple to understand** and color coded intuitively
- Promote **robust discussion** on risk
- **Help decision-makers focus** on the highest areas of risk
- Show complex risk data in **one visual**

| RISK ASSESSMENT MATRIX | | | | |
|---|---|---|---|---|
| SEVERITY / PROBABILITY | Catastrophic (1) | Critical (2) | Marginal (3) | Negligible (4) |
| Frequent (A) | High | High | Serious | Medium |
| Probable (B) | High | High | Serious | Medium |
| Occasional (C) | High | Serious | Medium | Low |
| Remote (D) | Serious | Medium | Medium | Low |
| Improbable (E) | Medium | Medium | Medium | Low |
| Eliminated (F) | Eliminated | | | |

https://acqnotes.com/wp-content/uploads/2014/09/Risk-Assessment-Matrix.png

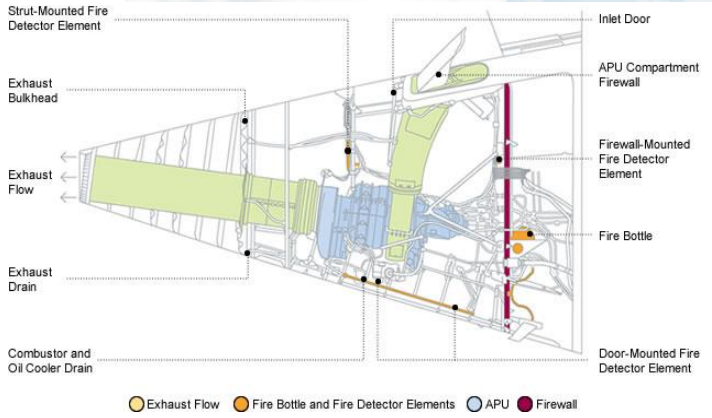
# Weaknesses of the Risk Matrix Leave Room for Improvement

- Lack of granularity, ordinal scales **oversimplify risk**
- General heuristic biases that inject **too much subjectivity**
- Inaccurate quantitative analysis with **poor likelihood assessments**

| RISK ASSESSMENT MATRIX | | | | |
|---|---|---|---|---|
| SEVERITY / PROBABILITY | Catastrophic (1) | Critical (2) | Marginal (3) | Negligible (4) |
| Frequent (A) | High | High | Serious | Medium |
| Probable (B) | High | High | Serious | Medium |
| Occasional (C) | High | Serious | Medium | Low |
| Remote (D) | Serious | Medium | Medium | Low |
| Improbable (E) | Medium | Medium | Medium | Low |
| Eliminated (F) | Eliminated | | | |

# Mitigation Effectiveness Replaces Probability and Drives New Risk Quantification

| Mitigation Level | Mitigation Description | Mitigation Effectiveness Score (MES) |
|---|---|---|
| Eliminated | The causal factor can be eliminated through design (proactive) | X |
| Reduction Through System Design | The occurrence of the causal factor can be reduced through system design (proactive) | 3 |
| Detected w/ Automated or Manual Response | The causal factor can be detected and requires a response to mitigate (reactive) | 2 |
| Training & Procedures | The causal factor can be mitigated through additional training and procedures (reactive) | 1 |
| None | No possible mitigation exists, or mitigation is never applied | 0 |





# STPA and Mitigation Effectiveness Create a new STPA-Informed Risk Matrix (SRM)

| Scenario-Based Approach | |
|---|---|
| **Step 1** | Complete STPA |
| **Step 2** | Assess the Pre-Mitigation Severity (PMS) of each casual scenario |
| **Step 3** | Generate mitigations to eliminate/control causal scenarios |
| **Step 4** | Complete scoring of Combined Mitigation Effectiveness Score (CMES) / Combined Post Mitigation Severity (CPMS) |
| **Step 5** | Plot each causal scenario onto the SRM |

| STPA-Informed Risk Matrix | | | | | |
|---|---|---|---|---|---|
| Least [A] | **0** | | | | |
| Somewhat [B] | **1** | | | | |
| Moderate [C] | **2-3** | | | | |
| Very [D] | **4-5** | | | | |
| Most [E] | **6** | | | | |
| Eliminated [F] | **N/A** | | | | |
| **CMES** | | **1** | **2** | **3** | **4** |
| | **CPMS** | Catastrophic | Critical | Marginal | Negligible |

*Definitions*:
***Risk:*** A combination of the severity of the hazard and the *mitigation effectiveness* in controlling the hazard
***Pre-Mitigation Severity***: Before any mitigations are applied, the worst-case severity of the risk
***Combined Mitigation Effectiveness Score (CMES)***: The combined impact of mitigation methods
***Combined Post Mitigation Severity (CPMS)***: The combined impact of all mitigations upon severity

# Future Rotary Wing Aircraft (FRWA) Are Highly Complex and Technologically Advanced

**Optionally Manned, Autonomous**

**Advanced Teaming with Unmanned Systems**

**Next Gen Propulsion**

**Ops in Degraded Visual Environment Systems**

https://i.ytimg.com/vi/yuSIvISH1aFA/maxresdefault.jpg

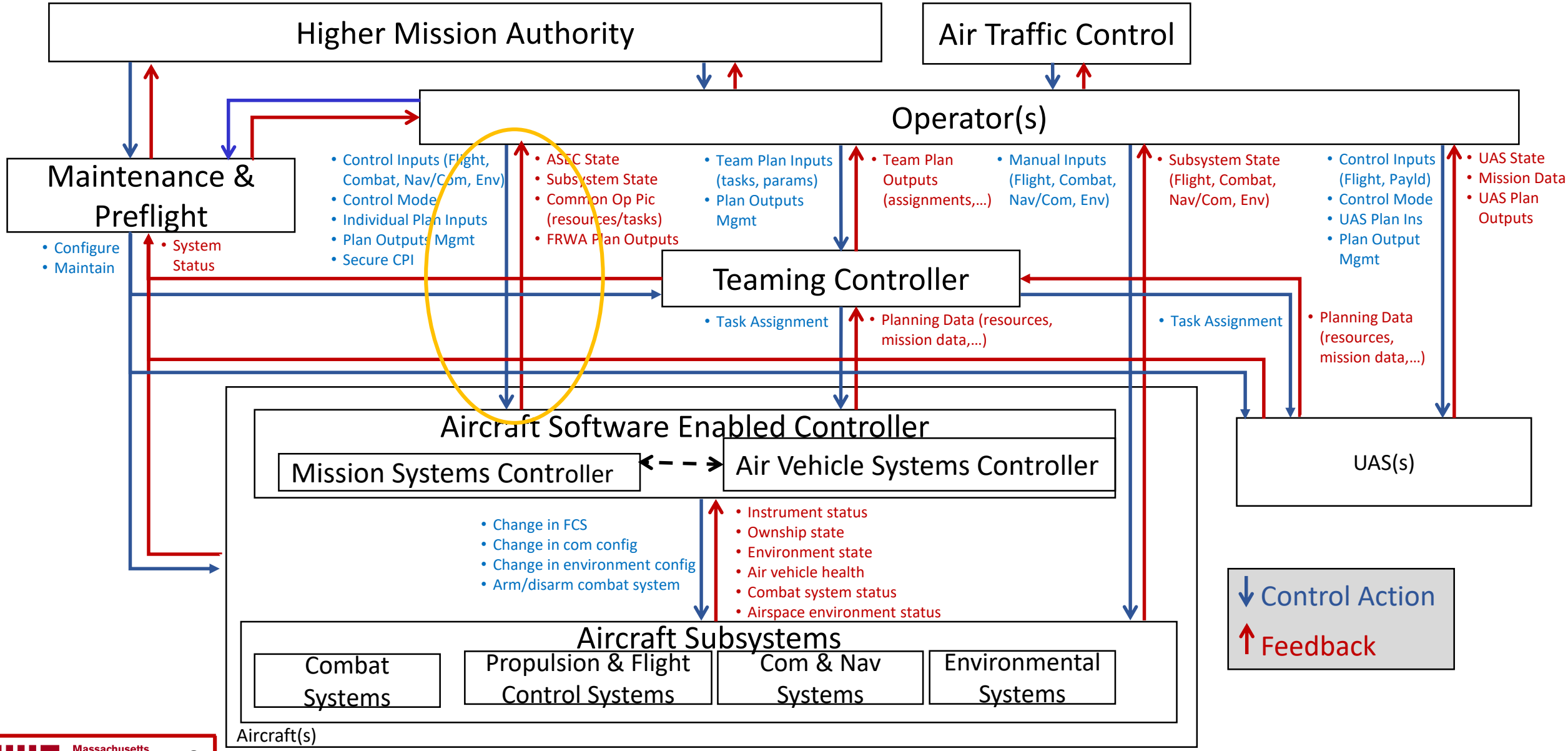
https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/photo/matrix/Sikorsky-MATRIX-2.jpg.pc-adaptive.480.high.jpg

https://www.armytimes.com/resizer/CqNLgROG0BigSMmO_mqfASB_xUM=/1200x0/filters:quality(100)/arc-anglerfish-arc2-prod-mco.s3.amazonaws.com/public/HRS2LZOVOJGZRL4XFCMKCUPORM.jpg


https://www.army.mil/article/191923/degraded_visual_environment_what_are_you_going_to_do_about_it

## How do we manage risk given this complexity?

# Safety Control Structure for FRWA



# Example of the Scenario-Based Approach

| Causal Scenario | | PMS | RM ID | Recommended Mitigation | Mitigation Level | MES | CMES | PPMS | CPMS |
|---|---|---|---|---|---|---|---|---|---|
| CS 2.0.1 | Operator is incapacitated by enemy fire, injury, illness and leans onto the controls accidentally activating them. As a result, aircraft can become uncontrollable. | 1 | RM01 | Aircraft monitors pilot health/posture/ attention and automatically engages autonomous mode when Operator is incapacitated/task saturated/inattentive/fixated; system can also alert and allow a remote operator to take control | Detection with Response | 2 | ELIM | 4 | 4 |
| | | | RM02 | Aircraft can be remotely controlled while in manned configuration | Reduction through System Design | 3 | | 4 | |
| | | | RM03 | Aircraft can autonomously execute specific flight maneuvers (e.g., return to base, climb/descend to specific altitudes, fly a specific straight-and-level profile, formation flight, reroute to designated airspace); maintains all structural limitations | Reduction through System Design | 3 | | 4 | |
| | | | RM04 | Operator engages in multiple training scenarios in a simulator environment where incapacitation could occur through multiple means and practices assisted aircraft recovery techniques through engagement of autonomous functionality or transfer of controls to remote pilot. | Training and Procedures | 1 | | 2 | |

# STPA-Informed Risk Matrix Is More Thorough and Objective Tool

| Operator-ASEC Risks | | | | | |
|---|---|---|---|---|---|
| Least [A] | **0** | | | | |
| Somewhat [B] | **1** | | 4.4.1 | | |
| Moderate [C] | **2-3** | | | 2.0.2, 2.0.5, 2.3.1, 2.4.2, 2.5.1, 4.0.2, 6.2.2, 6.3.1 | 2.1.1, 3.2.1, 4.0.3, 4.6.2, 5.3.1 |
| Very [D] | **4-5** | 4.1.2, 7.0.1 | 2.4.1, 4.2.1, 5.0.2 | 2.0.3, 2.0.4, 2.2.1, 2.7.3, 2.8.4, 3.0.1, 5.1.1, 7.1.1, 7.1.3 | 4.0.4, 4.6.1 |
| Most [E] | **6** | | | 2.6.1, 2.7.1, 2.7.2, 2.7.4, 2.8.1, 2.8.2, 2.8.3, 2.9.1, 2.9.2, 2.9.3, 4.3.1 | 2.5.2, 2.5.3 |
| Eliminated [F] | **N/A** | 2.0.1, 3.0.2, 3.1.1, 3.3.1, 3.4.1, 4.0.1, 4.1.1, 4.5.1, 5.0.1, 5.2.1, 5.4.1, 5.5.1, 5.6.1, 6.0.1, 6.1.1, 6.2.1, 6.5.1, 7.0.2, 7.1.2, 7.1.4, 7.1.5, 7.1.6 | | | |
| **CMES** | | **1** | **2** | **3** | **4** |
| | **CPMS** | Catastrophic | Critical | Marginal | Negligible |

- STPA allows for more **thorough risk identification**
- Approach enabled **more objective** analysis
- Provides risk planner with an **improved risk decision tool**



**ASEC**: Aircraft Software Enabled Controller

# Questions and Contact

- Please feel free to contact us with any questions or comments at **samyoo@mit.edu or drogreg@mit.edu**
- Read more details in our MIT thesis available for download free here:

https://tinyurl.com/STPA-Risk-Matrix

***A System-Theoretic Approach to Risk Analysis***

https://www.arlon.com/assets/icons/icon-contact-sales.png