SYSTEM-THEORETIC REQUIREMENTS DEFINITION FOR HUMAN INTERACTIONS ON FUTURE ROTARY-WING AIRCRAFT

Sam M. Yoo, Andrew N. Kopeikin, Dro J. Gregorian, Adam T. Munekata,
John P. Thomas, Nancy G. Leveson
Massachusetts Institute of Technology
Cambridge, MA

Future rotary-wing aircraft designs are highly complex, optionally manned, and include advanced teaming concepts that create unknown human-automation interaction safety risks. System-Theoretic Process Analysis (STPA) enables analysis of hazards on these complex systems. This paper demonstrates how to apply STPA in future helicopters' early concept development to prevent unacceptable losses. The system is modeled as a hierarchical control structure to capture interactions between components, including human and software controllers. Unsafe control actions are identified from these relationships and are used to systematically derive causal scenarios that arise from both hazardous interactions between system components and component failures. System requirements are then generated to mitigate these scenarios. A subset of the scenarios and requirements that address human factors related concerns are highlighted. Early identification of these problems helps designers (1) refine the concept of operations and control responsibilities and (2) effectively design safety into the system.

Future Rotary-Wing Aircraft (RWA) concepts are highly complex and include technologies such as autonomous flight, optionally manned capability, and cooperative teaming with other Unmanned Aircraft Systems (UAS). Some of the challenges related to developing concrete user requirements for future RWA are well documented in recent literature (Sushereba *et al.*, 2019). The technological complexity that supports future capabilities creates vulnerabilities for unsafe interactions between system controllers, especially in environments where operators perform under stress, high workloads, and face conflicting control authority over systems. A hazard analysis method is required to systematically identify these potential issues early in development so that mitigations can be designed into the system to enforce safety.

The SAE International Aerospace Recommended Practice (ARP) 4761 outlines methods for conducting safety assessments on civil airborne systems, such as the Functional Hazard Assessment (FHA) (SAE, 1996). However, a recent UH-60MU helicopter hazard analysis found that FHA limited its hazards to component failures and omitted humans from the study, except in instances where humans were assumed to mitigate the effects of some failures (Albrecht *et al.*, 2016). Additionally, specific hazards such as "loss of altitude indication in a degraded visual environment" or "loss of internal/external communications" were categorized as marginal in severity. In some cases, these hazards can be far more severe. For example, lost communications were cited as a significant contributor in the 1994 friendly shootdown of two US Army helicopters (Leveson, 2012). Other traditional hazard analysis techniques such as Fault Tree Analysis (FTA) or Failure Modes and Effects Analysis (FMEA) also emphasize failures

(Wasson, 2016). These methods are difficult to apply at the system level and are not recommended for complex human causality analysis (Cabosky, 2020).

The System-Theoretic Process Analysis (STPA) is a relatively new hazard analysis approach that is well suited to effectively handle complex systems like future RWA (Leveson and Thomas, 2018). Unlike traditional hazard analyses, STPA considers interactions between system entities, including software and human controllers. The top-down process begins at a high-level of abstraction and is then refined by iteratively adding design detail. This higher view enables STPA to provide early insights, even at the conceptual design stage, into potential causes of losses not typically discovered until much later in the engineering lifecycle. The results provide a critical opportunity to design safety features in early system development. This paper explains how STPA can be applied to future RWA to provide a top-down approach to hazard analysis. The subset of causal scenarios derived through the analysis highlights some of the human factors related challenges that need to be addressed in the program. The causal scenarios and requirements discussed in this paper represent a small portion of the completed STPA on future RWA.

STPA Applied to Future Rotary Wing Aircraft

STPA defines safety as a control problem rather than a component failure problem. The goal is to identify and design controls that enforce safety constraints uncovered through the analysis. The process systematically follows four steps described in the following subsections. The process can be used to rigorously derive design requirements that ensure the system behavior is safe and that the requirements are end-to-end traceable to the hazards they mitigate.

STPA Step 1: Define the Purpose of the Analysis

The STPA process begins by identifying the system losses unacceptable to the stakeholders (Leveson and Thomas, 2018). Safety is defined as the absence of such losses. In future RWA systems, unacceptable losses include (L-1) loss of life or permanent disabling injury, (L-2) loss or damage to aircraft or equipment, and (L-3) loss of mission. Next, the analysis identifies the system hazards. These are system states that will lead to a loss under a particular set of worst-case environmental conditions (Leveson and Thomas, 2018). Table 1 lists some of the hazards identified for the aircraft and traces each of them to the loss(es) they can lead to. High-level system safety constraints (SC) can be developed to address each of these hazards. For example, SC-1 can be derived as follows with traceability to H-1: *SC-1 the aircraft must remain controllable during all manned/unmanned operations [H-1]*. Many more traceable safety constraints with increasing details will be derived as the analysis unfolds.

STPA Step 2: Model the Control Structure

The next step of STPA is to model the hierarchal control structure. The model comprises feedback control loops and captures the relationships between various controllers and processes within the system (Leveson and Thomas, 2018). An effective control structure will enforce constraints on the behavior of the overall system. Each feedback control loop typically consists of five elements: *controllers* (in Figure 1, boxes at the top of each loop)*, control actions* (down

arrows), *feedback* (up arrows), *other inputs/outputs from components* (side arrows), *and controlled processes* (boxes at the bottom of each loop). Generally, the control structure starts at an abstract level and is iteratively refined to incorporate more system details. For example, the Operator(s) element might be refined into manned, remote, and autonomous configurations.

Table 1. Future rotary-wing aircraft system hazards.

Hazard ID	Hazard Description	Loss Link
H-1	Aircraft is uncontrollable (manned/unmanned)	L-1, L-2, L-3
H-2	Structural integrity of aircraft is violated	L-1, L-2, L-3
H-3	Minimum aircraft separation standards are violated	L-1, L-2, L-3
H-4	Aircraft environment is harmful to human health	L-1
H-5	Aircraft is unable to conduct mission tasks	L-1, L-2, L-3

STPA Step 3: Identify Unsafe Control Actions

The third step of STPA is to identify Unsafe Control Actions (UCAs). A UCA is a control action that will lead to a hazard in a particular context and worst-case environment (Leveson and Thomas, 2018). Each UCA consists of four parts: (1) the controller issuing the control action, (2) the **type** of control action, (3) the control action itself, and (4) the *context* under which it becomes hazardous (see Table 2). Each controller and control action in the control structure is considered. For each control action, there are four *types* of ways that each need to be considered on how a control action could cause a hazard: (1) not providing it, (2) providing it (incorrectly or in the wrong context), (3) providing it too early, too late, or out of order, and (4) providing for too long or short a time. Table 2 illustrates how a subset of the UCAs are developed for future RWA and how traceability is maintained to the hazards they cause.

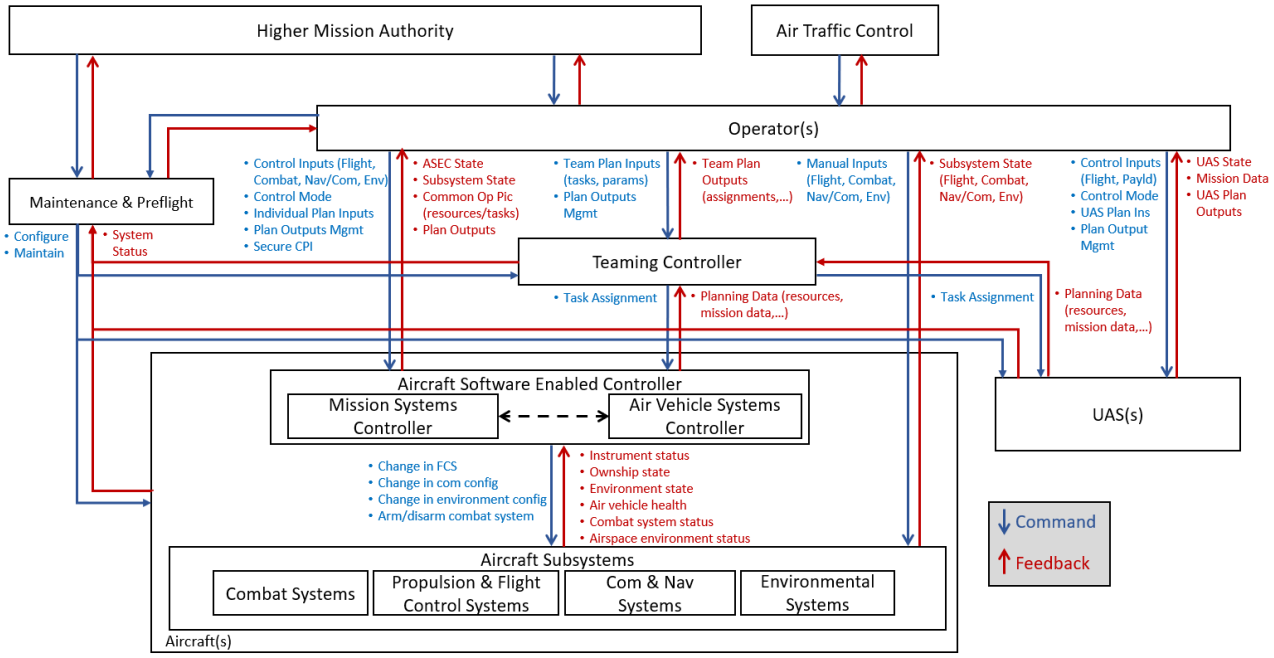

Figure 1. Safety Control Structure of the Future Rotary-Wing Aircraft System.

Table 2. Subset of UCAs for the "Flight Control Inputs" operator control action.

UCA Type	UCA	Hazard Traceability
Not Providing	[UCA-1] Operator **does not provide** flight control inputs *when needed during high power maneuvers (e.g., takeoff, formation, hover, ...)*	H-1, H-2, H-3, H-5
Providing	[UCA-2] Operator **provides** flight control inputs *when aircraft is in autonomous operation*	H-1, H-2, H-3, H-5
Too Early / Late / Wrong Order	[UCA 3] Operator provides flight control inputs **too early** *before the autonomous mode is disengaged*	H-1, H-2, H-3, H-5
Applied too long / Stopped too short	[UCA-4] Operator provides flight control inputs for **too long** *during high power maneuvers*	H-1, H-2, H-3, H-5

STPA Step 4: Identify Causal Scenarios

The final step in STPA is to identify causal scenarios for each UCA. Four potential flaws in the feedback control loop are systematically analyzed for each UCA by exploring reasons why (1) the controller would make an unsafe decision, (2) feedback would be inadequate, (3) the controlled process would not receive the command, or (4) the controlled process behavior would be unsafe despite receiving the command. Interactions between these elements of the feedback control loop and other control entities in the control structure are considered. The following are examples of each of these instances for UCA-1 in Table 2*: Operator does not provide flight control inputs when needed during high power maneuvers (e.g., takeoff, landing, hover, formation flight, ...).* Many more scenarios can be systematically created for this UCA using this method. Traceability is provided back to the UCA for each scenario.

Causal Scenario CS-1: The Operator has adequate feedback that a high-power maneuver is needed. However, confusion regarding the current operational mode of the Aircraft Software Enabled Controller (ASEC) leads the Operator to believe no inputs are necessary and that the ASEC will accomplish the behavior. This mode-confusion may result from maintenance personnel uploading new firmware into the vehicle that alters the modes or a remote operator performing teaming with the RWA and changes the mode remotely to manual flight. [UCA-1]

Causal Scenario CS-2: The Operator does not have adequate feedback that a high-power maneuver is needed. The aircraft is being operated in a degraded visual environment (DVE) enabled by an onboard sensor suite. However, the operator interface is devoted to a separate high workload mission operation, such as teaming with multiple UAS, and does not alert the Operator with sufficient time. [UCA-1]

Causal Scenario CS-3: The Operator does provide flight control inputs when needed for a high-power maneuver. However, the aircraft is being operated remotely, and insufficient communication bandwidth, potentially due to degraded channel capacity, is available to send the command. Or alternatively, the remote Operator inadvertently sends the command to a different aircraft. [UCA-1]

Causal Scenario CS-4: The ASEC does receive the flight control inputs from the Operator. However, the ASEC detects a different potential trajectory constraint, such as another aircraft, that could violate minimum separation standards. The ASEC overrules the Operator's control inputs, and the command is not issued to the aircraft's power and flight control system. Note that the other aircraft's detection may be caused by a malicious actor spoofing a transponder signal at a given location without a physical aircraft being there. [UCA-1]

Design Requirements

After scenarios have been identified, design requirements can then be generated to prevent those scenarios or UCAs from occurring or to mitigate their impact should they occur. For example, CS-1 may lead to the following design requirements. (R-1) The ASEC must inform the Operator about its control mode [CS-1]. (R-2) The ASEC must inform the Operator of any changes in control mode, actions taken by the ASEC as a result of that change, and the reason for the change [CS-1]. (R-3) The ASEC must be programmed with software consistent with operator tactics techniques and procedures [CS-1]. (R-4) Remote operators must not override onboard operators when they are actively controlling or supervising the aircraft.

The process described in the previous section provides end-to-end traceability between design requirements, scenarios, and back up to the unacceptable losses that should be prevented. The traceability provides an opportunity to document the rationale for each design requirement. The high-level abstraction of the presented analysis leads to the systematic development of high-level requirements in the early development stages. The early insight provides a new and unique opportunity to highlight the design trade-offs. As assessed through the analysis, features with significant risk may be candidates for removal from the architecture. The process can then be iterated by adding refinement in the design's details so that additional requirements can be uncovered. In addition to iterating with STPA, R-1 and R-2 might benefit from a more specific application of related human factors research in presenting critical information to operators at the right time using the Alerting and Reasoning Management System (ALARMS) framework (Saffell *et al.*, 2011). Additional details to R-3 and R-4 would benefit from the lessons learned through DARPA's Aircrew Labor In-Cockpit Automation System (ALIAS) program, as it works with Sikorsky to explore communication protocols between autonomously operated helicopters.

Conclusions

Future RWA will be increasingly complex and will challenge the traditional delineation between software and human controllers' responsibilities. This complexity creates new hazards that need to be identified and addressed early in design. Traditional hazard analysis methods are not capable of addressing complex systems with human interactions such as future RWA. However, STPA is well suited for this problem and is applied in this paper to demonstrate systematic identification of a subset of potential causal loss scenarios that emphasize human factors design elements. System requirements are then derived from the causal loss scenarios to design controls into the system to mitigate those scenarios and enforce safety. The process can be repeated for all control actions identified in the control structure to derive a rich set of safety requirements at this level of abstraction. As design decisions are made throughout the

engineering lifecycle, additional detail can be incorporated into the model as refinement. The analysis can then be continued at that level to generate lower-level system requirements.

Acknowledgments

DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited. This research is based upon work supported by the U.S. Army Combat Capabilities Development Command Aviation & Missile Center (DEVCOM 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 DEVCOM AvMC.

References

Abrecht, B., Arterburn, D., Horney, D., Schneider, J., Abel, B., & Leveson, N. (2016). *A new approach to hazard analysis for rotorcraft.* Cambridge, MA: Massachusetts Institute of Technology. Retrieved from: sunnyday.mit.edu/papers/AHS-final.pdf

Cabosky, R. (2020). *A human factors study on vehicle automation*. Cambridge, MA: Massachusetts Institute of Technology.

Leveson, N. (2012). *Engineering a Safer World: Systems Thinking Applied to Safety*. The MIT Press. Retrieved from: mitpress.mit.edu/books/engineering-safer-world

Leveson, N., Thomas J. P. (2018). *STPA Handbook*. Retrieved from: psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Reim, G. (2021). Sikorsky plans to autonomously fly multiple UH-60 Black Hawks in formation in 2021. Flight Global. Retrieved from: www.flightglobal.com/helicopters/sikorsky-plans-to-autonomously-fly-multiple-uh-60-black-hawks-in-formation-in-2021/141128.article

Saffell, T., Alexander, A., Carlin, A., Chang, A., & Schurr, N. (2011). An integrated alerting and notification system utilizing stages of automation and uncertainty visualization. In *16th International Symposium on Aviation Psychology*, 197-202. Retrieved from: corescholar.libraries.wright.edu/isap_2011/82

Society of Automotive Engineers. (1996). ARP 4761 - Guidelines and Methods for Conducting the Safety Assessment Process on a Civil Airborne Systems and Equipment. Retrieved from: www.sae.org/standards/content/arp4761/

Sushereba, C., Militello, L., Ernst, K., Diiulio, J., Roth, E., Scheff, S., Huff IV, W. (2019). Envisioning user requirements for first-of-a-kind future rotorcraft. In *20th International Symposium on Aviation Psychology,* 403-408. Retrieved from: corescholar.libraries.wright.edu/isap_2019/68

Wasson, C. (2016). *System Engineering – Analysis, Design, and Development*. 2nd ed. Wiley