5-1-2021

Hazard Analysis for Human Supervisory Control of Multiple Unmanned Aircraft Systems

Elias B. Johnson

Andrew N. Kopeikin

Nancy G. Leveson

Andrew W. Drysdale

Repository Citation

Johnson, E. B., Kopeikin, A. N., Leveson, N. G., & Drysdale, A. W. (2021). Hazard Analysis for Human Supervisory Control of Multiple Unmanned Aircraft Systems. *56th International Symposium on Aviation Psychology*, 274-279.
https://corescholar.libraries.wright.edu/isap_2021/46

HAZARD ANALYSIS FOR HUMAN SUPERVISORY CONTROL OF MULTIPLE UNMANNED AIRCRAFT SYSTEMS

Elias B. Johnson, Andrew N. Kopeikin, Nancy G. Leveson
Massachusetts Institute of Technology
Cambridge, MA

Andrew W. Drysdale
U.S. Army Combat Capabilities and Development Command - Data and Analysis Center
Aberdeen Proving Ground, MD

Unmanned Aircraft Systems (UAS) operations are shifting from multiple operators controlling a single-UAS to a single operator supervising multiple-UAS engaged in complex mission sets. To enable this, there is wide consensus in literature that limitations in human cognitive capacity require shifting low-level control responsibilities to automation so that human operators can focus on supervisory control. However, hazard analyses to identify related safety concerns have largely been unexplored. To address this shortfall, this paper applies System-Theoretic Process Analysis (STPA) on an abstracted model of a multi-UAS system. This hazard analysis approach handles complex systems and human-machine control interactions together. The paper describes both how to execute the analysis, and provides examples related to an operator approving or denying plans developed by the automation. Numerous traceable causal scenarios are systematically identified and generate both design recommendations and questions that must be addressed to ensure the system is designed to be safe.

Control of Unmanned Aircraft Systems (UAS) is undergoing a paradigm shift from multiple operators remotely *controlling* a single-UAS to a single operator *supervising* multiple-UAS (Belecastro et al., 2017). In this context, the difference between operator *control* and *supervision* is characterized by a shift in delineation of control responsibilities between the operator and the UAS automation. Operators that control UAS are responsible for providing lower-level control inputs directly to UAS flight, navigation, and payload sub-systems to achieve the flight and mission objectives. In contrast, when operators perform supervision of UAS, the responsibility for lower-level control is delegated to the UAS automation (Porat et al., 2016). The operator becomes responsible for providing higher level control actions to the UAS decision making automation entity. In examples of supervisory control in several multi-UAS implementations, the operator will input mission planning parameters into the autonomy so that it can develop courses of actions and present them to the operator for review (Porat et al., 2016).

The allocation of more control responsibilities to automated controllers has the potential to increase the mission reach without increasing human operator resource requirements. For example, early studies showed that a single operator could only control 4-5 vehicles (Cummings, 2007a), but they could supervise around 12 UAS at a time (Cummings and Guerlain, 2007). However, increase use of automation also introduces new human factors concerns which have been raised extensively in the literature (Belecastro et al., 2017). For example, the skills and training required for operators to perform supervisory control may be considerably different than those previously required in lower-

DISTRIBUTION STATEMENT A. Approved for public release. Distribution is unlimited.

level control. Furthermore, in certain conditions, the UAS operator may have to override the automation and revert to lower-level control, potentially leading to cognitive overload if the system is not designed to account for these situations (Leveson, 2012).

To ensure operators and automation can work together to safely control multi-UAS requires a rigorous safety guided design process. A large body of work points to numerous studies related to the design of control algorithm (Saif et al., 2019) or the human factors implications of various design and interface choices (Levulis et al., 2018). However, the two domains are often considered separately in initial design, rather than taking a holistic approach that integrates them from the onset. This leads to potential hazards that may emerge later in the lifecycle of the system.

Few hazard analyses have been performed on these systems, and the ones performed (Belecastro et al., 2017) assumed linear causality which limits the results and opportunity to address safety through design recommendations. In addition, much of the human factors research is centered on simulation, which while important, should not be the only tool used in early system development. Simulation only reveals what is being specifically tested, and relies on assumptions that limit their scope, such as: set configurations, limited adverse factors, simplified dynamics, and reliable automation (Levulis et al., 2018). In reality, these systems will face unforeseen scenarios that will challenge the brittle autonomy in ways not detected in simulation.

To begin to address this shortfall, this paper applies a System-Theoretic approach centered on human-machine control interactions for such systems (Leveson, 2012). It demonstrates examples from a larger analysis of how human factors and control system design can be integrated in early concept development, modelling, and analysis. This ensures the multi-UAS system designers consider strengths and limitations of the operator at the onset design. The example explores hazardous supervisory control actions associated with approving or denying plans developed by the automation. The results of this abstracted modelling approach (1) provide design recommendations that enable safety features to be designed early into the system when most effective, (2) are applicable to a wide range of multi-UAS systems. The approach allows more design details to be refined using STPA for iterative safety guided design.

System Modelling and Hazard Analysis Process

The System-Theoretic Process Analysis (STPA) is a top-down hazard analysis approach which treats safety as a control problem rather than just considering component failures. As a result, the method is effective at handling complex systems with unsafe interactions between components, software, and human controllers. Complexity is managed through abstraction, and the analysis is initiated at a high level, as illustrated below, and can then be iteratively refined by adding design details. The following subsections demonstrate the process.

Purpose of the Analysis and Description of the System

The first step is to define the purpose the analysis, and the assumptions about the system and the environment. For this paper, the purpose is to analyze safety hazards for an abstracted model of a multi-UAS system with supervisory control to provide early design recommendations. In the system under consideration, an operator provides high-level planning guidance, the UAS automation develops courses of action (COAs) to control multiple UAS, and an operator is responsible for approving or denying them. No restrictive assumptions are made about the environment of the UAS or the operator.

STPA begins by identifying the system losses unacceptable to the stakeholders (Leveson and Thomas, 2018). For this multi-UAS system, these may include (L-1) loss of mission, (L-2) loss of life or permanent disabling injury, and (L-3) loss or damage to UAS or equipment. Next, system level hazards are identified. A hazard is “a system state or set of conditions that, together with a particular set of worst-case environmental conditions, will lead to a loss” (Leveson and Thomas, 2018). Table 1 presents a sub-set of the hazards considered in this analysis, and traceability to the losses.

Table 1.
Example Multi-UAS System hazards.

Hazard ID	Hazard Description	Loss Traceability
H-1	UAS does not complete mission objectives and tasks	L-1, L-2
H-2	Structural integrity of UAS is violated	L-3
H-3	Violation of UAS separation standards (min & max)	L-1, L-2, L-3

Hierarchical Control Structure

The second step in STPA is to build a hierarchical control structure of the system. This is a conceptual functional model composed of feedback control loops that shows responsibilities, control actions, feedback and mental models of each element within the system boundary. The control structure enables a hazard analysis on the interactions between elements.

The abstracted control structure for the multi-UAS system with control responsibilities split between the pilot and UAS automation is shown in Figure 1. The operator provides high-level guidance on the mission objectives and constraints. The Multi-UAS Fleet Controller generates a COA plan based on its process models of the environment, mission objectives and physical UAS systems. The operator can then “Approve” or “Deny” the COA as guided by their mental models of the environment, mission objectives, and feedback provided by the Fleet Controller.

Unsafe Control Actions

The third step of STPA is to identify unsafe control actions (UCAs), which are control actions that, in a particular context, and worse-case environment, will lead to a hazardous state (Leveson and Thomas, 2018). There are four possible ways to consider how each control action in the control structure can lead to a hazard: (1) not providing the control action, (2) providing the control action, (3) providing a safe control action but too early, too late, or in the wrong order, and (4) providing a control action that last too long or is stopped too soon. Table 2 provides examples of some of the UCAs that are identified for the “Approve COA” control action from the operator. Additional UCAs may exist in each UCA Type, and additional UCAs are similarly identified for the other control actions in the control structure.

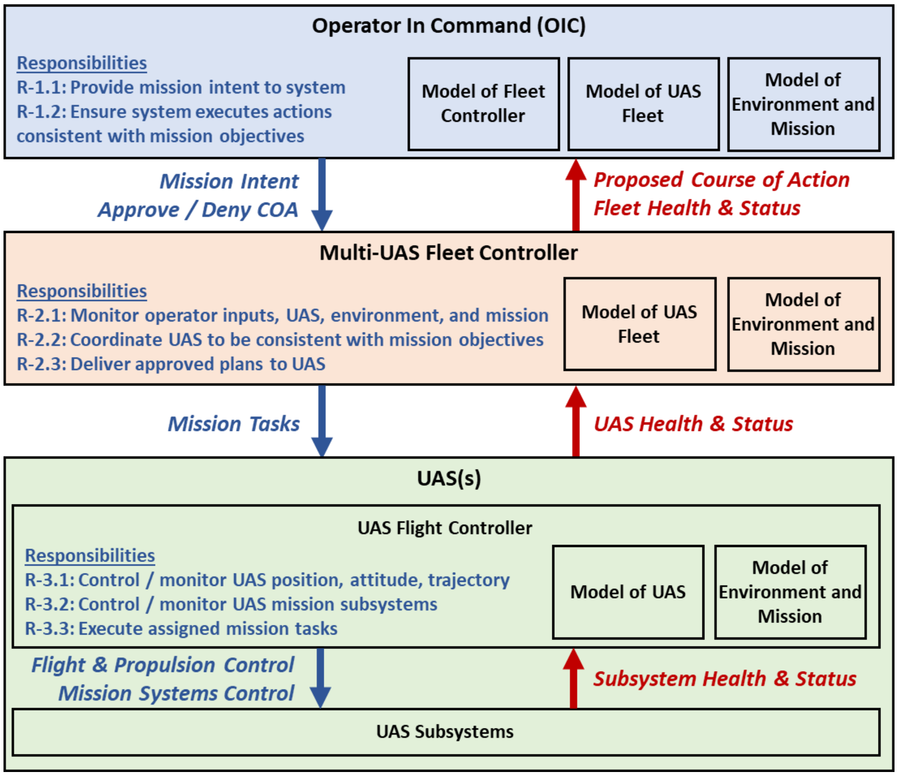
Operator In Command (OIC)
Responsibilities
R-1.1: Provide mission intent to system
R-1.2: Ensure system executes actions consistent with mission objectives
Model of Fleet Controller
Model of UAS Fleet
Model of Environment and Mission
Mission Intent
Approve / Deny COA
Proposed Course of Action
Fleet Health & Status
Multi-UAS Fleet Controller
Responsibilities
R-2.1: Monitor operator inputs, UAS, environment, and mission
R-2.2: Coordinate UAS to be consistent with mission objectives
R-2.3: Deliver approved plans to UAS
Model of UAS Fleet
Model of Environment and Mission
Mission Tasks
UAS Health & Status
UAS(s)
UAS Flight Controller
Responsibilities
R-3.1: Control / monitor UAS position, attitude, trajectory
R-3.2: Control / monitor UAS mission subsystems
R-3.3: Execute assigned mission tasks
Model of UAS
Model of Environment and Mission
Flight & Propulsion Control
Mission Systems Control
Subsystem Health & Status
UAS Subsystems

Figure 1. Safety hierarchical control structure of an abstracted multi-UAS system.

Table 2.
Example Unsafe Control Actions (UCA) for the "Approve COA" operator control action.

UCA Type	UCA	Hazard Traceability
Not Providing	[UCA-1] Operator *does not provide* "Approve COA" when the COA fulfills the flight or mission objectives	H-1, H-2, H-3
Providing	[UCA-2] Pilot *provides* "Approve COA" when the COA does not fulfill the flight or mission objectives	H-1, H-2, H-3
Too Early / Late / Wrong Order	[UCA 3] Pilot provides "Approve COA" *too late* when the COA will no longer fulfill the flight or mission objectives	H-1, H-2, H-3
Applied too long / Stopped too short	*Not applicable for this analysis because "Approve COA" is a discrete command*	

Causal Scenarios

The fourth step of STPA is to identify loss scenarios that describe the casual factors that can lead to the unsafe control actions and to the hazardous state. Scenarios help discover early design recommendations and questions that must be addressed to enforce safety constraints and refine the design. Causal scenarios consider potential breakdowns in feedback control loops as a result of unsafe interactions between elements of the control structure and component failures.

Of the 130 causal scenarios (CS) identified in the multi-UAS system analysis, three examples are highlighted that are traceable to Table 2 UCA-3: *The operator provides "Approve COA" too late and the COA which originally satisfied flight objectives will no longer fulfill the flight or mission objectives* [H-1, H-2, H-3]. Scenarios can potentially also trace to other UCAs.

CS-1: The Operator does not know that a proposed COA request is time critical. The COA was not originally time sensitive when the request was sent from the UAS Fleet Controller to the Operator, but became time sensitive because of dynamics in the mission or environment. The system is not designed to alert the operator when this occurs. [UCA-3]

CS-2: The Fleet Controller updates the COA request so frequently that the operator cannot assess its validity before it is replanned. Thus, the operator is in a perpetual cycle of reviewing proposed COAs. [UCA-3]

CS-3: In the time between operator approval and UAS execution, the COA becomes no longer consistent with mission objectives. Reasons for this include the following: (CS-3.1) The system design allows the operator to approve commands preemptively or with long time horizon; (CS-3.2) There is a delay in the UAS receiving execution commands because of environmental interference of system degradations; (CS-3.3) The Operator cannot modify the COAs once they are approved; (CS-3.4) The Fleet Controller generates an infeasible plan; (CS-3.5) The system is not designed to detect changes that may invalidate an already approved plan. [UCA-3]

Safety Guided Design Recommendations and Questions

Next begins an iterative cycle of safety guided design where the results of the hazard analysis are used to develop both design recommendations and questions to be addressed in refinement of the system. Recommendations are traceable directly to causal scenarios to provide critical context. The questions raise valuable insights to consider in the design. The full analysis revealed 65 design recommendations and 64 questions. The following are examples of Design Recommendations (DR) and their resulting questions (DR-Q) that illustrate how human factors considerations related to multi-UAS supervisory control were generated through analysis of the Causal Scenarios listed in the previous section. STPA is an iterative process. After design recommendations are implemented, changes must be reexamined using STPA to ensure they do not introduce sources of hazards themselves.

DR-1: There must be a feedback mechanism to alert the pilot when a non-time sensitive tasks becomes time sensitive [UCA 3, CS-1]. (DR-Q-1.1) How should the operator be alerted when a task becomes time critical? (DR-Q-1.2) How should the feedback for non-time critical tasks differ from time critical tasks?

DR-2: The system must not enter a state where the operator cannot provide input because the UAS perpetually updates the COA [UCA 3, CS-2]. (DR-Q-1.1) If there is [TBD] time gap in between approval and execution, which controller(s) is responsible for ensuring the command is still appropriate? (DR-Q-1.2) Which controller(s) is responsible for monitoring which tasks have been completed? (DR-Q-1.3) When is it appropriate for an operator to approve a COA in advance? (DR-Q-1.4) When is it not appropriate?

Conclusions and Recommendations

Multi-UAS supervisory control is a shift in the delineation of responsibilities between human operators and the automation. To date, few hazard analyses have been conducted on these systems to allocate responsibilities for safe operations. This paper demonstrated how to apply the STPA hazard analysis and safety guided design method on an abstracted model of a multi-UAS system. STPA specifically considers interactions within complex systems, in which components may or may not have failed, and that are controlled by both humans and software controllers. The analysis provides both design recommendations and questions, that if addressed, can help ensure safety is built into the system from the early design phases.

Acknowledgments

This research is based upon work supported by the U.S. Army Combat Capabilities Development Command (CCDC) Data and Analysis Center (DAC) under Contract W911NF-19-2-0124. Any opinions, findings, conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of CCDC DAC.

References

Belcastro, C. M., Newman, R. L., Evans, J., Klyde, D. H., Barr, L. C., & Ancel, E. (2017, June 5). Hazards identification and analysis for unmanned aircraft system operations. 17th AIAA Aviation Technology, Integration, and Operations Conference, Denver, Colorado.

Cummings, M. L., Bruni, S., Mercier, S., and Mitchell, P. J. (2007a). Automation architecture for single operator, multiple UAV command and control. Int. C2 J. 1, 1–24.

Cummings, M. L., & Guerlain, S. (2007). Developing operator capacity estimates for supervisory control of autonomous vehicles. Human Factors: The Journal of the Human Factors and Ergonomics Society, 49(1), 1–15.

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

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

Levulis, S. J., DeLucia, P. R., & Kim, S. Y. (2018). Effects of touch, voice, and multimodal input, and task load on multiple-uav monitoring performance during simulated manned-unmanned teaming in a military helicopter. Human Factors: The Journal of the Human Factors and Ergonomics Society, 60(8), 1117–1129.

Porat, T., Oron-Gilad, T., Rottem-Hovev, M., & Silbiger, J. (2016). Supervising and controlling unmanned systems: A multi-phase study with subject matter experts. *Frontiers in Psychology*, *7*. https://doi.org/10.3389/fpsyg.2016.00568

Saif, O., Fantoni, I., & Zavala-Río, A. (2019). Distributed integral control of multiple UAVs: Precise flocking and navigation. IET Control Theory & Applications, 13(13), 2008–2017.