HAZARD, SAFETY RISK AND UNCERTAINTY MODELING OF THE INTEGRATION OF UNMANNED AIRCRAFT SYSTEMS INTO THE NATIONAL AIRSPACE

Ahmet Oztekin, James T. Luxhøj
Rutgers University

Keywords: *safety and security, aircraft design, systems and systems integration*

Abstract

As the National Airspace System (NAS) in the United States becomes increasingly more complex and constrained, the associated hazard and safety risk modeling must also mature in sophistication. This paper discusses the need for new methods of hazard, risk and uncertainty modeling for a new generation of air vehicles and supporting systems, such as unmanned aircraft systems.

1 Introduction

As the complexity of the National Airspace System in the United States increases, hazard and safety risk analysis have fundamental roles to play in the identification of hazard source potentials, the understanding of the underlying causal factors, the likelihood assessment of these factors, the severity evaluation of the potential consequence(s) of mishaps, and the prioritization of mitigations. A significant challenge in modern aviation system safety practice is the analytical modeling of emergent operations in the NAS that include the use of a new generation of air vehicles and supporting systems, such as very light jets, reusable launch vehicles, unmanned aircraft systems, among others [1-3]. Since these air vehicle operations are new, accident and incident data are extremely rare, and alternative modeling approaches to conventional fault tree logic are required to understand the impact of the introduction of these operations into the NAS.

A research team at Rutgers University followed a multi-step process that included systems-level hazard identification and categorization, hazard prioritization and reviews of technology and analytical methods supportive of hazard and risk analysis for unmanned aircraft systems. The first version of a systems-level hazard taxonomy included the system hazard sources of Airmen, Operations and NAS Interconnectivity, Unmanned Aircraft Systems, and Environment and was reported in [4]. In addition, through a system decomposition process, hazard sub-system sources were identified. Through the use of 208 hypothesized and some real UAS mishap scenarios, it was demonstrated how the proposed hazard taxonomy could lead to an implicit prioritization of the hazard system and sub-system sources [4].

In this paper, a revised version of the systems-level taxonomy is presented. In addition, a framework for identifying and classifying hazard causal factors in proposed and a sample application of that framework is illustrated. Finally, a brief section is included that provides an overview of a new hybrid method for combining both discrete and continuous random variables in an integrated risk analysis. Finally, possible UAS research directions are presented.

2 Hazard Taxonomy

The systems-level hazard taxonomy developed for unmanned aircraft in this research is termed the Hazard Classification and Analysis System (HCAS). Brief descriptions of both the original and revised versions are provided below.

2.1 HCAS – original version

The original version of the HCAS was presented in [4-5] and is shown in Fig. 1. The

idea is to provide a structured framework to identify and classify or categorize both system and sub-system hazard sources for UAS operations. Before proceeding with describing the methodology used in UAS hazard categorization, it is important to establish some basic terminology. For purposes of the Rutgers research, the following definition of a hazard is used:

Hazard: A hazard is a state or set of conditions of a system that, together with other conditions in the environment of the system, may lead to an unsafe event (Source: adapted from [6]).

The first version of HCAS identified the four system-level hazard sources of Airmen, Operations and NAS Interconnectivity, Unmanned Aircraft Systems, and Environment. It was constructed from an analysis of 208 hypothesized UAS scenarios as well as some real UAS mishaps. Details are provided in [5]. Once the hazards for a given scenario set are categorized, an implicit prioritization of the hazards may be obtained by recomputing frequency counts as percentages as shown in Fig. 2 [4-5]. Such an approach provides a possible structured means to systematically weight the hazards.

2.2 HCAS – revised version

A review and critique of the original HCAS version by industry subject matter experts indicated a need to have the taxonomy become more aligned with FAA regulations, and in particular the Title 14, Code of Federal Regulations (14 CFR) chapters on Aircraft, Airmen, Certification/Airworthiness, Flight

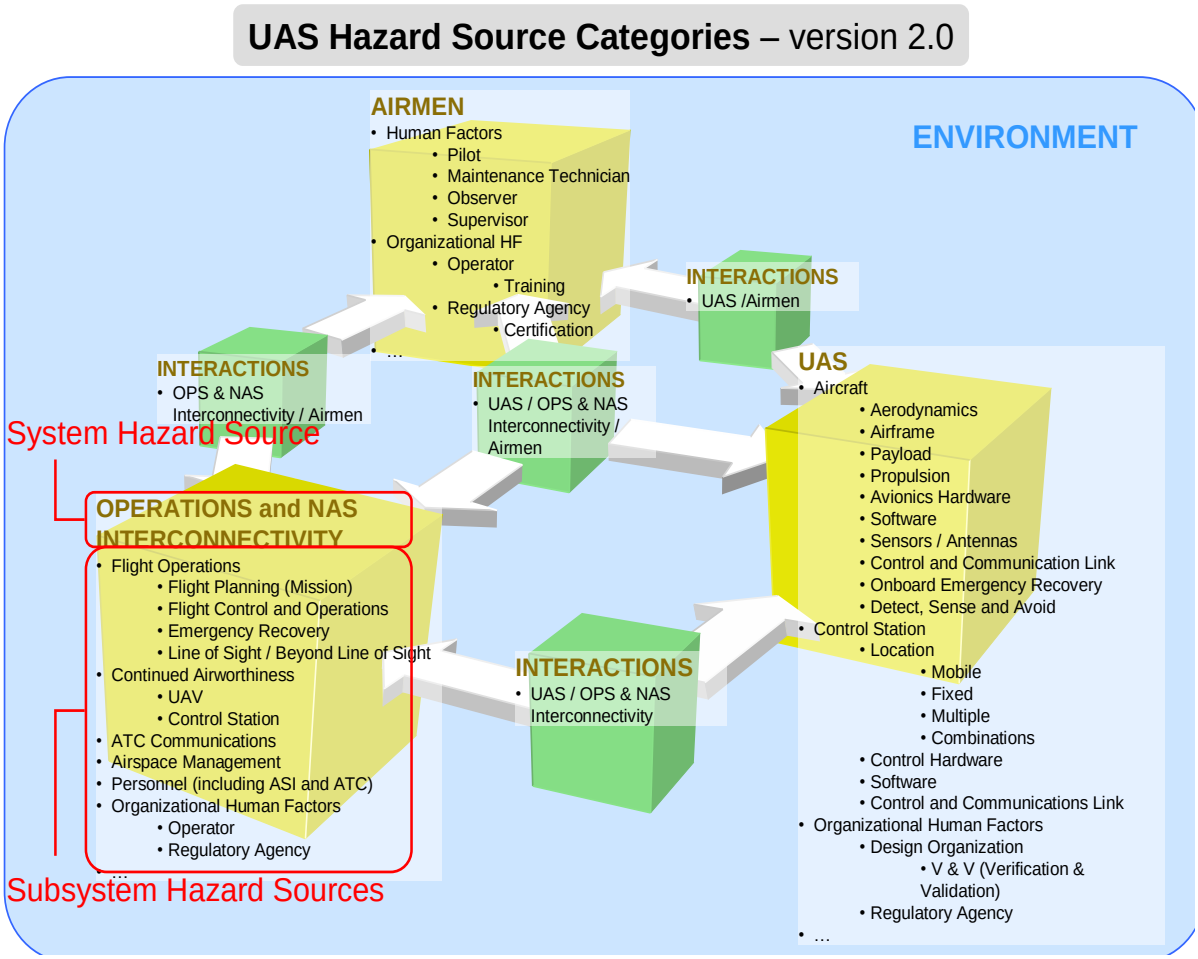

Fig. 1. HCAS taxonomy – original version

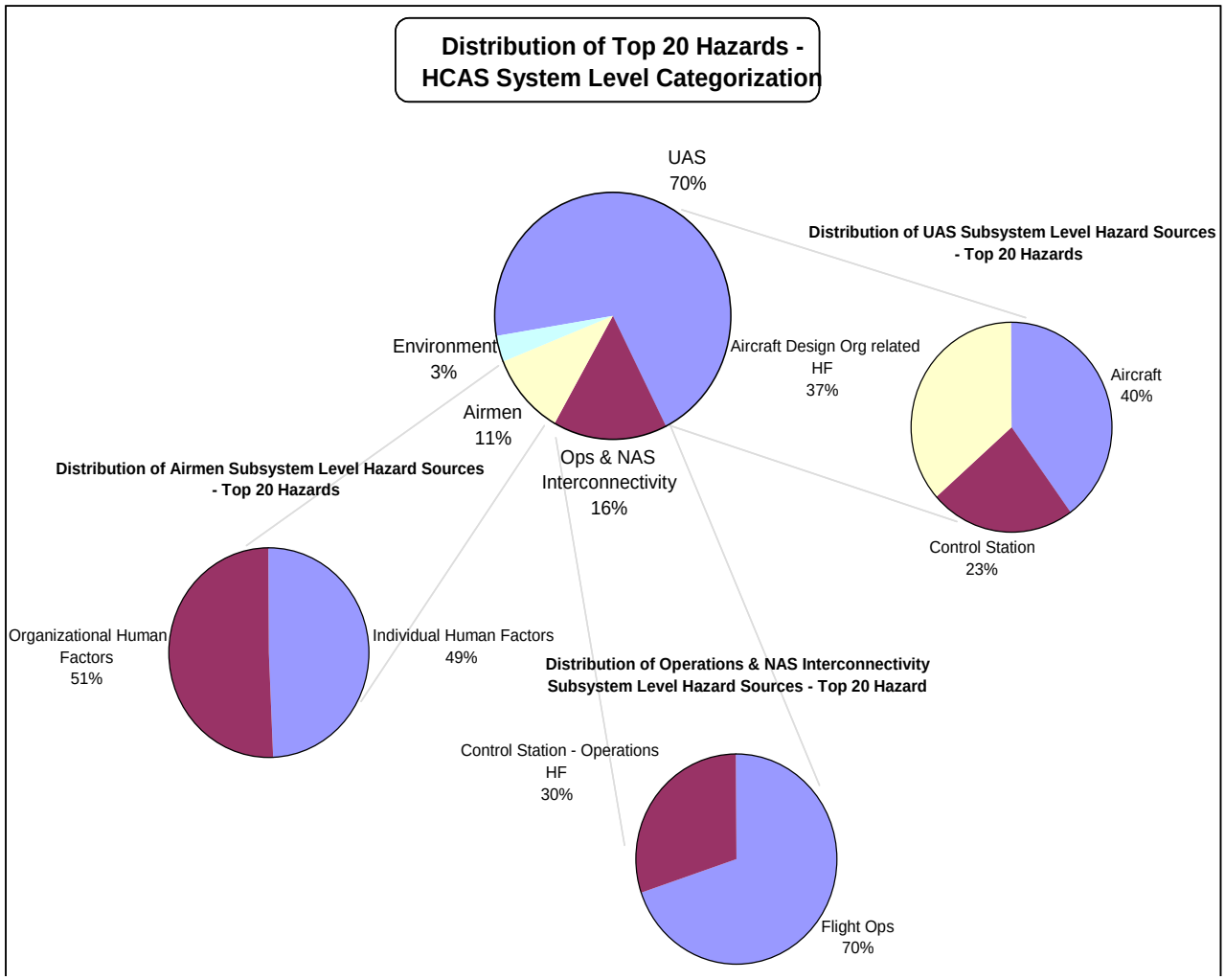

Fig. 2. Distribution of Hazards for given HCAS Scenario Set

Operations, etc.) as well as FAA guidance [7]. Such an approach uniquely distinguishes the HCAS taxonomy from all other UAS hazard analyses being performed by the Department of Defense (DoD), the RTCA-Special Committee (SC) 203, etc. The Rutgers Phase 1 research goal was to develop a generalized taxonomy of system-level UAS hazards that would have broad applicability across FAA part types.

The revised version of the HCAS taxonomy is shown in Fig. 3. Some of the significant changes include embedding the Control Station system source under the original Aircraft system source renamed as UAS. A fourth cube termed as Environment was added to the revised version and numerous sub-system hazard sources added. A detailed review of the HCAS taxonomy by industry subject matter experts improved the taxonomy by moving it to be more closely aligned with the existing FAA 14 CFR chapters.

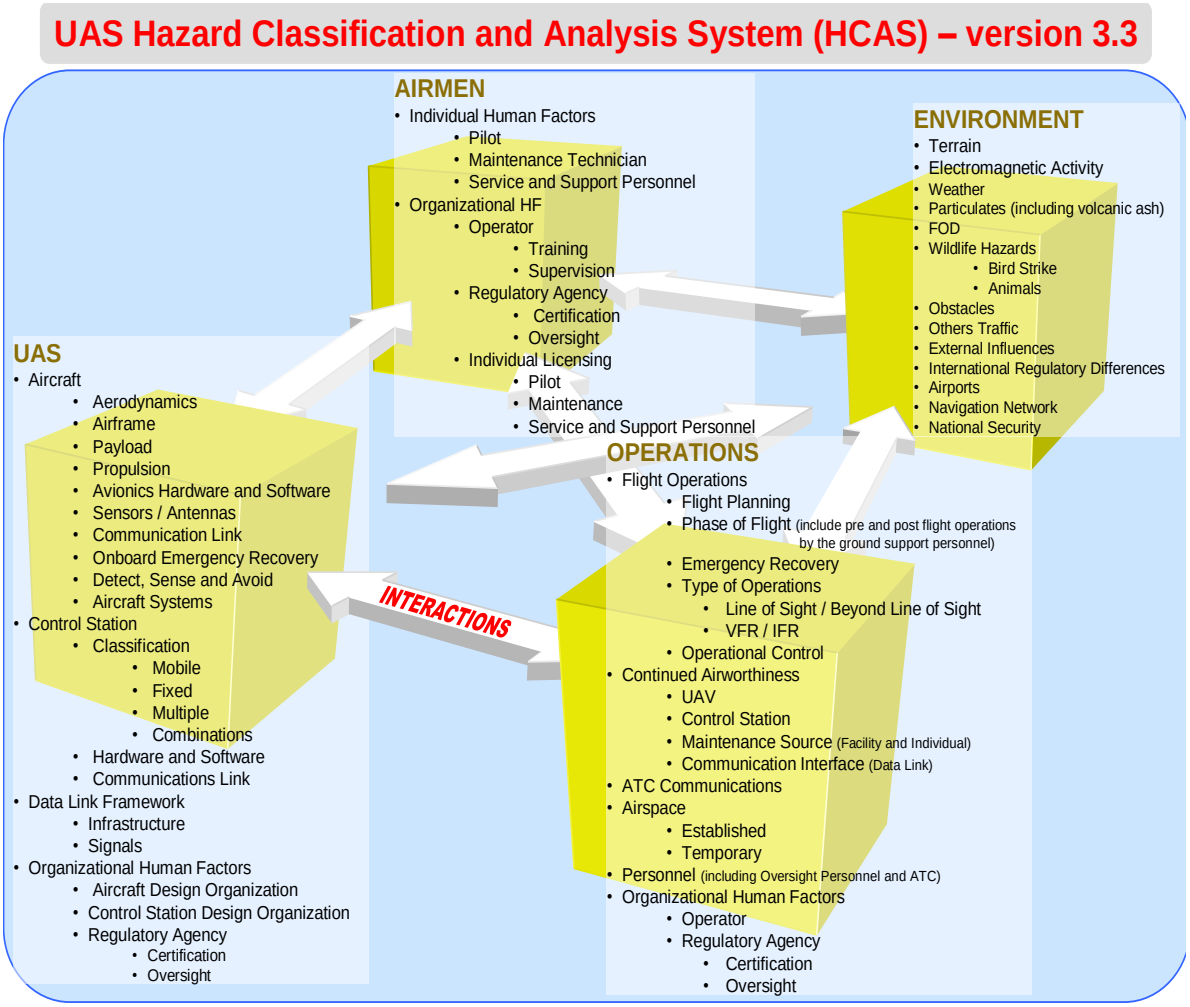

Fig. 3. HCAS – revised version

2.3 Hazard Causal Factors

Since civil UAS operations are relatively new and emergent, databases of mishaps are not readily available. In the Rutgers Phase 2 research, the proposed UAS hazard taxonomy depicted in Fig. 3 is being transformed into influence diagrams as conceptually shown in Fig. 4 for select UAS mishap scenarios. These influence diagrams will display specific hazard causal factors and their interactions. A high level, notional framework depicting the interactions among the HCAS system sources is portrayed in Fig. 5. The HCAS system sources may then be decomposed into their sub-system hazard sources as shown in Fig. 6. The use of modifiers placed on the HCAS taxonomy elements, such as "inappropriate", "inadequate", etc. may be used to create the causal factor diagram as shown for an exemplar scenario.

For example, suppose that a hypothesized UAS mishap scenario involves a UAS collision with terrain and loss of the vehicle. As illustrated in Fig. 7, an incident analysis of the hypothesized scenario reveals the existence of a strong wind conditions, thus the environment HCAS numbered element 4.2 is added. An analysis of the scenario further reveals that in switching control from one ground control station to the other due to a lock up, that UAS data links were lost. Further analysis of upstream causal factors indicated that due to deficient pilot training the UAS fuel valve was inadvertently shut off leading to a loss of engine power. Additional incident analysis noted that checklist procedures were not

followed in switching control from one ground control station to the other and some concerns about maintenance procedures may have contributed to the lock up. Fig. 7 graphically portrays how an influence diagram could be constructed using the corresponding HCAS taxonomy elements to depict possible causation. Such a causal diagramming approach is presented in [8-9] and also in [10].

Uncertainties will exist in likelihood and severity assessments and the impact of these uncertainties on UAS scenario risk evaluations need to be systematically explored. Future Rutgers research tasks will lead to the development of new analytical methods and corresponding prototype software tools for assessing the uncertainties associated with the construction of the influence diagrams of hazard causal factors for selected UAS scenarios. Such a research task will lead to more robust and defensible risk modeling and facilitate exploration of the sensitivities and impacts of both single-and multi-factor perturbations on the risk values.

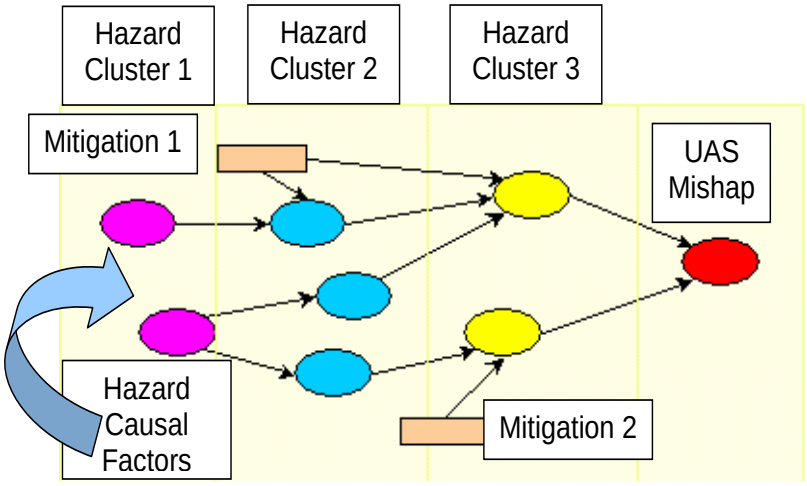

Fig. 4. Conceptual UAS Hazard Influence Diagram

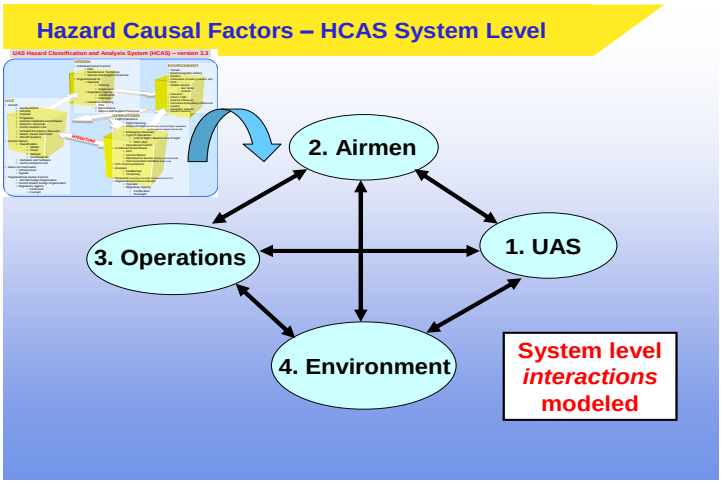

Fig. 5. Notional HCAS Causal Factor Framework

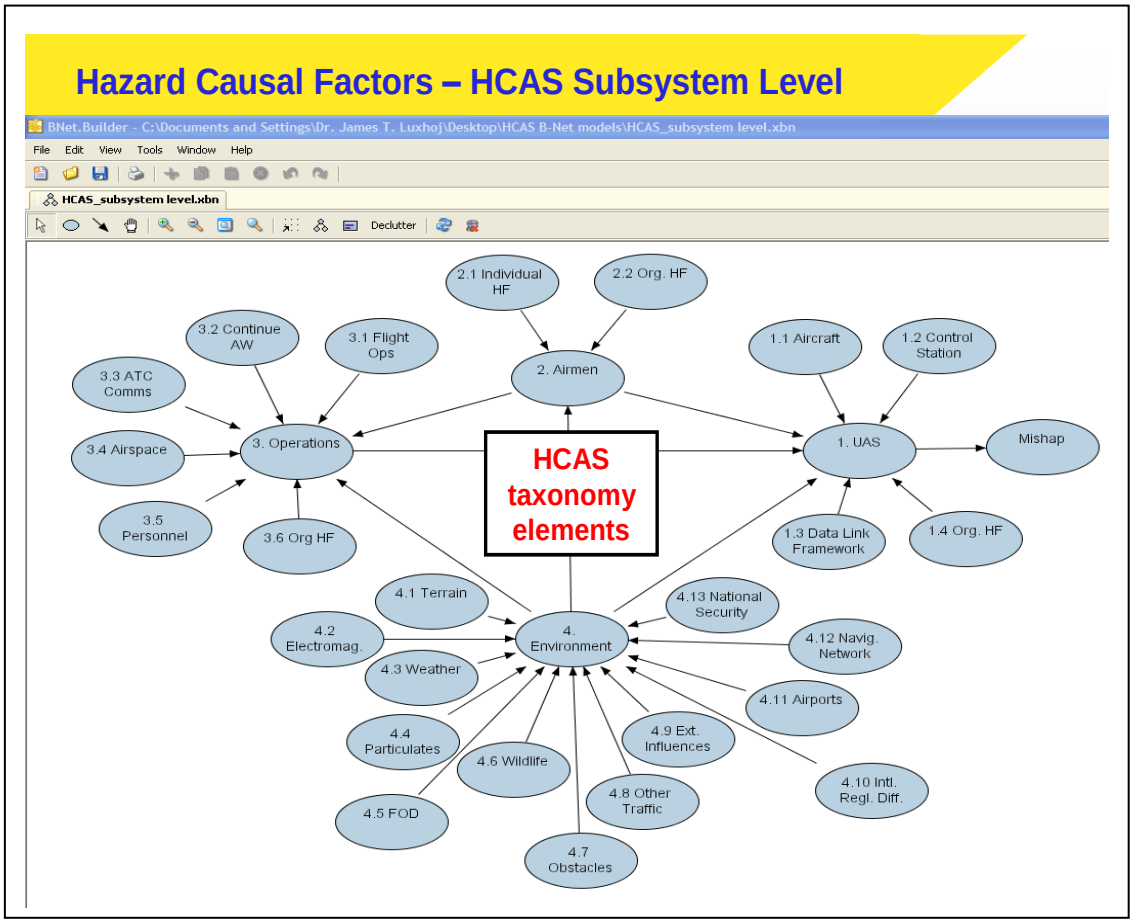

Fig. 6. Numbered HCAS Taxonomy Elements

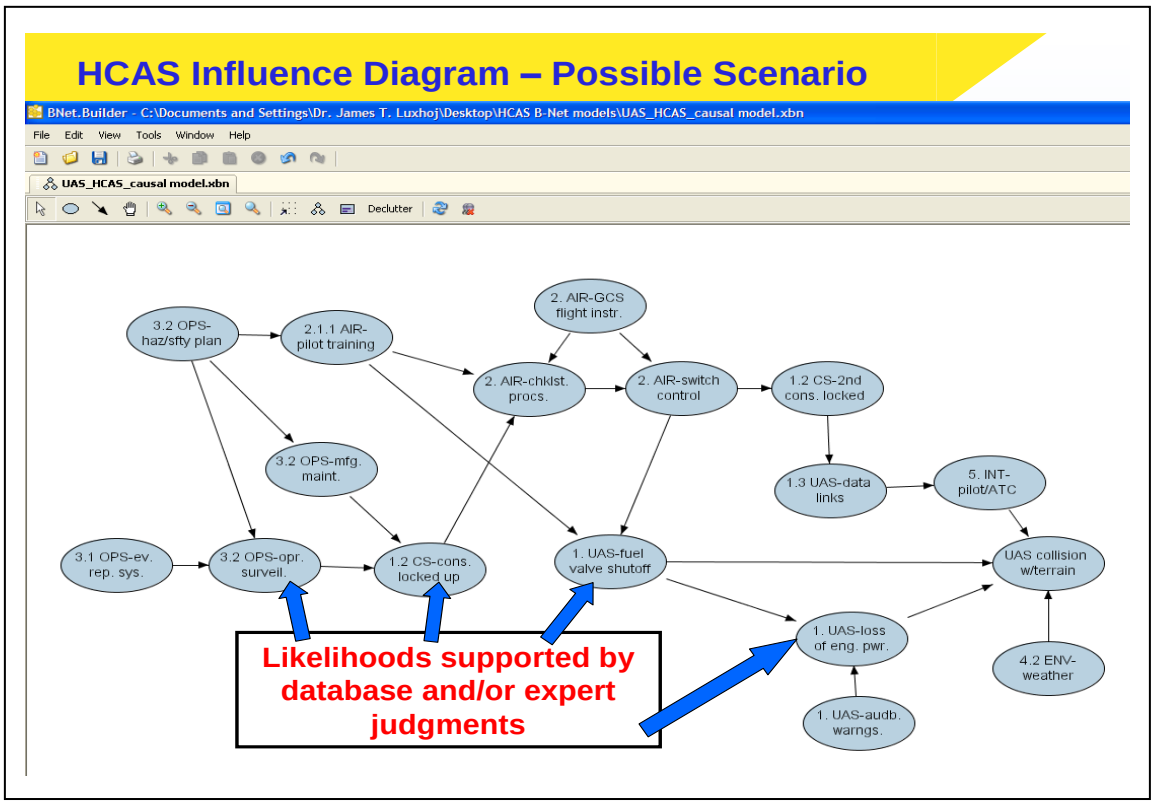

Fig. 7. Hypothesized UAS Mishap Scenario Characterization Using an Influence Diagram

3 Hybrid Risk Modeling Methodology

Consider the cluster of continuous and discrete variables shown in Fig. 8a. The variables *airspeed* measured in knots and *loss of engine power* represented by a percentage are continuous entities. The variables *data link* and *airspeed indicator*, represented by mutually exclusive states such as "up or down" and "operational or "not operational", respectively, are discrete in their nature. In this section we introduce the concept of an inferencing methodology for hybrid complex systems where the continuous variables are transformed into Fuzzy discrete variables whose states are represented by Fuzzy Sets. An example of such a transformation is illustrated in Fig. 8b. Next we outline this hybrid inferencing idea with incorporates Fuzzy Set theory and Bayesian Network.

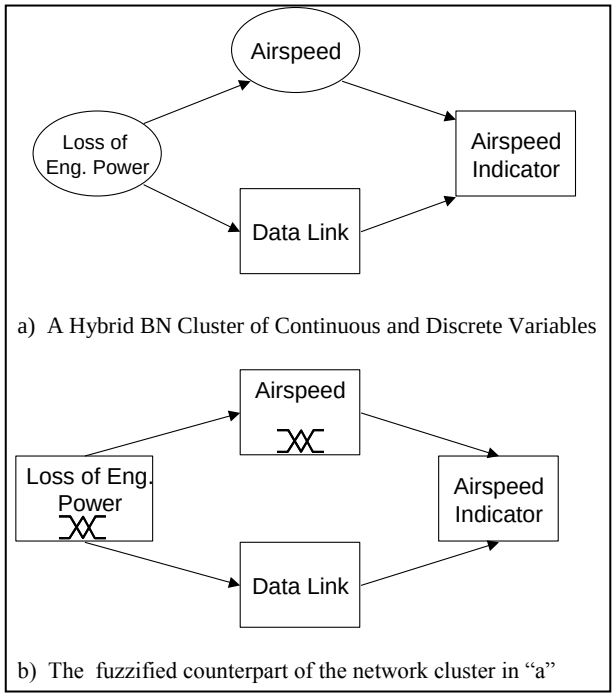

Fig. 8. A Sample Cluster of a Hybrid Bayesian Network (BN) and its Fuzzified Counterpart

Taxonomy development that is specific to a contextual domain such as UAS dramatically increases the analyst's understanding of the system to be modeled. However, without the appropriate theoretical tools supporting the proper modeling approach this contextual knowledge in the form of the taxonomy does not guaranty a realistic representation of the problem domain. In this section we introduce the conceptual basis of a hybrid risk modeling approach that, we believe, best suits the rather unique features of the UAS contextual domain.

Modeling complex systems is a very broad area of research where, more often than not, a multi-disciplinary approach is needed to achieve a meaningful representation of the subject matter. The analytical methods employed along the process remain as much art as science, especially, if the subject matter is safety and risk analysis of a complex system.

One aspect that particularly increases the complexity of modeling many real-world systems is the fact that they naturally include both discrete and continuous variables. We can further argue that because of the hybrid nature of real-world systems, many of them can best be modeled as hybrid stochastic processes, i.e., stochastic processes that contain both discrete and continuous variables. Due to their hybrid nature, they can be used in a wide variety of problem domains, such as fault diagnostics of complex machinery, pattern recognition, and risk analysis of complex systems. Although the problem domains are different, the task asked of the model is to perform probabilistic inference, such as to determine the probability of system failure given the malfunction of certain components of the machinery, to calculate the probability that a certain word is pronounced given the readings by the microphone, and to determine the likelihood that a mishap occurs given a set of precursors.

Within this context, in order to perform these tasks, an intelligent agent should be able to perform reasoning under uncertainty. As the most complex of intelligent agents, humans certainly can perform a complex reasoning task given little or no information regarding the situation they are in. The ultimate goal of a designer of an intelligent system is to mimic the human reasoning process under uncertainty and enhance it with the help of the infallible memory and unrivaled computational skills of computers.

The method of choice by the engineering and academic communities to deal with

uncertainty in real-world applications is probability theory. Probability theory is a well-established area of study with an extensive historical background of successfully understanding randomness in natural phenomena. However, its application as a tool to model uncertainty in complex real-world systems is quite recent. In particular, its use as a modeling tool started with Bayesian Networks (BNs) in the late eighties following the introduction of the concept by Pearl [11]. In a nutshell, Bayesian Networks are *directed acyclic graphs* (DAGs) that have the analogous form of an influence diagram discussed in section 2.3 and shown in Fig. 4 and Fig. 7. However, in a DAG, a probability distribution is attached to each element in the graphical structure. The DAG of a Bayesian Network is composed of *nodes* representing the variables in the domain of interest and *directed links* representing the conditional relations among the variables. Furthermore, each node is denoted by a *conditional probability distribution* (CPD) imposed by its parentage.

As popular tools for modeling uncertainty, models based on Bayesian Networks are used in a variety of complex problem domains, such as troubleshooting for MS Windows, junk e-mail filtering, medical diagnosis, and safety risk assessment in aviation.

There are two aspects of using Bayesian Networks to model uncertainty in complex systems. First is the representation of the problem domain and second is the inferencing within the resulting graphical structure. As one might expect, the majority of the research on Bayesian Networks focused on solving the inferencing problem. The research on the inferencing aspect can be further divided into two sub-categories: inferencing in discrete only Bayesian Networks and inferencing for hybrid Bayesian Networks, which include both discrete and continuous variables.

The problem of inferencing in discrete Bayesian Networks is fairly well understood and an overwhelming majority of existing studies either are based solely or focus mainly on discrete BNs. After the introduction of Bayesian Networks by Pearl, Lauritzen and Spiegelhalter proposed an exact inferencing algorithm for discrete BNs [12]. By exact inferencing, we mean that the inferencing algorithm results in exact answers to the probabilistic query given the graphical structure and CPDs of the BN. By now we have a few exact inferencing algorithms for discrete BNs and furthermore, we have a good understanding of the computational complexity of exact inferencing and how it relates to the graphical structure of the BN. Particularly, the existing exact inferencing algorithms can be very efficient for small discrete BNs.

Notwithstanding its accumulated knowledge on exact inferencing and wide acceptance on various problem domains, discrete BNs are not always adequate, since many real-world systems are not entirely composed of discrete variables. For example, consider the complex problem of assessing the safety risk associated with operating unmanned aircraft systems (UAS) in the airspace over a populated area. A Bayesian Network model of the system may include *flight-hours*, *altitude*, *speed*, and *fuel on board*, as model variables, none of which could easily be represented by discretization without sacrificing some of the representative power of the network. However, when employing BNs, crude discretization of continuous variables is commonly used to perform exact inferencing on the system model.

We understand the need for discretization of continuous variables especially in BNs where the lack of hard data forces the analysts to resort to expert judgment to quantify the model. It is quite hard, if not impossible to generate continuous conditional distributions when the distributions are required to be constructed by subject matter expert input only. However, we further argue that using simple discretization of a problem domain to be able to perform exact inferencing is equivalent to approximate reasoning and in most cases, leads to unreliable results. Consider the variable *airspeed*, which is inherently a continuous entity. Now, for the sake of computational simplicity and exact inferencing, the modeler may choose to treat it as a discrete variable with three mutually exclusive states: *slow*, *medium*, and *fast*. Further assume that the crisp boundary between states *slow* and *medium* is defined by “less than

or equal to" *80 knots* and "greater than" *80 knots* and we observe a reading from the sensors on the UAS that it is cruising at *85 knots*. According to our predetermined mutually exclusive three-state discretization scheme, we are observing a *medium* airspeed and perform the exact inferencing accordingly. However, one could argue that even though the states *slow* and *medium* are different, the actual observation about the airspeed is so close to the crisp boundary separating them that any inferencing using this discretization scheme is fundamentally flawed to produce meaningful results.

3.1 Hybrid Bayesian Networks

Hybrid Bayesian Networks (HBNs), which include both continuous and discrete variables, are a generalization on discrete only Bayesian Networks. HBNs are inherently more suitable for modeling complex systems; such as visual target tracking as in "*see and avoid*" type of applications where the variables defining location of the target and its speed are inherently continuous and speech recognition where the bits and pieces of processed audio signals are often continuous.

However, HBNs as the generalization of discrete BNs have their own shortcomings that arise when we would like to perform exact inferencing on them. Exact inferencing on general HBNs imposes restrictions on the network structure of the HBN. The state of the art exact inferencing algorithm for HBNs, the Lauritzen algorithm, requires that the network satisfies the constraint that *no continuous variables have discrete children* [13]. As one would expect, this restriction places quite a burden on the *generalization* claim of the HBNs. We propose an approach that, using *Fuzzy Set* theory, builds on the Lauritzen algorithm to generate a *hybrid* exact inferencing algorithm for *general* HBNs.

Fuzzy Set theory, introduced by Zadeh in the late sixties [14], proposes a framework to deal with a poorly defined concept in a coherent and structured way. Examples of poorly defined concepts suitable for the application of Fuzzy logic are semantic variables, such as *heavy workload, inadequate training, fast, slow, tall, short,* etc. Within the context of our current research, Fuzzy Sets present two important features worthwhile for further exploration:

- Fuzzy Sets provide a complete set of tools to partition continuous domains into overlapping membership regions, which result in a much more realistic discretization of the continuous domain in question.
- Uncertainty regarding any empirical observation can be represented as a Fuzzy measure.

Previously, we stated that Bayesian Networks are tools to model uncertainty in the form of a probability distribution imposed by a directed acyclic graph representing the domain of interest. Hence, BNs only address the uncertainty in the form of *randomness* about a problem domain. However, uncertainty in a typical real-world application has three dimensions: *vagueness*, *ambiguity*, and *randomness* [15] and BNs, being solidly anchored to probability theory, only address one of these dimensions, namely randomness. For instance, consider that there is ambiguity regarding the observed evidence associated with some variable in a given Bayesian Network.

We believe that Fuzzy Set theory offers a comprehensive structure to introduce the ambiguity dimension of uncertainty to the existing framework of classical Bayesian Networks and within this context, we are currently researching the development of a complete formalism that combines Fuzzy Sets and Bayesian Networks for reasoning about complex problems such as modeling the safety risk in UAS applications.

4 Conclusions

In this paper, a systems-level structured process for identifying, categorizing and modeling hazards for unmanned aircraft operations is presented. Termed the Hazard Classification and Analysis System (HCAS), the taxonomy comprises a core of four cubes representing

system and sub-system hazard sources. Hazards are not causal factors, so a notional method is also presented that relies upon influence diagrams to depict the interactions of causal factors in unmanned aircraft mishaps. These influence diagrams may then be used to facilitate subsequent risk analysis for a complex system. The concept of a hybrid fuzzy-Bayesian approach is outlined that is being developed to handle both discrete and continuous variables when uncertainty and vagueness may co-exist in the safety risk analysis. Future research involves more mathematical development of the hybrid methodology and applications to the unmanned aircraft contextual domain.

5 References

[1] Clothier, R, and Walker, R. Determination and evaluation of UAV safety objectives, *Proceedings of 21st International Unmanned Air Vehicle Conferenc*e, Bristol, United Kingdom, pp. 18.1-18.16., 2006.

[2] Hayhurst, K, Maddalon, J, Miner, P, DeEalt, M and McCormick, G. Unmanned aircraft hazards and their Implications for regulation, *25th Digital Avionics Systems Conference*, pp. 5B1-1 – 5B1-12, October 15, 2006.

[3] Weibel, R and Hansman, R. Safety considerations for operations of different classes of UAVs in the NAS," *AIAA's 4th Aviation Technology, Integration and Operations (ATIO) Forum*, Chicago, IL, September 20-22, 2004.

[4] Oztekin, A, Luxhøj, J and Allocco, M. A general framework for risk-based system safety analysis of the introduction of emergent aeronautical operations into the national airspace system, *Proceedings of the 25th International System Safety Conference*, Baltimore, MD, August 13-17, 2007.

[5] Luxhøj, J. *Safety Risk Analysis of Unmanned Aircraft Systems (UAS) Integration into the National Airspace System (NAS): Phase 1 Final Report*, Department of Transportation. Federal Aviation Administration, January 31, 2008.

[6] Leveson, N. *Safeware: system safety and computers*, Addison-Wesley Publishing Company, 1995.

[7] Unmanned aircraft system operations in the U.S. National Airspace System – interim operational approval guidance, Federal Aviation Administration, AFS-400 UAS Policy 05-01, September 16, 2005.

[8] Luxhøj, J. Probabilistic causal analysis for system safety risk assessments in commercial air transport, *Proceedings of the Workshop on Investigating and Reporting of Incidents and Accidents (IRIA)*, Williamsburg, VA, pp. 17-38, September 16-19, 2003.

[9] Luxhøj, J. Model-based reasoning for aviation safety risk assessments, *SAE World Aerospace Congress*, Dallas/Fort Worth, Texas, October 3-6, 2005.

[10] Ale, B, Bellamy, L, Cooke, R, Goossens, L, Hale, A, Kurowicks, D, Roelen, A and Smith, E. Development of a causal model for air transport safety, *Proceedings of the European Safety and Reliability Conference*, Tri City, Poland, pp. 37-44, June 27-30, 2005.

[11] Pearl, J. *Probabilistic reasoning in intelligent systems: networks of plausible inference*, Morgan Kaufmann, San Francisco, CA 1988.

[12] Lauritzen, S, Spiegelhalter, D. Local computations with probabilities on graphical structures and their applications to expert systems, *The Journal of the Royal Statistical Society*, B, 50(2), pp. 157-224, 1988.

[13] Lauritzen, S. Propagation of probabilities, means, and variances in mixed graphical association models, *JASA*, 87(420), pp. 1089-1108, 1992.

[14] Zadeh, L. Fuzzy sets, *Inf. Control*, 8, pp. 338-353, 1965.

[15] Ross, T. *Fuzzy logic with engineering applications*, McGraw-Hill, New York, 1995.

6 Acknowledgments

This research is supported by Federal Aviation Administration grant number 06-G-008. The contents of this paper reflect the views of the authors who are solely responsible for the accuracy of the facts, analyses, conclusions, and recommendations represented herein, and do not necessarily reflect the official view or policy of the Federal Aviation Administration. The authors acknowledge the support, participation and guidance of Dr. Xiaogong Lee, Mr. Michael Allocco, Mr. Steve Swartz, Mr. Robert Anoll and the FJ Leonelli Group, Inc. to the Rutgers research.

Copyright Statement