

Predictive Analytics for Modeling UAS Safety Risk

James T. Luxhoj
LCR

ABSTRACT

This paper illustrates the development of an Object-Oriented Bayesian Network (OOBN) to integrate the safety risks contributing to a notional “lost link” scenario for a small UAS (sUAS). This hypothetical case investigates the possibility of a “lost link” for the sUAS during the bridge inspection mission leading to a collision of the sUAS with the bridge. Hazard causal factors associated with the air vehicle, operations, airmen and the environment may be combined in an integrative safety risk model. With the creation of a probabilistic risk model, inferences about changes to the states of the mishap shaping or causal factors can be drawn quantitatively. These predictive safety inferences derive from qualitative reasoning to conclusions based on data, assumptions, and/or premises and enable an analyst to identify the most prominent causal factor clusters. Such an approach also supports a mitigation portfolio study and assessment.

An OOBN approach facilitates decomposition at the subsystem level yet enables synthesis at a higher-order systems level. It is essentially a System of Systems (SoS) approach that fosters the integration of sub-nets of risk factors. Such a study provides insight into the integration of UAS into the National Airspace System (NAS) that may be used to eventually inform type design, airworthiness, certifications, safety analyses and risk assessments, and operational requirements.

CITATION: Luxhoj, J., "Predictive Analytics for Modeling UAS Safety Risk," *SAE Int. J. Aerosp.* 6(1):2013, doi: 10.4271/2013-01-2104.

INTRODUCTION

Presently, manufacturers and operators of small Unmanned Aircraft Systems (sUAS) in the United States are seeking access to the National Airspace System (NAS) for a variety of emerging missions, such as border patrol, crop monitoring, firefighting, pipeline and police surveillance, scientific experiments, etc. As sUAS operations are relatively new when compared to manned aviation, non-military accident and incident data are extremely rare, so alternative modeling approaches to conventional fault tree and event tree logic are being developed to understand the potential impact of the introduction of sUAS operations into the NAS. While alternative real-time and fast-time simulation modeling research for UAS in the NAS is a major focus area of the aerospace industry and government agencies, the development of complementary probabilistic analytical methods and tools for hazard and risk modeling needs to similarly advance.

This paper presents a *hypothetical* case study gleaned from the author's participation in Federal Aviation Administration (FAA) and National Aeronautics and Space Administration (NASA) projects that address UAS hazard

and safety risk modeling. Analytical methods to address 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 are demonstrated with a case study application. In particular, a systems view of hazards and risks is discussed with a perspective toward regulatory concerns.

SYSTEM SAFETY ANALYTICS

System safety analysis emerged as a separate and unique discipline in the early 1960s with the advent of NASA's Apollo missions and the development of the U.S. Air Force Ballistic Missiles [1]. Safe integration of UASs into the NAS presents significant challenges to all parties of the aviation community. Although the main thrust of this emerging technology originates from entrepreneurs, both civilian and military, the burden of the safe integration resides with the regulatory agencies such as the FAA. The question of safety associated with this integration arises principally due to the unknowns of potential hazards and associated risks while operating in the NAS and interacting with existing NAS users. Formally, UAS is defined as: *A device used or intended*

to be used for flight in the air that has no onboard pilot, which is a clarification of the existing *Aircraft* definition, 14 CFR §1.1, which indicates that UAS operations are governed by the existing regulations [2]. The FAA Concept of Operations for UAS integration in the NAS was recently published [3].

In the past, when incidents or accidents occurred, a forensic approach was undertaken in the hazard analysis phase of the system safety approach. While such a forensic approach has merit and remains important and useful to system safety analysts, it is quite dependent on the contextual factors involved in the specific incident or accident. As such, the safety recommendations emerging from such a forensic analysis may be quite aircraft type or airport specific. The system safety approach involves an identify-analyze-control method of safety as opposed to a “fly-fix-fly” approach [1]. It may be contended that the system safety approach is better suited to safety analysis of new classes of aircraft where data is sparse and operations are limited. In particular, UAS represent a new class of aircraft that is emerging in the current NAS and that will most likely be an integral component of the U.S. Next Generation (NextGen) Air Transport System and the Single European Sky (SESAR). The basic building block for both NextGen and SESAR involves creating an operating environment in four dimensions: latitude, longitude, altitude, and time [4]. It is envisioned that the NextGen will facilitate the move to “free-flight” where satellite-derived positioning data is transmitted via a digital data link to the ground and every aircraft in the sky will then select its own flight path for optimal speed, fuel consumption and turbulence avoidance [4].

This new UAS frontier in civil aviation adds another dimension to the ever-increasing complexity of the current NAS in the United States. The future inclusion of private and commercial operations of UAS into the NAS, unavoidably, raises safety concerns. As the NAS becomes increasingly more complex and constrained, the associated hazard and safety risk modeling must also mature in sophistication. Thus, there is a need for advanced studies focusing on risk-based system safety analysis of emergent UAS operations.

Hazard Analysis

One of the first steps in a UAS system safety analysis is hazard identification and analysis. A nascent taxonomy, termed the Hazard Analysis and Classification System (HCAS) identifies four main hazard system sources: Airmen, UAS, Operations, and Environment [5]. The basic framework of the proposed taxonomy is based on the FAA regulatory perspective (i.e., Title 14, Code of Federal Regulations (14 CFR) chapters on Aircraft, Airmen, Flight Operations, Certification/Airworthiness, etc.). 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 [6,7], etc. A graphical depiction of the HCAS is included in the Appendix as Figure 16.

Safety Risk Management

The HCAS may be used for hazard identification when considering a possible UAS scenario. A six-step process has been developed and refined for aviation safety risk modeling. The model, termed the Aviation System Risk Model (ASRM), is described in [8]. The ASRM can be used to evaluate the causal factors linked to the vehicle and/or the NextGen systems and procedures that led to the unsafe state and the interactions among these factors that contributed to the safety risk. The ASRM can also assess the projected impact that new vehicle design changes and/or NextGen systems and procedures may have on potentially reducing the likelihood of some significant causal factors. The ASRM uses the flexible, probabilistic approach of Bayesian Belief Networks (BBNs) [9] and influence diagrams to model the *complex interactions* of aviation system risk factors. Accidents are seldom, if ever, the result of a single hazard. A shortcoming in the typical hazard analysis approach is to focus on a single hazard and risk assessment. Combining the individual hazard assessments inherent in a complex system to arrive at an overall level of system risk is a difficult challenge. Safety practitioners need to deal with numerous inherent hazard scenarios that a complex system operation can generate. The ASRM approach achieves a better understanding of the dynamics of these scenarios. It permits robust inductive reasoning on the hypothesized accident scenarios, ideal for addressing emergent NAS operations where there may be obvious data and experience limitations.

The ASRM essentially follows the FAA's safety risk management (SRM) approach. The initial ASRM has since been adapted for UAS safety risk modeling. A schematic of the 6-step ASRM process is depicted in Figure 1. The ASRM process involves systemically following six steps. These steps include:

1. Selecting and analyzing a “representative” case.
2. Identifying the case-based causal factors.
3. Constructing an influence diagram depicting causal factor interactions.
4. Building a Bayesian Belief Network (BBN).
5. Inserting technologies/interventions.
6. Evaluating the relative risk associated with the insertions.

The first two steps are fundamental to accident/incident analyses, but it is in step 3 that the process starts to depart from traditional approaches. Figure 2 displays the general structure of a Bayesian Belief Network (BBN) with chance nodes or variables represented as circles (see X1, X2, ...) and decision nodes (see D1, D2, and D3) shown as rectangles. A decision variable can be related to one or multiple chance variables or multiple decision variables can be related to one particular chance variable. In this research, the decision nodes represent the mitigations, such as new technologies and/or

procedures. After the UAS scenario causal factors have been identified and grouped into the HCAS “clusters”, the interactions among the factors as qualitatively discussed in the scenario description are drawn using an influence diagram. Such an influence diagram approach enables the depiction of multiple causalities and facilitates more complex, conditional reasoning. After the completion of this step, the basic causal structure has been created.

Risk Modeling Steps

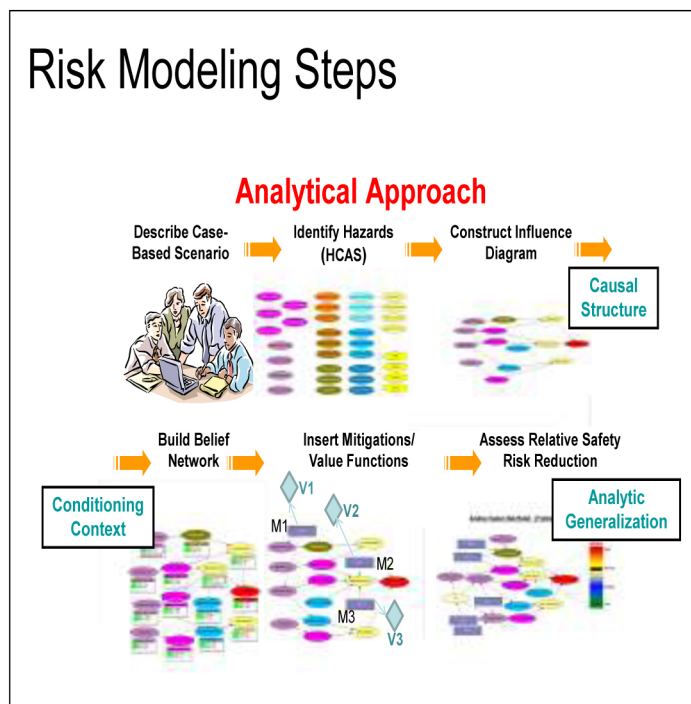


Figure 1. The Aviation System Risk Model (ASRM) steps. (Source: [8])

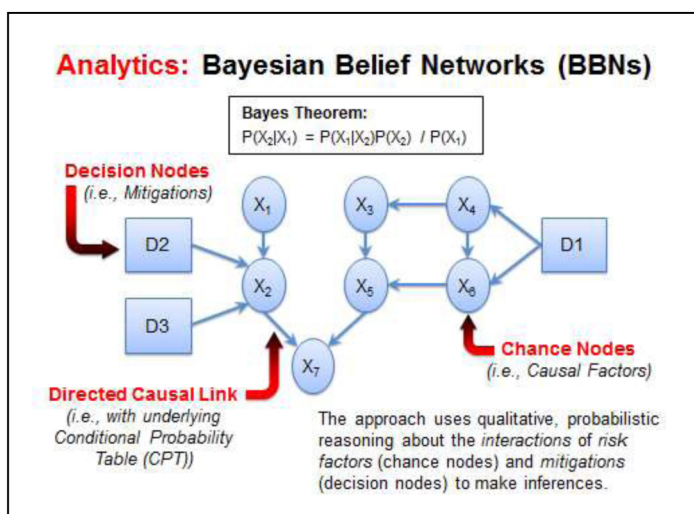


Figure 2. Elements of a Bayesian Belief Network (BBN). (Source: [10])

OBJECT-ORIENTED BAYESIAN NETWORKS

The development of the sUAS risk model follows an object-oriented approach. In general, a number of sub-nets of causal factors are created that model the Vehicle (i.e., UAS), Operations, Airmen and the Environment-related hazards at the sub-system level. Causal factors emanate from hazards. These sub-nets of causal factors are then linked using the instance node capability in the Hugin BBN software (<http://www.hugin.dk>; [9]). By explicitly labeling the output node in a sub-net, this output becomes the input to a “summary model” via the use of an “instance node”. The instance node provides interfacing functionality. Thus, the sUAS risk model prototype demonstrates the features of an OOBN. Such an approach facilitates decomposition at the sub-system level yet enables synthesis at a higher-order systems level. It is essentially a System of Systems (SoS) approach. Figure 3 illustrates the construction of a notional OOBN with two hypothetical sub-nets. Hierarchical BBNs or OOBNs are further discussed in [10,11]. Since the sUAS risk model is a prototype, the intent is to demonstrate a breadth of modeling capability rather than depth.

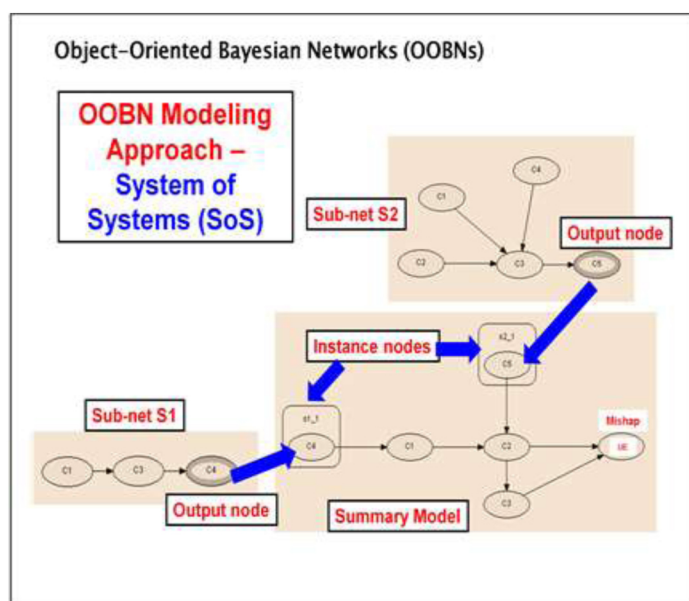


Figure 3. An Object-Oriented Bayesian Network (OOBN). (Source: [10])

Application Scenario

This application scenario is inspired from a technical report by [13] from the Intelligent Transportation Systems Institute in the Center of Transportation Studies at the University of Minnesota. The developed Hugin model demonstrates the features of an OOBN in that the approach facilitates decomposition at the sub-system level yet enables

synthesis at a higher-order systems level. As previously noted, it encompasses a System of Systems (SoS) approach.

sUAS CONOPS

As presented in [13], the Concept of Operations (CONOPS) involves a small UAS (sUAS) (< 55 lbs.) operating close to a bridge that is equipped with a camera that can be used to capture video or still images for the purpose of bridge infrastructure inspection. The sUAS could be transported in the trunk of most any vehicle to the area of operation. The scenario involves a tactical sUAS operation and the major safety risks are possible collisions with the bridge infrastructure or secondary collisions with objects below. Figure 4 presents a notional diagram of the scenario to be modeled.

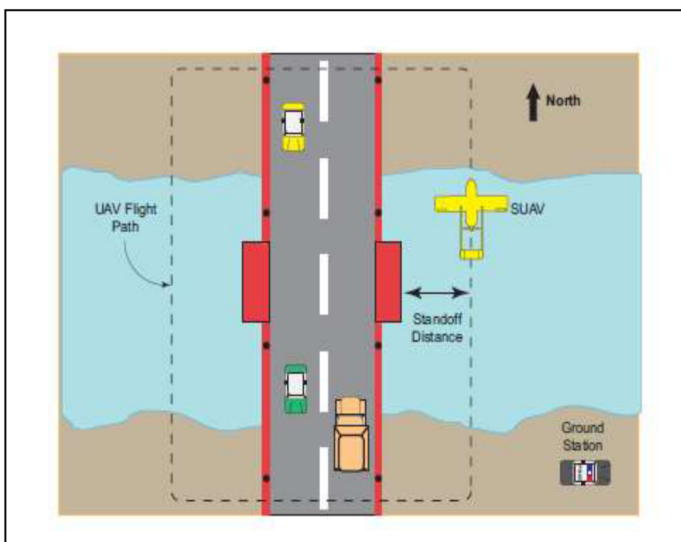


Figure 4. sUAS bridge infrastructure inspection. (Source: [13])



Figure 5. sUAS Unicorn. (Source: [14])

The sUAS is modified from a kit modified by Unicorn Wings (<http://unicornwings.stores.yahoo.net>). Known as the Unicorn it has a flying wing design with up to a 48 inch wingspan and is depicted in Figure 5. For this sUAS, an open-source Guidance, Navigation and Control (GNC) software suite for autonomous operation was used as a tool to enhance situational awareness. Figure 6 depicts a functional

block diagram of the airborne and ground systems that comprise the sUAS and highlights the information flow. The details of the components of this sUAS built from off-the-shelf components except for the ground station software are presented in [14].

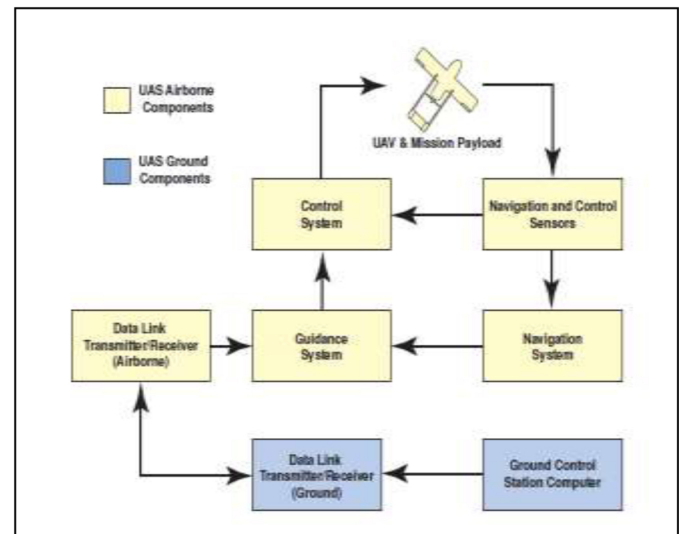


Figure 6. sUAS functional block diagram. (Source: [13])

As described in [13], this sUAS operation initiates by the crew setting up the ground station that is comprised of a laptop with a data link radio. As part of their normal safety procedures, the ground crew inspects the air vehicle (airframe, power plant and avionics) to ensure that the sUAS is airworthy. The crew also performs an operational check of the data link between the ground and air vehicle. Since the bridge inspection is in response to a scheduled infrastructure inspection, an operation plan was planned in advance that is consistent with the local weather and any operational constraints. Once the sUAS is launched, it begins operating per the operation plan and procedures unless an emergency arises. For example, the operational plan may stipulate that the sUAS fly a “race track” pattern as illustrated in Figure 4. The operational plan should specify how close the sUAS must be from the structure it is inspecting and these specifications are based on the mission payload requirements (camera resolution) and control system. For the bridge inspection, the “standoff” distance is an operational requirement.

As reported in [13], some possible safety risks include, but are not limited to, data link failure, engine failure, control system lack of authority, and navigation system stochastic errors. While some of the values in the conditional probability tables will change, much of the sUAS bridge infrastructure inspection scenario corresponds closely with the overall BBN structure of the two previously presented hypothetical sUAS scenarios.

To extend the sUAS bridge inspection operational scenario as described in [13], a causal narrative, or “story”