International Journal of Aviation, Aeronautics, and Aerospace

Volume 3 | Issue 1 Article 2

2-16-2016

System Safety Modeling of Alternative Geofencing Configurations for small UAS

James T. Luxhoj
LCR, jtluxhoj@gmail.com

System Safety Modeling of Alternative Geofencing Configurations for small UAS

Cover Page Footnote

This material is based upon research supported by NASA under Prime Award Number NNX11AO78A through a sub-contract from the University of Michigan. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author and do not necessarily reflect the views of NASA or the University of Michigan.

With the advent of small UAS (sUAS) into the National Airspace System (NAS), it is imperative that safety analysis play a fundamental role 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 sound system-level safety analysis relies heavily on properly identifying the key elements of the area of interest. In particular, the identification of potential hazard sources and sub-sources within the systemic structure of the problem domain should be considered as a fundamentally important step in system safety analysis. Furthermore, since semantics play a crucial role while defining the domain variables, a systematic hazard taxonomy that balances fidelity and generalization provides a solid foundation for a meaningful and relevant system safety analysis. System-level safety analysis relies heavily on accurately identifying the key elements from a socio-technical perspective of the area of interest that includes the human/machine interface and cyber-physical aspects. UAS hazard identification and safety risk modeling especially need to be performed within the context of operational scenarios. Hayhurst et al. (2015a) contend that design and performance criteria supporting the development of UAS airworthiness standards need to be examined "in tandem" with a specific UAS concept of operations (p. vii).

Significance

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. Since these air vehicle operations are new, accident and incident data are extremely rare, so alternative modeling approaches to conventional fault tree and event tree logic are required to understand the impact of the introduction of these operations into the NAS. A novel safety risk modeling approach that proposes the use of Bayesian Belief Networks (BBNs) to develop nonlinear, probabilistic risk models, at a systems level, of the socio-technical interactions of hazards, causal factors and mitigations is investigated.

Problem Statement

The problem examined is to determine if a probabilistic system safety model could be used to evaluate the efficacy of alternative configurations of a geofencing mitigation for sUAS from a socio-technical perspective.

Literature Review

Hazard Identification

Hazard identification precedes safety risk modeling (Ericson, 2005). To facilitate hazard identification in the aviation domain, a taxonomy, termed the Hazard Classification and Analysis System (HCAS), was developed for identifying sources of hazards for aircraft operations in the NAS (Luxhøj, 2009). The HCAS is a systems-level taxonomy that comprises the four main hazard sources of UAS, Airmen, Operations and Environment and their interactions as well as the constituent sub-sources. The underlying hazard approach builds upon the concepts previously presented in Hammer (1972) and Raheja and Allocco (2006). In discussing hazard analysis, Hammer presents concepts of initiators, contributors, and primary hazards. There is typically not a single hazard leading to an accident or incident, but rather multiple hazards activated by some triggering mechanism. Ericson (2005) presents the notion of a "hazard triangle" that involves defining the hazardous element, specifying the triggering mechanism, and identifying the target or threat. Raheja and Allocco (2006) further extend Hammer's approach to develop the Scenario-Driven Hazard Analysis (SDHA) process. The SDHA may be used to understand the dynamics of either an actual or hypothesized accident. When operational experience matures and incidents occur, the HCAS may be used to systematically classify the event data into hazard sources that will connect to a high level grouping of causal factors. Currently, there are approximately 125 system "elements" comprising the hazard taxonomy. Figure 1 provides a high-level notional diagram of the HCAS and its interactions while Figure 2 displays the current version of the HCAS taxonomy.

Safety Risk Modeling

The HCAS may be used for hazard identification when considering a possible aviation-related mishap scenario. From the hazards, a creative process is then initiated to use language to translate hazards into risk factors that are causal to the undesired event. Harkleroad et al. (2013) present a recent review of "state of the art" risk-based modeling approaches, with special emphasis on tools that are potentially useful during the concept development phase for the Next Generation Air Transportation System (NextGen). Six different current risk-based models are reviewed. These authors categorize the models along a spectrum of "influence-based" versus "event-based" with the mid-point on the spectrum being models that are equally influence- and event-based. Influence-based risk models include system-wide factors such as management oversight, training, maintenance, among others, that will influence the likelihood of discrete events. Event-based models treat risk as the result of various possible event sequences or

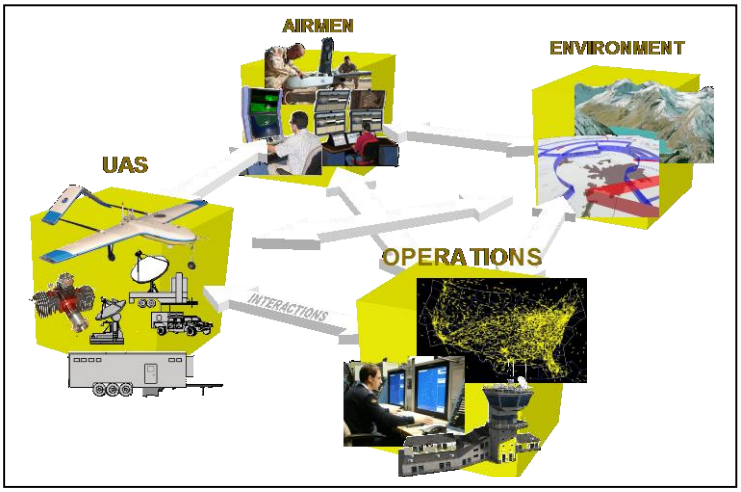

Figure 1. High-level Notional Diagram of the HCAS (Source: Luxhøj and Öztekin, 2009).

transitions between system sates. Harkleroad et al. (2013) note that an exemplar of a more influence-based risk model is the Systems-Theoretic Accident Model and Processes (STAMP) developed by Leveson (2004, 2011) and Leveson et al. (2006) that is also reviewed in Netjasov and Janic (2008). STAMP intends to integrate varied aspects of risks, including organizational and social issues. STAMP uses general concepts from control theory to support the building of shared mental models of complex system behavior and especially focuses on the role of explicit constraints in safety management. Harkleroad et al. (2013) note that an exemplar of a more event-based risk model is The Traffic Organization and Perturbation Analyzer (TOPAZ) that is also reviewed by Netjasov and Janic (2008). The TOPAZ method uses scenario analysis and Monte-Carlo simulation for safety risk assessment of Air Traffic Control (ATC)/Air Traffic Management (ATM) operations.

While Monte Carlo analysis supports broad uncertainty quantification by sampling from alternative probability distributions, a criticism of Monte Carlo simulation is that it has a narrower range than "what if" scenario analysis as "what if" analysis provides equal weighting to all scenarios while the Monte Carlo method seldom samples rare events in the very low probability regions. TOPAZ also aims to include organizational, environmental, human-related and other hazards, as well as their combinations, in an integrative risk assessment. With its focus on ATC/ATM operations, the primary goal of TOPAZ is to identify safety bottlenecks that can then be used to guide improvements to the operations (Blom et al., 2002). A recent article by Wallace and Loffi (2015) examines the emergence of security issues, threats and defenses associated with UAS technology.

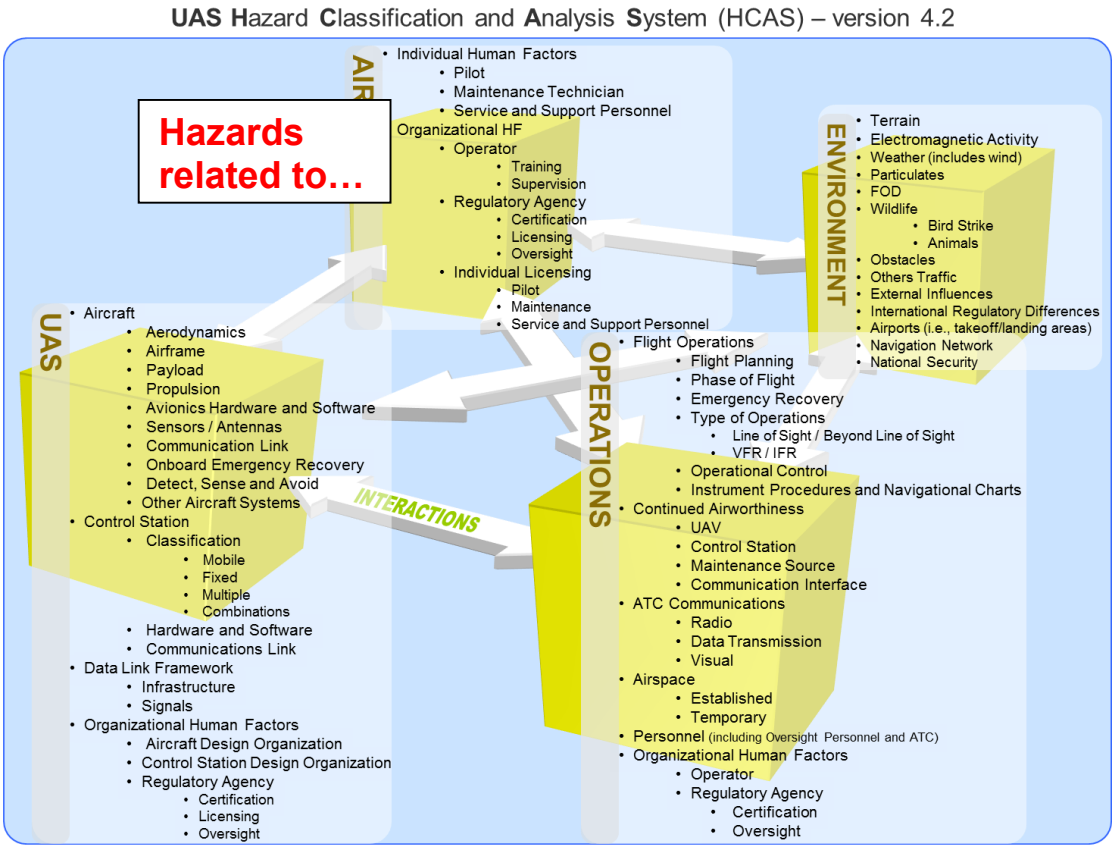

Figure 2. Hazard Classification and Analysis System (HCAS) Taxonomy (Source: Luxhøj, 2014a).

Harkleroad et al. (2013) and Griffin et al. (2105) report on a risk-based method for integrative aviation safety risk modeling and analysis developed and refined by Luxhøj (2003) termed the Aviation System Risk Model (ASRM). Harkleroad et al. (2013) position the ASRM as an exemplar of a risk-based method that is equally influence- and event-based. The ASRM can be used to evaluate the causal factors linked to a *hypothesized* scenario involving an air vehicle and/or the NextGen systems and procedures that led to an unsafe state and the interactions among these factors that contributed to the safety risk. The ASRM, a first generation socio-technical model, 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 significant causal factors. The ASRM uses the flexible, probabilistic approach of Bayesian Belief Networks (BBNs) and influence diagrams to model the *complex interactions* of aviation system risk factors.

The ASRM is viewed as complementary to both the STAMP and TOPAZ methods since all three methods focus on an integrative safety risk assessment. However, the ASRM may be considered to be at a more macro-level than the STAMP and TOPAZ methods and may be more appropriate for operations that are completely novel where statistical data do not exist, such as for the sUAS application under study. Thus, the ASRM was identified as the risk-based method to investigate for possible use as a decision support tool for this sUAS study. Accidents are seldom, if ever, the result of a single hazard. Combining the individual hazard assessments inherent in a complex system to arrive at an overall level of system risk is a difficult challenge, especially for emergent flight operations with obvious data limitations.

The ASRM process, as described in Luxhøj (2003), involves systemically following six steps:

1. Selecting and analyzing a scenario.
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 mitigations and value functions (optional).
6. Evaluating the relative risk associated with the insertions.

Geofencing

There is growing research in the use of autonomy for UAS, especially as missions become more complex (NRC, 2014; How et al., 2009). However, there are a number of issues confronting autonomous operations for UAS that deal with safety and latency (McKinlay, 2014; Wagner, 2008). How et al. (2009, p. 43) contend that "a critical component for networks of autonomous vehicles is the ability to detect and localize targets of interest in a dynamic and unknown environment". Typically, the architecture for a system of autonomous vehicles involves an onboard vision module (OVM), an onboard planning module (OPM) and an autopilot module (APM) that work together to perform the sensing, planning and control of each vehicle as shown in Figure 3. A geofence, one component in the move towards UAS autonomy, uses the Navstar Global Positioning System, or herein referred to as simply GPS, to check that a UAS is within its designated area of operation. If the UAS approaches or exits this area, a return-to-operating area instruction is automatically executed to bring the UAS back inside its designated area of operation that is defined by minimum and maximum altitude as well as by lateral latitude and longitude constraints (http://itlaw.wikia.com/wiki/Geofencing). GPS performance parameters include availability, continuity, integrity and accuracy (GPS, 2008). The Wide Area Augmentation System (WAAS) provides

an augmentation signal to GPS that provides correction and integrity information intended to improve positioning, navigation and timing (PNT) service over the US and portions of Canada and Mexico (WAAS, 2008). Badura (2004) presents a general discussion of mitigations for GPS vulnerabilities. There remain a number of challenges for the integration of UAS into the NAS but autonomous operations, if certified, could provide a progressive step towards routine use of UAS in the NAS (Dalamagkidis, et al., 2008; NASA Tech Briefs, 2016).

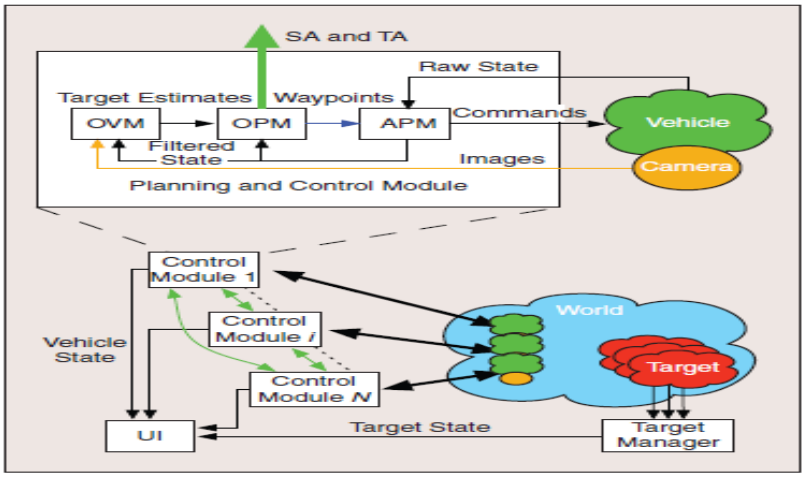

Figure 3. Basic Components of an Autonomous System (Source: How et al., 2009, p. 44).

Methodology

Building a Bayesian Belief Network (BBN)

When constructing causal models, one of the most important factors that should be considered is the impact of uncertainty. In essence, probability theory derives solutions from reasoning under uncertainty in the face of limited information. In recent years, Bayesian Belief Networks (BBNs) have emerged as the principal methodology for numerous problems that involve reasoning under uncertainty in complex decision making arenas (Fenton and Martin, 2013). Belief networks provide symbolic representations of probability models combined with efficient inference algorithms for probabilistic reasoning (Jensen, 1996). An Undesired Event (UE) is not deterministic so any modeling effort needs to capture the probabilistic nature of multiple causalities as shown in Figure 4. A BBN is a graphical approach that allows the "quantification" of safety risk models by using conditional probability theory. It is in this step where the conditional probability of one causal factor given the presence of other factor(s) is estimated using the

"beliefs" of subject matter experts. While BBNs have also been combined with the Analytic Hierarchy Process (AHP) (Ha & Seong, 2004, Ahmed et al., 2005; Park, et al., 2014) to assist in the probability quantification of accident precursors in some cases, the AHP is not used in this initial UAS geofencing study due to resource constraints. The gathering of the AHP data presents another elicitation burden and only offers an indirect method of obtaining the desired conditional probabilities.

Aviation accidents are rare events so it is challenging to obtain hard data to quantify the models, particularly in the case of UAS. An event tree could possibly be used to obtain some numerical "seeds" for the model, but an event tree is not an influence diagram and the interpretation of the numbers is not the same. With the BBN approach, the numbers in the Conditional Probability Tables (CPTs) essentially represent the strength of the belief in the conditional causality as assessed by the expert for the scenario under study. A similar approach was used by Ang and Buttery (1997) in their risk assessment study of nuclear power plants. The approach involves moving up the systems ladder a bit and necessitates that the subject matter experts rely upon their mental model repository of similar cases. With a systems expansion viewpoint, the experts establish some basic boundary conditions, such as a towered airport, moderate traffic density, time period, etc. to set the conditioning context. This systems interpretation is consistent with the conceptual notion of "analytic generalization". These conditional probabilities serve to baseline the safety risk model.

Alternative Geofencing Configurations

Luxhøj (2015) presents a UAS precision agriculture application that involves the analysis of a geofencing mitigation. In that paper, the geofence is considered as a decision node with Boolean state variables (i.e., either present or absent). Atkins (2014) proposes alternative geofencing configurations, such as using a single onboard processor that integrates the datalink, autopilot and geofencing functions vs. the use of a separate processor solely for the geofencing function. As Atkins (2014) proposes, a single onboard processor as conceptually shown in Figure 5 could handle all nominal functionality plus geofencing. If other software on the shared processor fails, the geofence will also fail suggesting a fault tree logic OR gate. As in Atkins (2014), a second configuration conceptually depicted in Figure 6 is where the "geofence software is pulled onto a separate (micro)processor with the sole purpose of ensuring that the vehicle remains within its designated operating area" (Atkins, 2014, p. 11). A third configuration suggested by Atkins (2014), involves full redundancy as conceptually depicted in Figure 7 where the processors use "independent servo connections and inertial navigation sensors as well as logic

such as a watchdog-triggered bypass for servo output source selection" (Atkins, 2014, p. 11).

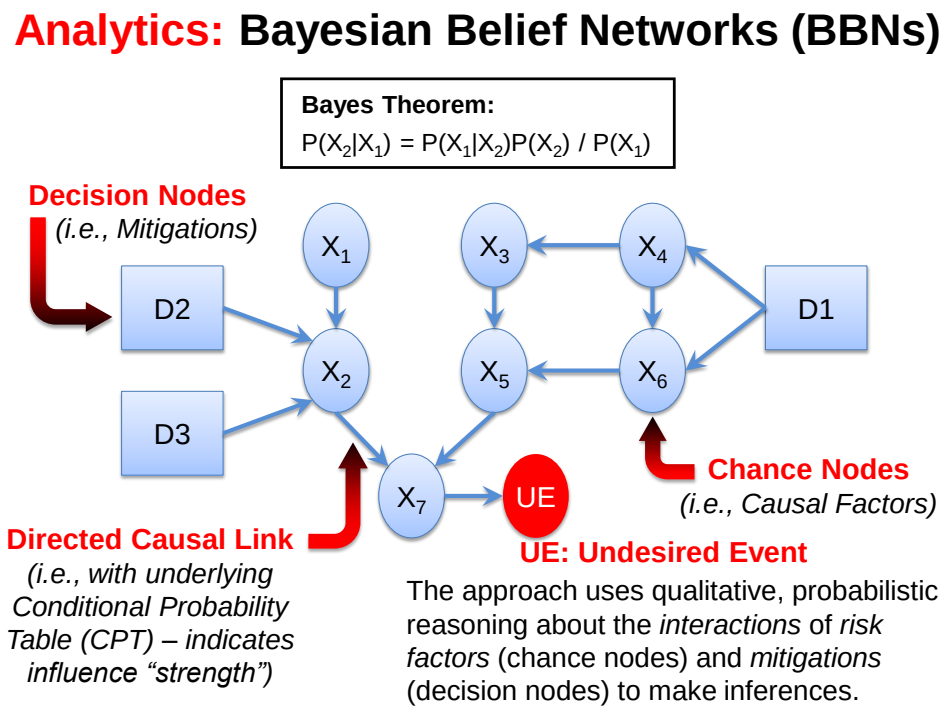

Figure 4. BBN Analytics where UE is the Undesired Event (Source: Luxhøj et al., 2012).

With the BBN approach, the alternative geofencing configurations may be modeled as separate "objects" or sub-nets in a fault tree-type analysis. Once created, these sub-nets are re-usable in other models. The sub-net for the geofencing configuration is then linked to the main model using the instance node capability in the Hugin BBN software (Jensen, 1996). By explicitly labeling the output node in a sub-net (note the interior shading in the output node), this output becomes the input to a top-level model via the use of an "instance node". The instance node provides interfacing functionality. Thus, the prototype demonstrates the features of an Object-Oriented Bayesian Network (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. Hierarchical or OOBNs are further discussed in Fenton and Neil (2013) and Luxhøj (2014b). The geofencing fault tree analyses can then be iteratively linked with the top-level network to comparatively assess the efficacies of the alternative

geofencing configurations on reducing the likelihood of a mid-air collision between the sUAS and the GA aircraft. Probabilities for the components in the geofencing objects or sub-nets mainly come from Reimann (2013). Thus, rather than Boolean geofencing failure in the BBN decision (i.e., mitigation) node as in the previous research by Luxhøj (2015), the alternative configurations allow for degradation in the geofencing failure probabilities.

It is suggested that the safety risk model may also be used to strategically assess alternative "assured containment" concepts as posited by Hayhurst et al. (2015b). An assured containment system as described by Hayhurst et al. (2015b) is a "localization system, independent of the unmanned UA autopilot system, which acts to keep the UA within given bounds" (p. 261). An assured containment system involves more than just hardware and consists of the "hardware, software and operational procedures as well as the evidentiary material (e.g., safety analysis, reliability data, proofs, etc.) that demonstrate the system performs its intended containment function" (Hayhurst et al., 2015b, p. 265). Thus, the proposed system safety modeling approach of the ASRM with its inherent hazard clustering from the HCAS taxonomy is consistent with notion of "hazard partitioning" (Hayhurst et al., 2015b, p. 261) and could be used to support the assessment of an assured containment system. As Hayhurst et al. (2015b) state "In the assured containment concept, flight is confined exclusively within a predefined volume of airspace such that hazards outside of that volume (e.g., related to harming persons or property on the ground and interfering with air traffic) have been partitioned from other hazards inside of the volume" (p. 261). It is suggested that the safety risk model may also be used to strategically assess alternative "assured containment" concepts as posited by Hayhurst et al. (2015b).

Notional Scenario

Wind power in the U.S. is becoming increasingly popular in the United States and abroad (Frangoul, 2015). For example, the Block Island Wind Farm off the coast of Rhode Island will be a 30 megawatt five-turbine facility that will provide the island with most of its power (Frangoul, 2015). However, numerous challenges remain as the environmental conditions may be harsh. The Alaska Village Electric Cooperative has plans to construct a wind turbine farm for St. Mary's and Pitkas Point near the Yukon River in Alaska. The Pilot Station airport is nearby the site of the wind turbine farm. In the proposed notional scenario, suppose that a small fixed wing UAS, such as ScanEagle, is being used in the siting of the wind farm and is taking aerial photography. There are numerous environmental conditions to confront, such as the strong wind gusts, so there are sensors placed on the ground to gather time-dependent wind data, such as wind velocity and turbulence intensity.

It is known that the sensors may be faulty leading to inaccurate measurements. Suppose that a young, low flight hour pilot is aware of the UAS mission and decides to fly his Cessna from the Pilot Station airport to be near the UAS flight operation for observation. A number of scenario assumptions are provided in Figure 8.

To further develop the causal narrative, some "what ifs" are proposed:

- *What if* there are local radio frequencies (RF)/power levels that interfere with the continuous connectivity required of the communication and control links?
- *What if* there is a loss of data link from the Ground Control Station (GCS) to the UAS?
- *What if* the GCS transmission disruption is due to faulty maintenance?
- *What if* there are strong wind gusts and turbulence intensity that contribute to the loss of separation between the UAS and the piloted aircraft?
- *What if* there is a power system malfunction on the piloted aircraft leading to a human factors issue that causes the aircraft not to maintain separation?
- *What if* the waypoints for the ScanEagle are incorrectly programmed?

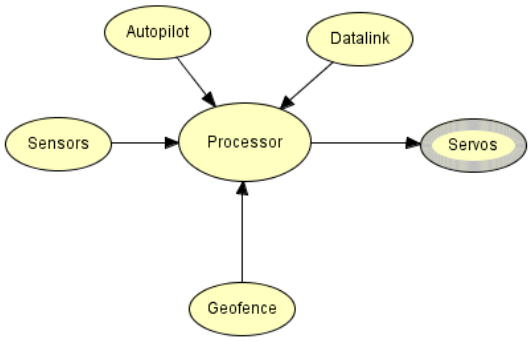

Figure 5. Geofencing with Single Processor (Source: adapted from Atkins, 2014).

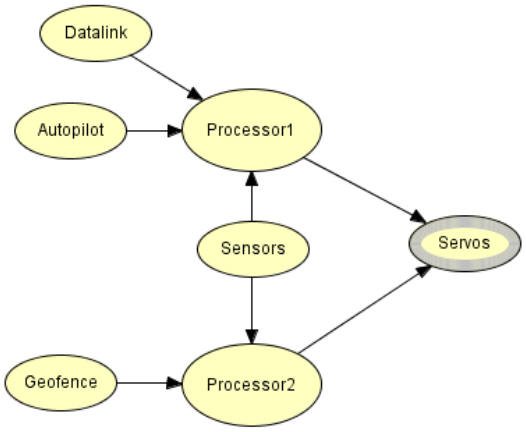

Figure 6. Geofencing with Multiple Processors and Partial Sensor Redundancy (Source: adapted from Atkins, 2014).

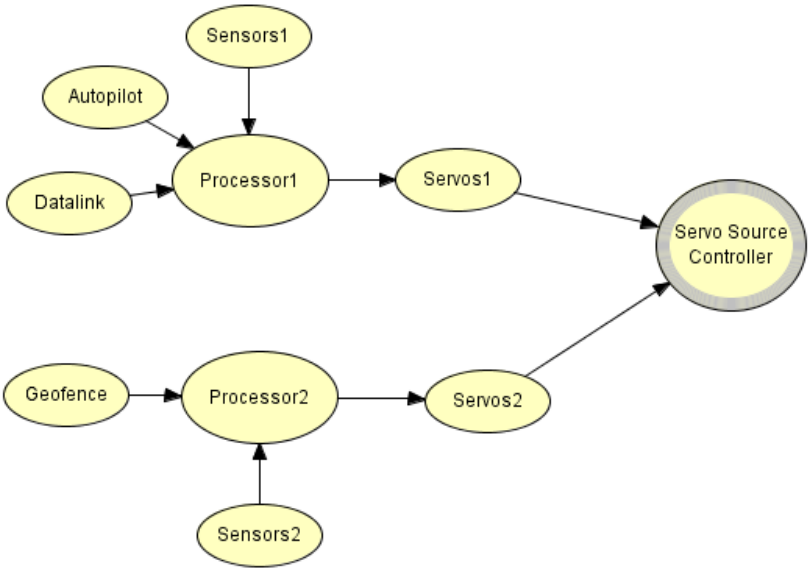

Figure 7. Geofencing with Multiple Processors and Full Sensor Redundancy (Source: adapted from Atkins, 2014).

- Vehicles – UAS - ScanEagle, Gross Takeoff Weight (GTOW) approximately 44 lbs.
  - GA - Cessna
- Who sees what:
  - GA aircraft and UAS vehicle seen by ANSP via ADS-B.
  - GA aircraft and UAS vehicle seen by the UAS pilot (ADS-B reports via net-centric system).
  - GA aircraft sees the UAS vehicle (short range ADS-B on UAS vehicle).
- Sense and avoid:
  - The UAS pilot senses a potential conflict and uses a conflict avoidance processor capable of providing multiple avoidance maneuvers and transmits an avoidance maneuver to the UAS.
  - The GA aircraft pilot can also sense (using ADS-B IN) and avoid the UAS vehicle.
- Avionics:
  - Manned aircraft –
    - ADS-B IN and OUT.
    - VHF communications.
  - UAS
    - Low power ADS-B OUT.
    - Communications link with the UAS pilot that allows the UAS pilot to "fly" the UAS vehicle.
    - A system that senses loss of pilot control and allows the UAS to go to pre-programmed waypoint (typically back toward the launch waypoint).
    - The UAS vehicle ADS-B signal includes a code that will indicate that it is no longer controlled by the UAS pilot.

Figure 8. Notional Scenario Assumptions.

While the sUAS scenario in this study is notional, the BBN approach was used in a previous system safety study for analyzing causal factors contributing to Loss of Control (LOC) accidents for commercial aircraft. For the Loss of Control Accident Framework (LOCAF) BBN study, following the calibration/adjustment of the raw data supplied by the experts, Ancel et al. (2014) report that the LOCAF model was compared with the results obtained from two different datasets. The first dataset used to compare the LOCAF baseline results was the original 54 accident cases which were used to develop the LOCAF model. This dataset depicts that System Component Failure (SCF) occurred in 50% of the accidents (27 SCF cases) and environmental-related causes were present in 31.5% of accidents (17 cases). Following the insertion of these values at the top-level LOCAF BBN, the model indicated 15.92% LOC probability versus 13.81% historical LOC (2.11% higher). A similar effort was performed to replicate the LOC probabilities in the dataset given in Evans (2007). This dataset indicated that within all commercial aircraft (i.e., parts 121/135) accidents (total of 1962 cases, from 1988 to 2004), SCFs were encountered in 20.8% of the cases and environmental factors were present in 14.37% of the accidents. These values were manually inputted to the LOCAF model and the LOC probability was calculated as 10.11%, where the dataset indicates a historical 12.84% LOC occurrence (2.73% lower) (Ancel & Shih, 2012).

Safety Risk Model

The Hugin BBN software (Jensen, 1996) is used to construct the model and to perform all probability calculations based on the Lauritzen-Spiegelhalter (1988) algorithm that is embedded in the software. The topology or structure of the BBN shown in Figure 9 is characterized by 31 nodes with 264 CPT values. The CPT values are generated from combinations of using modeling segments or causal factor sub-nets from other similar BBN models based on knowledge engineering sessions with Subject Matter Experts (SMEs) (Luxhøj 2013, 2014a,b; Luxhøj et al, 2014) that are proportionately scaled for the specific scenario under study. It should be noted that each causal factor or "node" in Figure 9 has the binary states of "present" or "absent" with their corresponding probabilities in the CPTs. The "weighting factors" for each of the nodes is based on the Bayesian probability computations as determined by the embedded Lauritzen-Spiegelhalter algorithm (1988). For example, for the node "Degraded Operating Environment", the computed baseline unmitigated probability is 0.10. The key unmitigated nodal probabilities for this geofencing study are shown in Table 1. For purposes of this model, the Collision Volume is defined as 5 nmi horizontal distance and 1,000 ft. vertical distance, a Loss of Separation (LoS) as when two aircraft are in the collision volume at the same time, a Near Mid Air Collision (NMAC) as when two aircraft

come closer than 500 ft. horizontally and 100 ft. vertically, and a Mid Air Collision (MAC) as when two aircraft are at the same location at the same time.

Results

Baselining the Safety Risk Model

Once the BBN is constructed and the CPTs populated, the model is executed using the Lauritizen-Spiegelhalter (1988) algorithm that is embedded in the Hugin software (Jensen, 1996). The unmitigated baseline probabilities are provided in Table 1. The mitigated probabilities for the three alternative geofencing configurations are provided in Table 2. Note that while there is a marginal gain or improvement with the full redundancy option, there would be an additional cost for such a configuration. The marginal benefit may not exceed the marginal cost in this case. Option 2 with partial redundancy for the sensors appears to be the most promising of the three geofencing configurations that are evaluated.

Table 1. Baseline Safety Risk Values without Geofencing Mitigation.

	Unmitigated baseline probability
P(Mid-Air Collision, MAC)	0.00007
P(Loss of Separation, LoS)	0.00345
P(Separation Assurance Function on the ScanEagle Fails)	0.01
P(ScanEagle Leaves Area of Operations)	0.039

Table 2. Safety Risk Values for Modeling Segment with Alternative Geofencing Mitigations.

	Geofencing Failure Probabilty	P(Separation Assurance Function on the ScanEagle Fails)	P(LoS)	P(MAC)
Single Processor (SP)	0.0075	0.005 (-50%)	0.00326 (-5.5%)	0.000065 (-7.1%)
Multiple Processors – Partial Redundancy (MP-P)	0.0066	0.00452 (-54.8%)	0.003246 (-5.9%)	0.00006491 (-7.3%)
Multiple Processors – Full Redundancy (MP-F)	0.0014	0.004468 (-55.3%)	0.003243 (-6.0%)	0.00006487 (-7.43%)

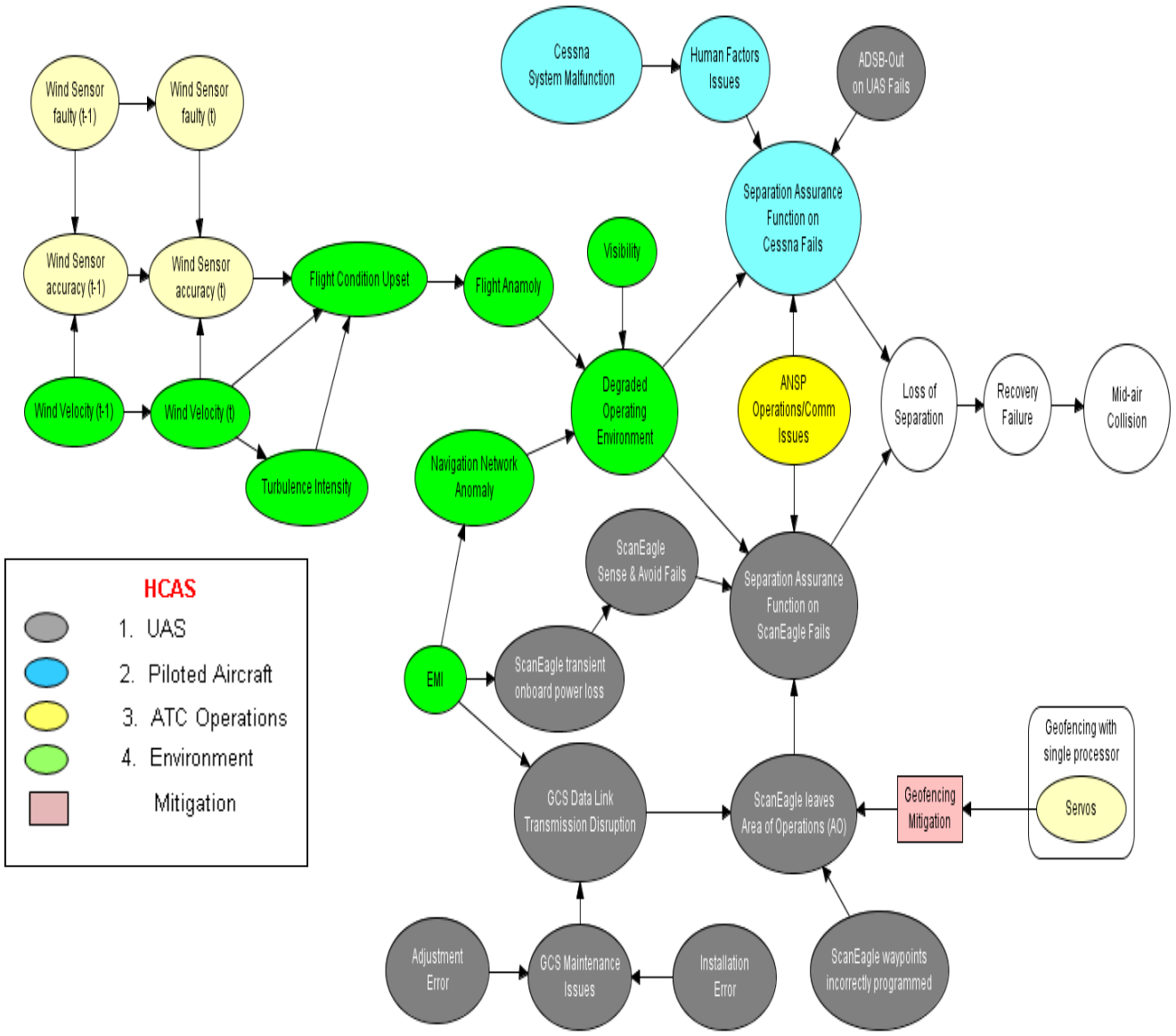

Figure 9. BBN shown with the Single Processor Geofencing Mitigation.

The Logic Risk Ratio (LRR) is a metric that is used in the MIT Lincoln Labs study of the Terrain Collision Avoidance System (TCAS) and also in EuroControl studies of the international version of TCAS – the Airborne Collision Avoidance System (ACAS) (Arino et al., 2002; Kuchar et al., 2007). The Logic Risk Ratio is computed as follows:

$$\text{Logic Risk Ratio (LRR)} = \frac{\text{P (with Mitigations)}}{\text{P (without Mitigations)}} .$$

The risk ratio is not an absolute measure but can be used in a relative way to assess the efficacy of mitigations. A risk ratio of 0.10 means that that risk is reduced to 10% of that which existed if no mitigations were inserted (or in other words, there was a 90% reduction in risk due to the mitigation). The lower the risk ratio, the more the risk is reduced. The LRRs are assumed to be 0.1, 0.01, and 0.001, respectively, for the mitigation effect of the geofencing on the node "ScanEagle Leaves Area of Operations" for the SP, MP-P, and MP-F configurations, respectively. The LRRs in these mitigation cases are based on qualitative reasoning of the effect of the technical improvement in the geofencing configuration upon reducing the likelihoods in the CPT for the "ScanEagle Leaves Area of Operations" node.

Hazard Clusters

The ASRM hazard cluster output is provided in Figure 10. To create this figure, the following process is followed:

- "Evidence" (*e*) is entered into the BBN by removing uncertainty and changing probability of a Causal Factor (CF) to 1.
- Probabilities of *all* causal factors in each respective HCAS Hazard Cluster (HC), i.e. UAS, General Aircraft, Environment, and Operations are changed to 1.
- The Likelihood Multiplier (LM) for a Node =

$$\sum_{HC} P(CF|e) \Big/ \sum_{HC} P($$

for all node precursors. Note that a Likelihood Multiplier (LM) of 1 indicates no impact, and a higher LM indicates a stronger influence of the hazard cluster relative to the baseline probability of the MAC in this case.

The LM is a relative safety metric that is platform/scenario dependent and, as such, it has meaning *within* a scenario to help identify the most promising mitigations.

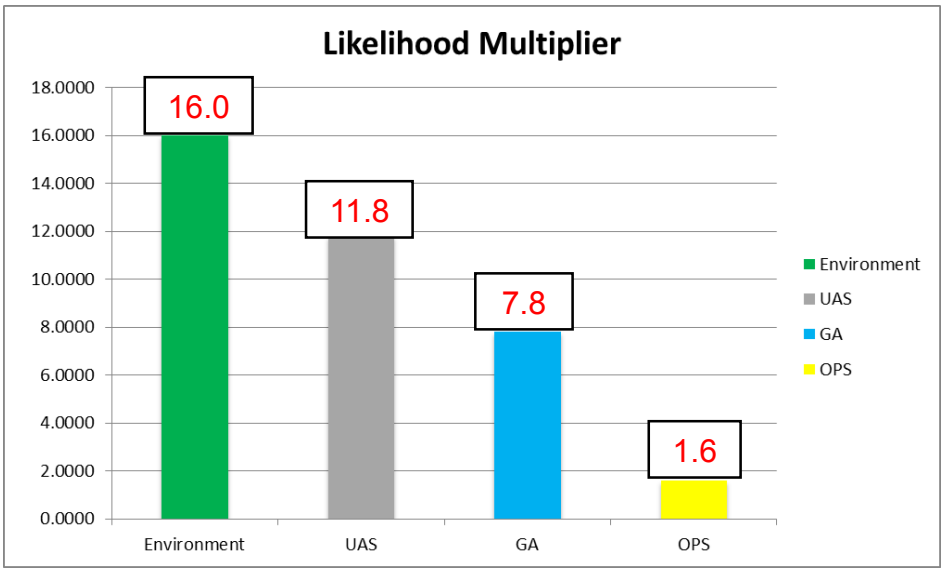

Figure 10. Likelihood Multipliers for the Primary Hazard Clusters Relative to the MAC Baseline, *p*(MAC) = 0.00007.

As expected, the Environment hazard cluster is the most predominant in the notional scenario of a sUAS being used for aerial surveillance in the siting of a wind turbine farm near the Yukon River in Alaska. Should all the Environment-related causal factors be "present" (i.e., their probabilities changed to 1), then it is 16 times more likely that a MAC will occur. The UAS hazard cluster is also significant, thus the interest in evaluating a geofencing mitigation.

Model Calibration

Clignan (2007) reports that the overall ScanEagle accident rate varies from 4.67 accidents / 1,000 FH = 0.00467 accidents/FH to 2.0 accidents / 1,000 FH = 0.002 accidents/FH. However Lum and Waggoner (2011) suggest that these rates are overly pessimistic as they account for more than just crashes, so they suggest 1.0 per 1,000 FH (0.001 accidents/FH) is a more reasonable assumption and use this number in their safety risk model. The accident rate is not the MAC rate. For piloted aircraft, Gambold (2011) reports that 3.6% of the accidents in 2010 were NMACs and MACs. Using this percentage, we obtain the approximation of (0.001)(0.036) = 0.000036 MACs/FH. A recent Academy of Model Aeronautics

(AMA) report of an analysis if FAA drone sightings and encounters contends that the drone-piloted aircraft near miss incident rate is approximately 3.5% (AMA, 2015). Assuming a UAS mission duration of 2 hours, the estimated failure probability is then approximated as (0.000036 MACs/FH)(2.0 hrs.) = 0.000072. From the Hugin BBN, the ASRM unmitigated MAC failure probability is computed as 0.00007. Using the MAC estimate based on the literature calculations, there is an approximately -2.8% difference between the Hugin BBN estimate and the literature estimate. While there are a number of underlying assumptions in the literature estimate, the small difference suggests that a plausible safety risk model has been calibrated for the given scenario.

Conclusions

The integration of sUAS into the NAS offers significant benefits; however, the safety risk needs to be understood and managed. A strength of the ASRM BBN method compared to traditional fault or event trees is that it provides a visual, non-linear systems-level framework for the integration of socio-technical hazards related to the UAS, the piloted aircraft, operations and the environment. The population of the CPTs, however, is challenging given the sparse data for sUAS. However, as experimental operations become more frequent, data from the FAA UAS test sites, for example, offer promise in probability quantification. Geofencing or establishing a "virtual barrier" in the sky, offers one mitigation strategy in the avoidance of mid-air collisions. As is demonstrated, the ASRM may be used to evaluate the efficacy of alternative geofencing configurations using a socio-technical systems perspective that probes interaction effects.

Recommendations for Research

Future research study will focus on identifying the most predominant hazards in each hazard cluster in the notional scenario and demonstrate both forensic and prognostic system safety analyses with the safety risk model. Future research will investigate the use of time-dependent Bayesian modeling to support real-time system safety analyses. For example, the time-dependent causal factors associated with wind velocity need further investigation as to their impact upon the MAC. It may be insightful to decompose the accident rate based on whether the accidents occurred during operator control (mid-flight) or during unaided launch/recovery. Luxhøj & Morton (2011) develop a time-phased BBN that captures UAS phase-of-flight modeling segments with phase-of-flight weights determined by experts that could enhance the current geofencing system safety model. Where possible, more detail will be added to the components in the geofencing configurations. Sensitivity analyses of the CPTs will also be performed. More efficient methods to ease the

CPT elicitation burden with BBNs still need to be developed (Luxhøj et al., 2014). Finally, the use of utility nodes added to the geofencing mitigation will facilitate the inclusion of costs and will support a cost/benefit analysis.

References

Ahmed, A., Kusumo, R., Savci, S., Kayis, B., Zhou, M. & Khoo, Y. (2005). Application of analytical hierarchy process and Bayesian belief networks for risk analysis, *Complexity International*, 12, 1-10.

Ancel, E., Shih, A.T., Jones, S.M., Reveley, M.S., Luxhøj, J.T. & Evans, J.K. (2014). Predictive safety analytics: Inferring aviation accident shaping factors and causation, *Journal of Risk Research*, 18, 428-451, doi: 10.1080/13669877.2014.896402.

Ancel, E. & Shih, A.T. (2012). The analysis of the contribution of human factors to the in-flight loss of control accidents. *12th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference*, Indianapolis, IN.

Ang, M.L., & Buttery, N.E. (1997). An approach to the application of subjective probabilities in level 2 PSAs. *Reliability Engineering and System Safety*, *58*, 145-156.

Academy of Model Aeronautics (AMA, 2015*). A closer look at the FAA's drone data*. Retrieved from http://www.modelaircraft/gov/docs/AMAAnalysis-Closer-Look-at-FAA-Drone-Data_091415.pdf.

Arino, T., Carpenter, K., Chabert, S., Hutchinson, H., Miquwl, T., Raynaud, B., Rigotti, K., & Vallauri, E. (2002). *WP 1: Studies on the safety of ACAS II in Europe*, ver. 1.3, March.

Atkins, E.M. (2014). Autonomy as an enabler of economically-viable, beyond-line-of-sight, low-altitude UAS application with acceptable risk. *AUVSI Unmanned Systems*, Orlando, FL, 200-211.

Badura, H. (2004). Mitigating GPS vulnerabilities, *COTS Journal*, *October*. Retrieved from http://www.cotsjournalonline.com/articles/view/100205

Blom, H.A.P., Stroeve, S.H., Everdig, M.H.C., & van der Park, M.N.J. (2002). Human cognition performance model based evaluation of safe spacing in air traffic, *ICAS Congress*, Toronto, Canada.

Clingan, B. (2007). *FY 2008 Navy UAS, UCAS and EPX programs.* Statement before the Tactical Air and Land Forces Subcommittee.

Dalamagkidis, K., Valvanis, K.P., & Piegl, L.A. (2008). On Unmanned Aircraft Systems issues, challenges and operational restrictions preventing integration into the National Airspace System. *Progress in Aerospace Sciences*, *55*, 503-519.

Ericson II, C.A. (2005). *Hazard analysis techniques for system safety.* Hoboken, NJ: Wiley-Interscience.

Evans, J.K. (2007). *An application of CICTT accident categories to aviation accidents in 1988-2004, NASA/CR-2007-214888.* Hampton, VA: NASA.

Fenton, N., & Martin, N. (2013). *Risk assessment and decision analysis with Bayesian networks*. Boca Raton, FL: CRC Press.

Frangoul, A. (2015). *Is this the greatest untapped resource in the US?* Retrieved from http://www.msn.com/en-us/money

Gambold, K. (2011). *Unmanned Aircraft System access to national airspace,* Background Paper [unpublished].

Global Positioning System (GPS) (2008). *Standard positioning service performance standard*, 4th ed. Washington, D.C.: Department of Defense.

Global Positioning System Wide Area Augmentation System (WAAS) (2008). *Performance standard.* Washington, D.C: Department of Transportation.

Griffin, T., Young, M, & Stanton, N. (2015). *Human factors models for aviation accident analysis and prevention*. Oxon, UK: Ashgate.

Ha, J. and Seong, P (2004). A method for risk-informed safety significance categorization using the analytic hierarchy process and Bayesian belief networks, *Reliability Engineering and System Safety, 83,* 1-15, doi:10.1016/j.ress.2003.08.002.

Harkleroad, E., Vela, A., Kuchar, J., Barnett, B., & Merchant-Bennett, B. (2013). *Risk-based modeling to support NextGen concept assessment and validation, Project Report ATC-405*. Lexington, MA: MIT Lincoln Laboratory.

Hammer, W. (1972). *Handbook of system and product safety*. Englewood Cliffs, NJ.: Prentice-Hall.

Hayhurst, K.J., Maddalon, J.M., Neogi, N.A., Verstynen, H.A., Buelow, B., & McCormick, G.F. (2015a). *Mock certification basis for an unmanned rotorcraft for precision agricultural spraying, NASA/TM-2015-218070*. Langley, VA: NASA Langley Research Center.

Hayhurst, K.J., Maddalon, J.M., Neogi, N.A., & Verstynen, H.A. (2015b). A case study for assured containment, *International Conference on Unmanned Aircraft Systems* (ICUAS), Denver Marriott Tech Center, Denver, CO, 260-268.

How, J.P., Fraser, C., Kulling, K.C., Bertuccelli, L.F., Toupet, O., Brunet, L., Bachrach, A., & Roy, N. (2009). Increasing autonomy of UAVs. *Robotics & Automation Magazine, IEEE 16*(2), 43-51.

Jensen, F.V. (1996). *Introduction to Bayesian networks*. New York: Springer Verlag.

Kuchar, J., & Drumm, A. (2007). The Traffic Alert and Collision Avoidance System. *Lincoln Laboratory Journal*, *16*(7), 277-296.

Lauritzen, S.L, & Spiegelhalter, D.J. (1988). Local computations with probabilities on graphical structures and their applications to expert systems. *Journal of the Royal Statistical Society, Series B (Methodological)*, *50*(2), 157-224.

Leveson, N.G. (2004). A new accident model for engineering safer systems. *Safety Science, 42***,** 237-270.

Leveson, N.G., Dulac, N., Zipkin, D., Cutcher-Gershenfeld, J., Carroll,J., & Barrett, B. (2006). Engineering resilience into safety-critical systems. In E. Hollnagel, D. D. Woods, & N. G. Leveson (Eds.), *Resilience Engineering* (95-123). Oxon, UK: Ashgate Publishing.

Leveson, N. (2011). *Engineering a safer world: Systems thinking applied to safety*. Cambridge, MA: MIT Press.

Lum, C. and B. Waggoner (2011). A risk based paradigm and model for Unmanned Aerial Systems in the national airspace. *Infotech@Aerospace 2011 AIAA.* St. Louis, Missouri.

Luxhøj, J.T. (2003). 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.

Luxhøj, J.T. (2013). Predictive analytics for modeling UAS safety risk. *SAE International Journal of Aerospace*, *6*(1), 128-138.

Luxhøj, J.T (2014a). Probabilistic safety analytics for UAS integrated risk modeling [Powerpoint Slides]. Retrieved from file:///C:/Users/William/Downloads/Jim_Luxhoj_%20Mid Atlantic%20Symposium%20Presentation-v2.0.pdf .

Luxhøj, J.T. (2014b). An Object-Oriented Bayesian Network (OOBN) for modeling aircraft carrier- based UAS safety risk. *Journal of Risk Research*, *18*(10), 1230-1258 doi: http://dx.doi.org/ 10.1080/13669877.2014.913664.

Luxhøj, J.T. (2015). A socio-technical model for analyzing safety risk of Unmanned Aircraft Systems (UAS): An application to precision agriculture. *1st International Conference on Human Factors and Unmanned Systems.* Las Vegas, NV.

Luxhøj, J.T. & Öztekin, A. (2009). A regulatory-based approach to safety analysis of Unmanned Aircraft Systems. *HCI 2009: 13th International Conference on Human-Computer Interaction*, San Diego, CA.

Luxhøj, J.T. & Morton, M. (2011). Probabilistic safety risk analysis in complex domains: Application to Unmanned Aircraft Systems. *11th AIAA Aviation Technology, Integration, and Operations (ATIO) Conference*, Virginia Beach, VA.

Luxhøj, J.T., Shih, A.T., Ancel, E., Jones, S.M., & Reveley, M.S. (2012). Safety risk knowledge elicitation in support of aeronautical R&D portfolio management: A case study. *Proceedings of the International Conference of the American Society for Engineering Management*, Hilton Virginia Beach Oceanfront, Virginia Beach, VA.

Luxhøj, J.T., Ancel, E., Green, L.L., Shih, A.T., Jones, S.M. & Reveley, M.S. (2014). Lessons learned from multiple knowledge elicitation sessions. *32nd International System Safety Conference*, St. Louis, MO.

McKinlay, A. (2014). Safety, autonomy, latency, and the Unmanned or Remotely Piloted Vehicle. *32nd International System Safety Conference*, St. Louis, MO.

NASA Tech Briefs (2016). Drone control: Flying the crowded skies. *Tech Briefs*, *40*(2), 12-17.

National Research Council (2014). *Autonomy research for civil aviation: Toward a new era of flight.* Washington, DC: The National Academies Press.

Netjasov, F., & Janic, M. (2008). A review of the research on risk and safety modelling in civil aviation. *3rd International Conference on Research in Air Transportation*, Fairfax VA, 169-176.

Park, S., Yang, H., Heo, G., Zubair, & Ur, R. (2014). Study on nuclear accident precursors using AHP and BBN, *Science and Technology of Nuclear Installations*. doi: 10.1155/2014/206258.

Raheja, D.G. and Allocco, M. (2006). *Assurance technologies principles and practices: A product, process, and system safety perspective,* 2nd ed. Hoboken, NJ: Wiley-Interscience.

Reimann, S., Amos, J., Bergquist, E., Cole, J., Phillips, J., & Shuster,S. (2013). *UAV for reliability, University of Minnesota, AEM 4331-Aerospace Vehicle Design*. Retrieved from http://www.aem.umn.edu

Wagner, B. (2008), Worries about mid-air collisions keep civilian drones grounded. *National Defense Magazine*. Retrieved from http://www.nationaldefensemagazine.org

Wallace, R., & Loffi, J. (2015). Examining Unmanned Aerial System threats & defenses: A conceptual analysis, *International Journal of Aviation, Aeronautics, and Aerospace*, *2*(4), 1-33.