Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 20 (2013) 331 – 336
Procedia Computer Science

Complex Adaptive Systems, Publication 3
Cihan H. Dagli, Editor in Chief
Conference Organized by Missouri University of Science and Technology
2013- Baltimore, MD

Predictive Safety Analytics for Complex Aerospace Systems

James T. Luxhøj, Ph.D.*

LCR, 40 MacAfee Road, Somerset, NJ 08873 USA

Abstract

The complexity of the National Airspace System (NAS) in the United States presents a number of novel and unique challenges for the integration of Unmanned Aircraft Systems (UAS). In particular, one challenging aspect is the modeling of UAS safety risk for civil applications given the scarcity of actual operational data. With the creation of a probabilistic model, inferences about changes to the states of the accident shaping or causal factors can be drawn quantitatively. These predictive safety inferences derive from qualitative reasoning to plausible conclusions based on data, assumptions, and/or premises and enable an analyst to identify the most prominent causal factors leading to a risk factor prioritization. Such an approach also facilitates the study of possible mitigation effects. 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) with the mission of aerial surveying for a bridge infrastructure inspection. As a System of Systems (SoS) approach, an OOBN facilitates decomposition at the sub-system level yet enables synthesis at a higher-order systems level. In essence, the methodology serves as a predictive safety analytics platform to support reasoning to plausible conclusions from assumptions or premises.

Selection and peer-review under responsibility of Missouri University of Science and Technology

Keywords: Object-Oriented Bayesian Networks (OOBNs); Unmanned Aircraft Systems (UAS); safety risk; System of Systems (SoS)

1. Introduction

Due to the novelty of Unmanned Aircraft Systems (UAS) operations 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 diagrams are required to logically understand the impact of the introduction of these operations into the National Airspace System (NAS). While alternative real-time and fast-time simulation modeling research for UAS in the NAS is a significant focus area of the aerospace industry and government agencies, the rigorous development of complementary probabilistic analytical methods and tools needs to similarly advance. This paper presents a *notional* system safety case study inspired from the aerospace literature and 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. The question of system safety associated with the integration of UAS

* Corresponding author. Tel.: (732) 259-9623
E-mail address: jtluxhoj@gmail.com

Selection and peer-review under responsibility of Missouri University of Science and Technology
doi:10.1016/j.procs.2013.09.281

in the NAS 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 [1]. A system safety approach involves an identify-analyze-control method of safety as opposed to a "fly-fix-fly" approach [2]. Hazard identification and analysis is an initial and integral step in any system safety study. A nascent taxonomy, termed the Hazard Analysis and Classification System (HCAS) identifies four main clusters of hazards: *UAS, Airmen, Operations, and Environment* [3].

2. Safety Risk Management

Luxhøj [4] reports on the development of a six-step process for aviation safety risk modeling. The model is termed the Aviation System Risk Model (ASRM) and it can be used to evaluate the causal factors linked to the air vehicle and/or the Next Generation (NextGen) systems and procedures that lead to the unsafe state and the interactions among these factors that contribute to the safety risk. The ASRM uses the flexible, probabilistic approach of Bayesian Belief Networks (BBNs) [5] 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 UAS 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 been adapted for UAS safety risk modeling. 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 departs from traditional approaches. Fig. 1 displays the general structure of a Bayesian Belief Network (BBN) with chance nodes or random 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 are identified and grouped into the hazard "clusters" using the HCAS, then the interactions among the factors as qualitatively discussed in the scenario description are drawn using an influence diagram. Each link in the influence diagram possesses an underlying Conditional Probability Table (CPT) that indicates the "strength" or the degree of belief in the depicted causation. 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 is created.

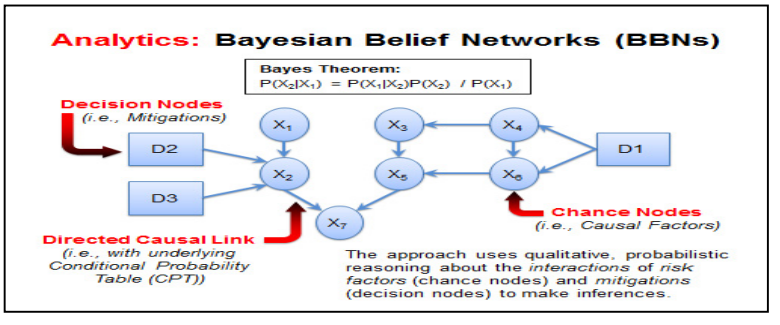

Fig. 1. General structure of a Bayesian Belief Network (BBN). (Source: [6])

The development of the UAS 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*; [5]). By explicitly labeling the output node in a sub-net, this output becomes the input to a "summary model" via the use of the Hugin "instance node". The instance node provides interfacing functionality. Thus, the UAS risk model prototype demonstrates the features of an Object-Oriented Bayesian Network (OOBN). The OOBN approach facilitates decomposition at the sub-system level yet enables synthesis at a higher-order systems level [7]. With its hierarchical structure, the OOBN approach is inherently a System of Systems (SoS) approach [6,7; *http://en.wikipedia.org/wiki/System_of_systems; http://www.odu.edu/ncsose*].

3. UAS Notional Application Scenario

The UAS application scenario is inspired from a technical report by Gebre-Egziabher and Xing [8] from the Intelligent Transportation Systems Institute in the Center of Transportation Studies at the University of Minnesota. Luxhøj [9] provides additional details of the UAS notional application scenario. The Concept of Operations (CONOPS) involves a small UAS (sUAS) (< 55 lbs.) operating close to a bridge that is equipped with a camera capable of capturing video or still images for bridge infrastructure inspection [8]. 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. Gebre-Egziabher [10] provides engineering details for the UAS. 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 is provided in advance that is consistent with the local weather and any 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. The operational plan specifies how close or a "standoff" distance that 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. 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 [8]. Much of the UAS bridge infrastructure inspection scenario corresponds closely with the overall BBN structure of two previously presented hypothetical sUAS scenarios by the author. To extend the sUAS bridge inspection operational scenario, a causal narrative, or "story" could start with some suppositions based on "what if" propositions. The "what ifs" to explore are:

- *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 sUAS?
- *What if* there are strong wind gusts (> 40 knots) suddenly present that contribute to loss of the "standoff" distance between the sUAS and the bridge?

By exploring some possible impacts of the foregoing "what if" propositions, a causal narrative is developed as follows. Suppose that a *hypothesized* sUAS *mishap scenario* derived from the operational scenario involves a loss of command and control or a "lost link" for the sUAS in the scenario that leads to a potential collision with bridge. A "lost link" scenario refers to a lost data link and occurs when the sUAS is no longer receiving command/control data from the ground control station (GCS). Suppose further that the sUAS conflict avoidance subsystem fails at a critical time in this scenario due to an inadvertent shutdown of the sUAS ground control station. There could a number of different causes for the GCS shutdown, but further suppose that electro-magnetic activity of local RF equipment frequencies/power levels in the vicinity of the bridge interfere with the continuous connectivity of the sUAS equipment. These power levels are sufficient to trigger an adverse reaction by critical GCS equipment and lead to a software malfunction of the firmware in the ground control station. The RF interference (usually from non-regulated equipment, such as microwaves, garage door openers, electronic research equipment, etc.) could potentially adversely affect the UAS pilot's communications link. A strong wind gust is present near the bridge that causes the sUAS to deviate from its planned "race track" flight. The system fault of a lost link caused by the inadvertent shutdown of the sUAS ground control station by a software malfunction triggered by electro-magnetic interference (EMI) from local RF equipment frequencies/power levels potentially leads to a loss of control of the

sUAS. It is reasonable to surmise that this system fault of loss of communications between the sUAS pilot and the UAS creates a safety risk. Continuing with the hypothetical sUAS causal narrative, suppose that it was subsequently discovered that during maintenance to the sUAS ground control station, the new version of the firmware was not properly installed by the support personnel and GCS "lockups" were known to occur intermittently in the presence of certain local RF equipment frequencies/power levels leading to GCS shutdown, thus there was a continued airworthiness issue. A lockup is any malfunction that causes the GCS screen to stop updating and to "freeze". Further investigation revealed that the GCS software support personnel were not properly trained in installing the latest version of the software with the proper settings and the installation error led to the inadvertent shutdown of the ground control station, thus leading to the failure of the conflict avoidance system. The next step in the system safety analysis is to delineate the hazards in the causal narrative using the HCAS and to create an influence diagram depicting the interactions of the causal factors deriving from hazards. It is through the Hugin functionality of an "instance node" that multiple sub-nets may be linked [5]. The top-level or "summary model" for the sUAS bridge infrastructure scenario is presented in Fig. 2. Fig. 3 presents the primary sub-net of causal factors associated with the sUAS failure. Note the gray shading in the output node of "UAS flight failure." This indicates that it is an output node linked to the top level model via the instance node in Fig. 2. Fig. 3 also includes two other sub-nets – *Maintenance Preconditions* and *Flight Crew Performance Deficiency*. Additional details and influence diagrams for these sub-nets are provided in Luxhøj et al. [6].

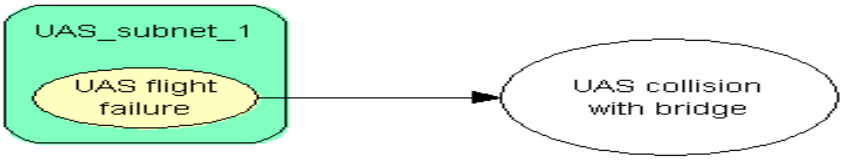

Fig. 2. OOBN top level model for sUAS bridge inspection scenario with sUAS flight failure sub-net. (Source: [9])

For the sUAS collision with the bridge consequence node and UAS flight failure sub-net, engineering flight test data [8] and sUAS accident rate data from the Joint Authorities for Rulemaking on Unmanned System or JARUS [11] are used to populate the CPTs. Based on numerical bounding analyses [8], one second into the upwind leg the P(UAS collision with bridge) is 3 x 10^{-5} and increases to 1 x 10^{-3} four seconds later. At the end of the upwind leg or five seconds later, a collision risk of 2.5 x 10^{-2} is reported [8]. These probabilities are inserted into the CPT for the sUAS collision with the bridge consequence node. The JARUS report noted a sUAS equivalent accident rate of 1 x 10^{-4} so this rate is used to benchmark the probability of a sUAS flight failure conditioned on the premise that the "sUAS pilot fails to regain control of the UAS due to signal latency" is non-conducive to the sUAS flight failure.

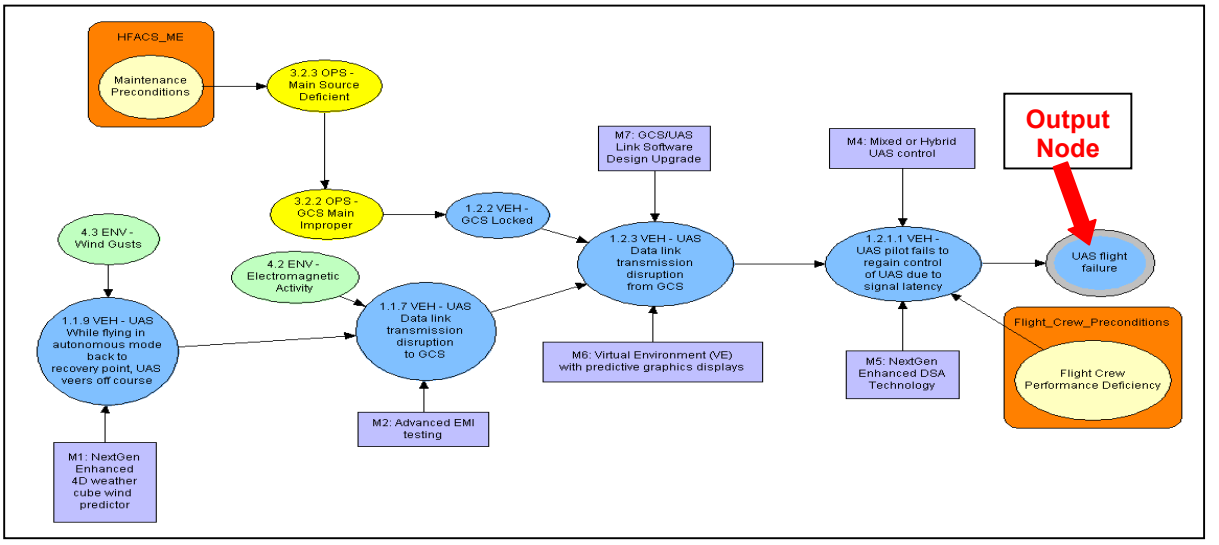

Fig. 3. sUAS flight failure sub-net with flight crew performance deficiency and maintenance preconditions sub-nets. (Source: [9])

The Hugin Expert BBN software tool [5] with its embedded Bayesian propagation and inferencing algorithms is used to construct and analyze the model. With the creation of a probabilistic model, inferences about changes to the states of the mishap shaping or causal factor clusters 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 leading to a prioritization. Luxhøj [9] explores the analytical impact of the sub-nets on the overall risk assessment. The inclusion of the sub-nets leads to an approximate 55% reduction in the *P*(UAS flight failure) and an approximate 26% reduction in the *P*(UAS collision with bridge). Intuitively, it is reasoned that the inclusion of the refined probabilities for human variability on maintenance and flight crew performance leads to more refined safety risk estimates for these sub-nets and improves the level of granularity in the integrated risk model. However, the safety risk is reapportioned between the hazard causal factor clusters. In this paper, we further analyze the *relative ranking* of the risk factors for the UAS bridge infrastructure inspection scenario using the Hugin BBN software. Fig. 4 displays the relative ranking of the casual factors *inclusive* to the *Flight Crew Performance Deficiency* sub-net. For example, the interpretation is that if there is evidence to suggest that Personal Readiness is deficient (i.e., the probability of this causal factor changes to 1.0), then the likelihood of Flight Crew Performance Deficiency is increased by a factor of 1.97 or approximately 2.0. The next most influential casual factors contributing to Flight Crew Performance Deficiency are CRM and Inappropriate Operations. Similar results are obtained for the *Maintenance Preconditions* sub-net. Space limitations preclude the elaboration of the mathematical details of the Hugin BBN algorithm for the sUAS bridge inspection scenario in this paper; however, Jensen [5] provides a full treatment of the algorithm.

Fig. 5 displays the relative risk prioritization for the *P*(UAS flight failure). Note that in this case, the risk factor of "Pilot fails to regain control of the UAS due to signal latency" dominates the other risk factors. If there is evidence to suggest that this risk factor is present (i.e., the probability changes to 1.0), the likelihood of an UAS flight failure increases by a factor or multiplier of approximately 20.6. The next two most influential risk factors that contribute to the UAS flight failure in this scenario are the "Data link transmission disruption to the Ground Control Station (GCS)" and the "GCS locked". A similar analysis was performed for the *P*(UAS collision with bridge).

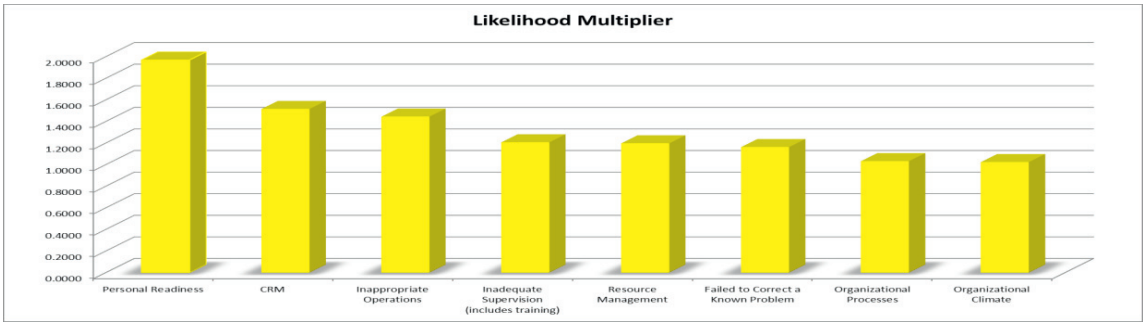

Fig. 4. Baseline *P*(flight crew performance deficiency) = 0.3906.

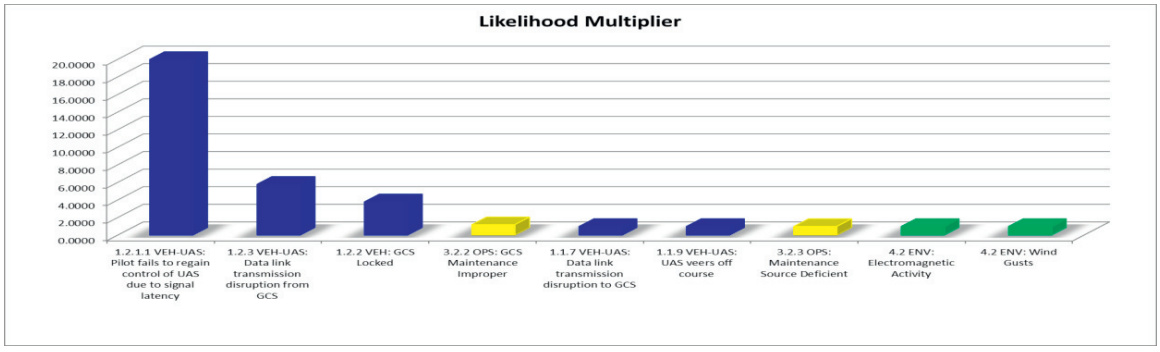

Fig. 5. Baseline *P*(UAS flight failure = 4.9×10^{-4}).

Finally, if we are interested in ascertaining the most influential grouping of risk factors or hazard clusters for the bridge infrastructure inspection collision scenario we obtain the results in Fig 6. To obtain these results, the probabilities of all risk factors in that grouping are changed to 1.0 and the likelihood impact on the *P*(UAS collision with bridge) computed. Note that the risk factors associated with the Vehicle or UAS hazard cluster dominate the other two hazard clusters. Such an analysis suggests the next step – the development and impact assessment of potential mitigations.

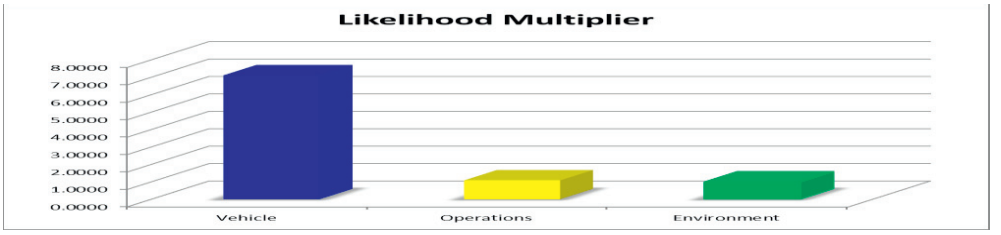

Fig. 6. Rank ordering of hazard clusters: Baseline *P*(UAS collision with bridge = 4.2 x 10^{-5}).

4. Conclusions

With the creation of a probabilistic safety risk model, inferences about changes to the states of the causal factors or the presence or absence of mitigations can be made. These inferences may be built on either quantitative or qualitative reasoning, or both, and enable an analyst to identify the most prominent causal factor groupings (i.e., Vehicle or UAS, Operations, Environment or Human) leading to a prioritization of the most influential causal factors. A systematic approach to risk factor sensitivity may lead to vulnerability discovery of emerging hazard causal factors for which mitigations do not yet exist that then informs possible future R&D efforts.

Acknowledgements

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.

References

1. Federal Aviation Administration, Unmanned Aircraft System Operations in the U.S. National Airspace System – Interim Operational Approval Guidance, AFS-400 UAS Policy 05-01, September 16, 2005.
2. H. Roland and B. Moriarty, System Safety Engineering and Management, 2nd ed., John Wiley & Sons, Inc., New York, 1990.
3. J. Luxhøj and A. Öztekin, A Regulatory-Based Approach to Safety Analysis of Unmanned Aircraft Systems, HCI 2009: 13th International Conference on Human-Computer Interaction, San Diego, CA, July 19-24, 2009.
4. J. Luxhøj, 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), 17-38, Williamsburg, VA, September 16-19, 2003.
5. F. Jensen, Introduction to Bayesian Networks, Springer Verlag, New York, 1996.
6. J. Luxhøj, A. Shih, E. Ancel, S. Jones, and M. Reveley, 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, October 17-20, 2012.
7. W. Philippe and J. Lionel, Complex System Reliability Modelling with Dynamic Object-Oriented Bayesian Networks (DOOBN), Reliability Engineering and System Safety, 9(2):149-162, 2006.
8. D. Gebre-Egziabher and Z. Xing, Analysis of Unmanned Aerial Vehicles: Concept of Operations in ITS Applications, Intelligent Transportation Systems Institute, Center for Transportation Studies, University of Minnesota, Report No. CTS 11-06, March 2011.
9. J. Luxhøj, Predictive Analytics for Modeling UAS Safety Risk, SAE 2013 AeroTech Congress & Exhibition, Palais des Congress de Montreal, Canada, September 24-26, 2013 (to appear).
10. D. Gebre-Egziabher, RPV/UAV Surveillance for Transportation Management and Security, Intelligent Transportation Systems Institute, Center for Transportation Studies, University of Minnesota, Report No. CTS 08-27, December 2008.
11. N. Brewer, Working Group 6 (System Safety): AMC UAS.1309 Development – Brief to Industry, Joint Authorities for Rulemaking on Unmanned Systems (JARUS), Brussels, December 6, 2012.