Towards Formalization of a Data Model for Operational Risk Assessment

Vidhya Tekken Valapil
GE Research
Niskayuna, NY, USA
vidhya.valapil@ge.com

Heber Herencia-Zapana
GE Research
Niskayuna, NY, USA
heber.herencia-zapana@ge.com

Michael Durling
GE Research
Niskayuna, NY, USA
durling@ge.com

Kristen Armstrong
GE Aviation
Grand Rapids, MI, USA
KristenM.Armstrong@ge.com

Saswata Paul
GE Research
Niskayuna, NY, USA
saswata.paul@ge.com

Szabolcs Borgyos
GE Research
Niskayuna, NY, USA
szabolcs.borgyos@ge.com

Abha Moitra
GE Research
Niskayuna, NY, USA
moitraa@ge.com

William Premerlani
Niskayuna, NY, USA
wjpremerlani@gmail.com

***Abstract*—Operational Risk Assessment (ORA) is a process used to demonstrate and verify that the resultant risk of a planned operation meets certain required safety standards. Subject matter experts (SME) from different domains often use different approaches and terminologies to design ORAs. This leads to long review cycles and creates potential for inconsistent understanding of risks and/or application of mitigations by different practitioners across the safety-risk-chain. In this paper, to formalize ORA data representation we propose a set of common terminologies to be used while capturing ORA data. The proposed terminologies trace to existing standards and to terminologies used in risk data visualization methodologies. We also present a formal data model for ORA, that uses the proposed terminologies, in SADL (Semantic Application Design Language), thereby allowing SMEs to capture their knowledge as formal artifacts that are amenable to machine manipulation and automation. Furthermore, since ORA data is often captured in an excel format, we illustrate the use of an excel template that uses the proposed terminologies, by capturing assessment data corresponding to an example use case scenario in the template. Finally, to enable visualization of the ORA data, we discuss representing them as Bowtie diagrams. A Bowtie diagram is a pictorial representation that captures the relationship between a hazard, its causes and its consequences in a given specific environment or system state. To enable the benefits of Bowtie representation we map the proposed ORA terminologies to elements in a Bowtie model. We illustrate visualization of the ORA data as a Bowtie diagram by generating a Bowtie diagram capturing the ORA data corresponding to the example use case scenario considered in the paper.**

Keywords— operational risk assessment, Bowtie diagrams, data modelling

I. INTRODUCTION

The Part 107 waiver allows drone pilots to deviate from certain rules under part 107 by demonstrating that they can still fly safely using alternative methods. The waiver application consists of CONOPS and ORA. The proposed CONOPS (Concept of Operations), that typically includes description of the system, its intended use, proposed area of operations and intended classes of airspace, is analyzed during the Operation Risk Assessment process to ensure that there are sufficient mitigations in place to conduct desired operations within an acceptable level of risk. [1] Specifically, ORA involves identification of hazards associated with each operation or function of the system and identification of corresponding mitigations like operational limitations in place to mitigate each hazard. Traditionally ORA data is captured and analyzed manually using excel spreadsheet or other textual documents. Visualizing the ORA data diagramatically can help provide insight into the risk management effort taken like operational or design mitigations used at different functional granularity. For example, bow-tie diagrams are one of the most commonly used visual representation of hazards and mitigations.

A Bow-tie model or diagram captures the relationship between a hazard, its causes and its consequence in a given specific environment or system state in a pictorial format. In Federal Aviation Administration's Safety Risk Management Guidance manual [2], a Bowtie- model is defined as a structured illustration of the relationship between causes, hazards, and kind of environment (system state) that enables their propagation into different outcomes or effects. Furthermore, Bowtie diagrams can also be used to capture any mitigations or controls used in the system to prevent hazards or recover from them. Bowtie models are used in safety assessment by aviation regulators like Civil Aviation Authority. Aside from aviation [3] [4], Bowtie diagrams are used in several other industries [5] like oil and gas, chemical, defense, banking, healthcare, marine, mining, nuclear energy and so on.

In [5], Bowtie diagrams are used for risk analysis of visual borescope inspection during aircraft engine maintenance. In the context of inspection, some of the benefits of using the Bowtie representation identified in [5] were helping inspectors understand the risks, understand specific mitigations or controls that are in place to prevent or minimize the risks and why it is important to maintain them. Representing the Operational Risk Assessment data as Bowtie diagrams can have similar benefits in the context of certification, where the reviewer can easily identify mitigations used to alleviate effect of specific hazards. However, the challenge in representing the information captured during ORA as bow-tie diagrams is that there are discrepancies in terminologies used in the context of Risk Assessment and bow-tie methodology. To bridge this gap, in this paper, we propose a set of normalized terms that we will use to capture the ORA data. We define each of these terms and identify elements that they correspond in a bow-tie model.

In this paper, to aid analysis and visualization of the ORA data, we also propose a data model to formally capture the assessment information. Capturing the assessment data in a formally defined data model enables easy querying of the data to suit the needs of the target audience, thereby enabling effective visualization of specific aspects of the assessment data.

II. Preliminaries

In this section, we provide some background on operational risk assessment and Bowtie methodology. Since terminology used in the context of operation risk assessment differ from terminology used in the Bowtie methodology, we propose a set of normalized terms that the safety engineers can use to define their ORA template. Furthermore, to aid creation of Bowtie diagrams corresponding to the ORA data, for each of the normalized terms, we identify corresponding elements in the Bowtie model in Table 1.

A. Operational Risk Assessment

The operational risk assessment (ORA) is an iterative analysis that identifies hazards, effects, likelihoods and mitigations pertaining to the vehicle, avionics, remote control, ground station, and environment. To understand various aspects of operational risk assessment, we will consider ORA in the context of Unmanned Aviation Systems (UAS). The identified hazards inherent to the UAS system of systems will be specific to the type of equipment being used, area of operations, and type of operation. This type of assessment provides a methodical, repeatable process, to make sure there is sufficient potential hazard coverage. The severity of the hazard is determined by the effects in accordance with predefined safety criteria, the effects of which are dependent upon the vehicle, location and type of operation.

The likelihood of each of the hazards will be determined following the probabilities of occurrence. Typically, the probabilities that are used for quantitative analysis are based upon at least several thousands of flight hours achieved through airplane fleets. For UAS, this is not possible. Rather than assigning a probability to equipment failure, we are using operational mitigations in place for risk control.

The residual risk score is calculated by multiplying the severity and likelihood. Mitigations for each hazard are documented as well. These may be incorporated into the UAS equipment design, flight operation procedures, or the restrictions on the operational environment. These reduce the likelihood or eliminate the hazard. For example, for the hazard of failure to retain one or more propellers during takeoff or landing, this hazard can be mitigated by keeping all crew behind a flight line that is further than a propeller could be thrown. By using this mitigation, the risk is controlled by ensuring that no people can be hurt by a thrown propeller, not by reducing the probability of throwing the propeller. These types of mitigations allow us to control the risk in situations where the probability is not typically understood. The ORA activity meets the intent of both the FHA (Functional Hazard Assessment) and the PSSA (Preliminary System Safety Assessment) process, while also meeting the needs of the work scope.

In accordance with ASTM F3178, the ORA is used to establish the residual risk associated with the system of systems. Residual Risk is dependent upon hazard severity and likelihood severity classification. Mitigations can be used to reduce the likelihood of a hazard and are used to drive design and procedural requirements. In the context of UAS, when the ORA data is captured in an excel spreadsheet format, the following column headers are used,

ID: unique identifier for each individual functional failure/hazard.

Phase of Flight: operational phases of the mission.

Hazard: a potentially unsafe condition resulting from failures, malfunctions, external events, errors, or combinations thereof and this term is intended for single malfunctions or loss of function that are considered foreseeable based on either past service experience or analysis with similar components in comparable manned aircraft applications or both. [6]

Effect: the description of the potential result of a failure. [7]

Severity: consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm. [6]

Components Involved: the subsystem/components that contribute to the functional failure.

Notes: any comments or remarks.

Unmitigated Likelihood: the estimated probability or frequency, in quantitative and qualitative terms, of a hazard's effect or outcome [6].

Unmitigated Risk Score: composite of predicted severity and likelihood of the potential effect of hazards [6].

Considerations and Mitigations: the features of the system and/or con-ops as well as the operational actions of the flight crew that reduce the likelihood of failure effects .

Mitigated Likelihood: the estimated probability or frequency, in quantitative and qualitative terms, of a hazard's effect or outcome once the considerations and mitigations are taken into account [6].

Residual Risk Score: composite of predicted severity and mitigated likelihood of the potential effect of hazards [6].

*Residual Risk Acceptable?:*whether or not the residual risk meets the team's objective.

B. Bowtie Methodology

Effective visualization of safety and risk aspects of safety critical systems and their operation can help increase stakeholder's trust in them. For instance, visualizing safety assurance cases [8] graphically [9] can help convey and justify safety claims about the system based on evidence. From the risk perspective, the Bowtie method can be used to analyze and communicate how high-risk scenarios develop. The Bowtie consists of plausible risk scenarios around certain hazard, and ways in which the mitigations stop those scenarios from

happening. Bowtie methodology brings the following benefits for the risk scenarios analysis: provide a structure to systematically analyse a hazard, help make a decision whether the current level of mitigation or control is sufficient, help identify where and how investing resources would have the greatest impact in hazard mitigations and increase risk mitigation awareness.

The definitions of the Bowtie method elements generally fall into two leading paradigms. The first paradigm described in [10, 5] has the following elements:

Hazard: The condition, object, or activity with the potential of causing injuries to personnel, damage to equipment or structures, loss, or material reduction of ability to perform a prescribed function. It often describes a normal aspect or activity within the operating environment and set the context and scope of the Bowtie. Also describes the potential source of harm being considered. What makes a hazard special is that it is a part of the system operation that introduces the possibility for harm to occur.

Top event: A point in time which describes the release or loss of control over hazard. This undesired system state exposes the potential harm of the hazard. There is also the possibility to have more than one top event from one hazard.

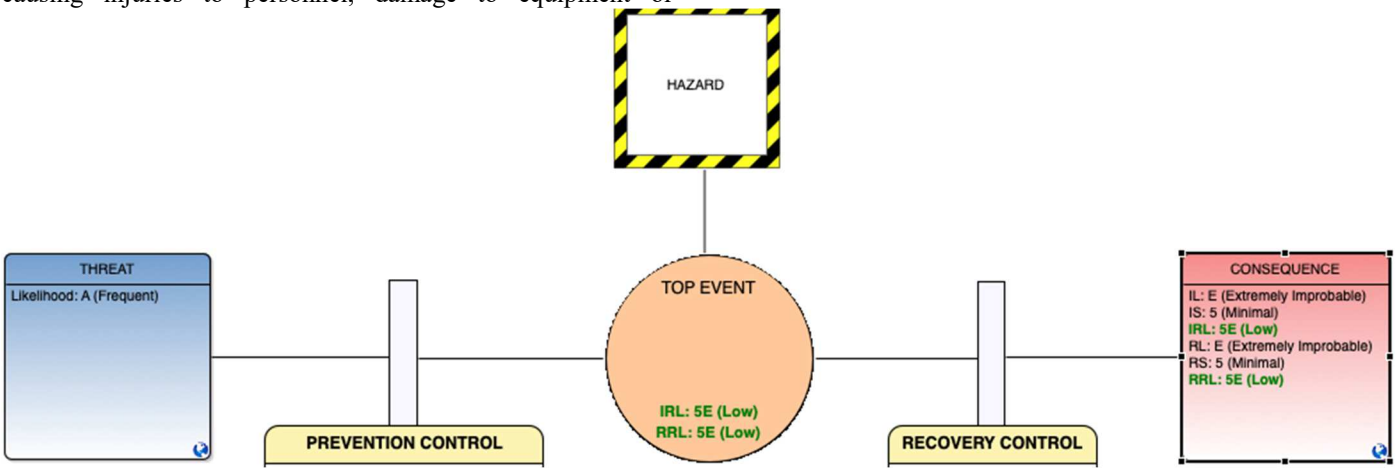

Figure 1: Elements in the Bowtie model

Threats: A possible direct cause that will potentially release a hazard by producing a top event. Each threat should be capable of causing the top event independently.

Consequences: A potential event resulting from release of a Hazard, which directly results in loss or damage. Consequences should be expressed in operational terms and consequences are events not the actual loos or damage.

Prevention controls: Any measure taken which acts against some undesirable force or intention, in order to maintain a desired state. These controls prevent the threat from developing into a top event.

Recovery controls: These are place to reduce the likelihood of the top event developing into a consequence as well as mitigating the severity of the consequence.

The second paradigm described in [11, 12] has almost all the elements from the first paradigm, but this paradigm collapses the elements *hazard* and *top event* into one element and call it *top event* and is defined as the moment when control is lost. There are two additional Bowtie properties described in [13, 14, 15, 16, 17], which are risk matrices and risk mathematical model.

Risk matrices are used in the Bowtie to assess the possible loss or damage that a consequence might cause. A risk matrix has two dimensions which are severity and likelihood of an unwanted event. *Severity* is the consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm. And *Likelihood* is defined as the estimated probability or frequency, in quantitative or qualitative terms, of a hazard's effect or outcome. More specifically, likelihood is a rate of how often a given effect is expected to occur. These two dimensions create a risk matrix. The combination of likelihood and severity will give any event a place on a risk matrix. They are mainly used to determine the size of a risk and whether or not the risk is sufficiently controlled.

The risk mathematical model focuses on computing the reduction in the likelihood of the consequences and top events, as the foundation to establish whether the risk posed has been reduced to an acceptable level. The risk mathematical model depends on two main concepts. First, control/barrier integrity which is the probability that the control/barrier is not breached in a dangerous manner. In other words, it is a measure of the effectiveness of the control to mitigate the likelihood of a top event or consequence. The second concept focuses on the way that the controls/barriers are linked together. They can be put together in series or parallel, where the meaning of series is: if

one control fails then the next control would come into play and the meaning of parallel is: one of the controls come into play.

C. Normalized Terminology

The terminologies used in the context of ORA are different from those used in the context of Bowtie methodology. Furthermore, to visualize ORA data as Bowtie diagrams one can utilize tools like AdvoCATE [14], where the ORA data can be captured and corresponding Bowtie diagrams can be generated. Assurance Case Automation Toolset (AdvoCATE) is a research tool developed by NASA that automates the generation of a safety assurance case. While, the terminology used in AdvoCATE for risk assessment data partially overlaps with the terminology used in the context of ORA and Bowtie models, there is still substantial amount of ambiguity. For example, the definition of *Hazard* in context of ORA (from ASTM F3178) is generic and includes unsafe conditions resulting from failures, malfunctions, external events, errors, or their combinations. Whereas, *Hazard* in Bowtie methodology is used to set the context and scope of the Bowtie, which is often a normal aspect or activity within the operating environment. Whereas, in AdvoCATE, where the risk assessment data can be captured using an interface called Hazard Log Editor, there are two separate entities: "Hazardous Activity" and "Hazard". "Hazardous activity" in AdvoCATE would correspond to *Hazard* in the context of Bowtie methodology, and "Hazard" in AdvoCATE would correspond to *Hazard* in ORA i.e. in ASTM F3178. Therefore, to bridge this gap, we identify a list of normalized terms in Table 1, where each term corresponds to a specific piece of information captured during ORA. To resolve discrepancies in the terminologies we provide definitions for each of the identified terms.

Since traditionally ORA data is recorded in an excel spreadsheet or equivalent format, the proposed list of terms can be used as column headers while capturing ORA data. Furthermore, to aid the creation of Bowtie-diagrams from the ORA data, we will clearly identify which element of the Bowtie model (defined in the previous section) does each normalized term correspond to. Normalized terms that do not have corresponding Bowtie elements in the table are terms that are needed to capture some specific aspects of ORA but are not used or captured in the Bowtie representation.

In addition to the normalized terms in Table 1, in Table 2 we provide auxiliary terms that aid in the calculation of Risk Score. Specifically, the Initial Risk Score i.e. risk score in the absence of prevention and recovery controls, depends on the likelihood of each of the following : cause, top event, effect, cause leading to the top event and top event leading to the effect. The Residual Risk Score, i.e. risk score in the presence of prevention and/or recovery controls depends on the strength of the controls and the likelihood of each of the following : cause, top event, effect, cause leading to the top event and top event leading to the effect. We discuss this in detail in Section III.B.

Normalized Term	Source of the Normalized Term	Definition	Element in Bowtie Model
Hazardous Activity	AdvoCATE [14]	The condition, object or activity with the *potential* of causing injuries to personnel, damage to equipment or structures, loss or material reduction of ability to perform a prescribed function. [10]	Hazard (refer to Figure 1)
Top Event	Bowtie Methodology [10]	A point in time which describes the release or loss of control over a Hazard. The undesired system state. [10]	Top Event (refer to Figure 1)
Cause	AdvoCATE [14]	A possible direct reason or root event that will potentially release a hazard by producing a top event. [10]	Threat (refer to Figure 1)
Allocation	AdvoCATE [14]	Intended behavior of a product based on a defined set of requirements regardless of implementation. (Definition of Function as per [7])	
Source		The sub-system/components that contributed to the functional failure.	
Components Involved		Components impacted by the functional failure.	
Prevention Control	Bowtie Methodology [10]	Any measure taken which acts against some undesirable force or intention, in order to maintain a desired state. [10]	Control to the left of Top Event (refer to Figure 1)
Prevention Control Type	Corresponds to Mitigation Type in AdvoCATE [14]	Category or type of the Prevention Control; A control can be of one of the following types: Design Modification, Safety Feature, Safety Device, Warning Device, Procedures and Training, Operational Controls, Technical Controls and Management Controls [14] [18].	
Prevention Control Strength	Corresponds to Control Integrity in AdvoCATE [14]	Strength of the Prevention Control. Strength of a control can be captured by a value in the range [1, 5], where 1 corresponds to the weakest and 5 corresponds to strongest.	
Recovery Control	Bowtie Methodology [10]	Similarly, to prevention controls, on the right-hand side of the top event, controls are added that show how the scenario is to be managed to stop the effect of the hazard from occurring. These controls are in place to reduce the likelihood of the top event leading to its effect as well as mitigating the severity of the effect. [10]	Control to the right of Top Event (refer to Figure 1)
Recovery Control Type	Corresponds to Mitigation Type in AdvoCATE [14]	Category or type of the Recovery Control; A control can be of one of the following types: Design Modification, Safety Feature, Safety Device, Warning Device, Procedures and Training, Operational Controls, Technical Controls and Management Controls [14] [18].	

Recovery Control Strength	Corresponds to Control Integrity in AdvoCATE [14]	Strength of the Recovery Control. Strength of a control can be captured by a value in the range [1,5], where 1 corresponds to the weakest and 5 corresponds to strongest.	
Effect	ARP4754A [7]	A potential event resulting from the release of a Hazard, which directly results in loss or damage. [10]	Consequence (refer to Figure 1)
Initial Severity	AdvoCATE [14]	Consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm in the absence of mitigation controls. (extension of definition from [6]) It can take values from: Negligible/Minimal 1, Minor 2, Major 3, Hazardous 4, Catastrophic 5	Initial Severity (refer to Figure 1)
Initial Likelihood	AdvoCATE [14]	Estimated probability or frequency, in quantitative and qualitative terms, of a hazard's effect or outcome before the prevention and/or recovery controls are applied. (extension of definition from [6]) It is calculated using likelihood of the top event and likelihood of top event leading to the effect. (c.f. Table 2) It can take the following values: Extremely Improbable = 1, Improbable = 2, Remote = 3, Occasional = 4 and Frequent = 5.	Initial Likelihood (refer to Figure 1)
Initial Risk Score	Corresponds to Unmitigated Risk Score in ASTM F3178 [6]	A composite of predicted severity and likelihood of the potential effect of hazards before the prevention and/or recovery controls are applied. (extending definition of Risk in [7]) It is calculated using the Initial likelihood and Initial Severity.	
Residual Likelihood	AdvoCATE [14]	Estimated probability or frequency, in quantitative and qualitative terms, of a hazard's effect or outcome after the prevention and/or recovery controls are applied. (extension of definition from [6]) It is calculated using the likelihood of the cause leading to the top event in presence of prevention controls and the likelihood of the top event leading to the effect in presence of recovery controls. (c.f. Table 2)	Residual Likelihood (refer to Figure 1)
Residual Severity	AdvoCATE [14]	Consequence or impact of a hazard's effect or outcome in terms of degree of loss or harm after the addition of mitigation controls. (extension of definition from [6]) It can take values from: Negligible/Minimal 1, Minor 2, Major 3, Hazardous 4, Catastrophic 5	Residual Severity (refer to Figure 1)
Residual Risk Score	ASTM F3178 [6]	A composite of predicted severity and likelihood of the potential effect of hazards after the prevention and/or recovery controls are applied. (extending definition of Risk in [7]) It is calculated using Residual Severity and Residual Likelihood.	

Table 1: Normalized terms to capture ORA data and aid creation of corresponding Bowtie diagram

Auxiliary Term	Description
Likelihood of the cause leading to the top event	Provided by the user. It can take the following values: Extremely Improbable = 1, Improbable = 2, Remote = 3, Occasional = 4 and Frequent = 5.
Likelihood of the cause leading to the top event in presence of prevention controls	It is calculated. It can take values from 1 to 5, where 5 is the worst and 1 the best.
Likelihood of the top event leading to the effect	Provided by the user. It can take the following values: Extremely Improbable = 1, Improbable = 2, Remote = 3, Occasional = 4 and Frequent = 5.
Likelihood of the top event leading to the effect in presence of recovery controls	It is calculated. It can take values from 1 to 5, where 5 is the worst and 1 the best.

Table 2: Auxiliary terms that aid in calculation of Risk Score

III. USE CASE

ORA data is traditionally captured in an excel spreadsheet. To illustrate capturing of ORA data in an excel template containing the proposed normalized terminologies, in this section we first introduce an example UA operation scenario and then discuss how the corresponding ORA data can be captured in the excel template.

A. Introducing the use case - ORA of drone operation beyond visual line of sight

We consider operational risk assessment of a drone operated beyond visual line of sight by first responders to rescue a lost hiker under cold weather conditions. Specifically, we consider the operation of drones of two types. One type of drone is a small and faster drone equipped with a non-infrared camera and

This research was performed with funding from NASA.

an infrared camera. The other type of drone is larger in size and has the ability to carry payload. Drones of both types have collision avoidance capability. The mission is to search for the lost hiker, deliver water, food and a blanket to him, and guide the rescue team by providing them the location of the hiker.

A swarm of faster light-weight drones perform surveillance of the mapped area (identified and provided by the operator) and when one of the drones spots a human it uses its camera to capture images and sends it to the operator. After sending the images it switches to "hover-hold" mode. At this point the drone waits for further commands from its operator. When the first responders/operator receive the image, they can control/direct the drone that reported to an appropriate location and right altitude by providing navigational commands to it, to perform closer investigation of the object identified by the drone as a human. Once the identified object is confirmed by the drone-operator as a human and if it is the lost hiker, the operator fetches the location of the drone and provides it as input to the second drone, which is responsible for delivering needed supplies. The operator also reports the location to the rescue team. If it is a night-time rescue mission, the operator provides navigational commands to the faster drone to move it closer to the hiker but at a higher altitude, then issues the "spotlight" command. Upon receiving this command, the drone turns on the LED light beneath it, so that the hiker is in the spotlight (to help the rescue team in finding the hiker in the dark easily). The operator issues "return-to-home" command to all other faster drones.

The second drone navigates to the provided input location. Once the drone reaches the correct location and altitude it reports to the operator its current location, then waits for the operator to issue further commands. The operator verifies that the drone's location is far enough from the hiker (to avoid harming him during the package delivery) but is within the visibility of the hiker (so that the hiker can see the delivery and go fetch it) and issues the "drop" command. The drone drops the package containing water, food and blanket. After dropping the package, the second drone is programmed to return to home. In the meanwhile, first responders use the location of the first drone to reach and rescue the hiker.

B. Capturing the use case in excel

In this section, we discuss how the ORA data corresponding to the use case discussed in Section III.A can be captured in an excel spreadsheet that uses the normalized terminologies introduced in Section II.C. For the sake of illustration, we focus on a specific event where the drone operator loses situational awareness and this is considered as the Top Event. Table 3 shows the ORA data captured in an excel spreadsheet that uses the normalized terminologies. Rows in light green are populated by the user and the rest of the rows are calculated and populated automatically. Calculation of the risk scores in ORA can differ based on the domain, severity/likelihood scales and risk categories under consideration. For the sake of completeness, we next discuss how the risk scores in Table 3 were computed in detail.

Hazardous Activity	Drone is performing surveillance of the mapped area beyond visual line of sight		
Cause	Communication between the UAV and the operator goes down	UAV situational system failure	Display system failure
Likelihood of the cause leading the Top event	5	3	4
Initial Likelihood of the Top Event	5		
Prevention Control	Backup communication system	Heterogenous situational awareness	Backup monitor
Likelihood of cause leading the top event in the presence of prevention control	1	2	3
Likelihood of the top event in the presence of prevention controls	3		
Top Event	Drone operator loses situational awareness		
Recovery Control	Hover in place to establish communication and return to base if unable to establish communication		Collision avoidance
Effect	Loss of UAV		Flight into terrain
Likelihood of the top event leading to the effect	4		5
Likelihood of the top event leading to the effect in the presence of recovery controls	1		1
Initial Severity	3		5
Initial Likelihood	4		5
Initial Risk Score	12		25
Residual Severity	3		5
Residual Likelihood	1		1
Residual Risk Score	3		5

Table 3: Excel template with normalized terms filled in with sample ORA data for the hiker rescue scenario – Main Sheet

	Control Name	Control Strength
Prevention Controls	Backup communication system	5
	Heterogeneous situational awareness	4
	Backup Monitor	3
Recovery Controls	Hover in place to establish communication and return to base if unable to establish communication	5
	Collision Avoidance	5

Table 4 Excel template filled in with controls data for the hiker rescue scenario – Controls Sheet

Risk Calculation

We use risk categories from ASTM F3178-16 as criterions to decide if a risk is acceptable or not. More specifically, it dictates appropriate actions when the risk falls in a particular category. This is shown in Figure 2.

Risk Score		Definition
1-4	Low	Acceptable without review
5-11	Moderate Risk	May be acceptable with review
12 to 19	High Risk	Shall be mitigated
20 to 25	Very High Risk	Unacceptable

Figure 2: ASTM F3178-16 Risk Categories

Function	Purpose
LCT	Likelihood of the Cause leading to the Top Event
ILT	Initial Likelihood of the Top Event
LTE	Likelihood of the Top Event Leading to the Effect
IL	Initial Likelihood
LCTPC	Likelihood of the Cause Leading to the Top Event in the Presence of Prevention Controls
LTPC	Likelihood of the Top Event in the presence of Prevention Controls
LTERC	Likelihood of the Top Event Leading to the Effect in the Presence of Recovery Controls
SPC	Set of Prevention Controls for a Cause
SRC	Set of all Recovery Controls for an Effect
RS	Residual Severity
RL	Residual Likelihood
RRS	Residual Risk Score

Table 5 Functions for expressing the risk calculations.

To express the reasoning that governs the risk calculations described later, we define some abstract functions in Table 5.

Initial Risk Calculation: For a top event **T** and an effect **E**, the following rules can be used for calculating the initial risk:

- **ILT(T) = Max(**∀ cause **C** : **LCT(C,T))**
- **IL(E) = Min(ILT(T), LTE(T,E))**
- **IRS(E) = IS(E) * IL(E)**

Series and Parallel Controls: To calculate the effect of controls in series and parallel combinations**,** we use the *disjunctive normal form* (DNF), which is a canonical normal form for logical formulae consisting of a disjunction of conjunctions. DNF can also be described as OR of ANDs or a sum of products. In our case a DNF form is a parallel combination of one or more series combinations, *i.e.*, a set of controls in series is in parallel with one more other similar sets of controls in series. Given a set of controls **S** which are applied in a parallel combination of subsets of **S** : $\mathbf{S_1}$, $\mathbf{S_2}$, …, $\mathbf{S_n}$ where each subset $\mathbf{S_i}$ is a series combination of one or more controls, the Net Effect (**NE)** of **S** can be calculated as follows:

- **NE(S) = Max(**∀ subset $\mathbf{S_i}$ **in parallel : SE(**$\mathbf{S_i}$**))**

where **SE(**$\mathbf{S_i}$**)** represents the effect of subset $\mathbf{S_i}$ in series and is given by**:**

- **SE(**$\mathbf{S_i}$**) = Min(**∀ control **X in** $\mathbf{S_i}$ **: 6 – CS(X))**

where **CS** represents the Control Strength.

Residual Risk Calculation: When the initial risk of an effect has an unacceptable score, a way to reduce the risk score is to reduce the likelihood of the top event and/or reduce the likelihood of the effect. This is accomplished by using prevention controls, recovery controls or a combination of both. The following rules can be used to compute the residual risk given a top event **T** and an effect **E**:

- **LCTPC(C,T) = Max(LCT(C,T), NE(SPC(C)))**
- **LTPC(T) = Max(**∀ cause **C : LCTPC(C,T))**
- **LTERC(T,E) = Min(LTE(T,E), NE(SRC(E)))**
- **RL(E) = Min(LTPC(T), LTERC(T,E))**
- **RRS(E) = RL(E) * RS(E)**

After the implementation of the appropriate controls, it is expected that each effect will have an acceptable risk score according to the risk category from ASTM F3178-1

IV. ORA DATA MODEL FORMALIZATION

In this section as a first step to enable automated analysis and visualization, we discuss formalization of a data model for ORA. We defined the model in Semantic Application Design Language (SADL). SADL is a language and it is also an IDE for building, viewing, exercising and maintaining semantic models over their lifecycle. The data model defined in SADL is shown in the snippet below.

```
uri "http://sadl.org/ora" alias ora.

HAZARDOUS_ACTIVITY (note "The condition, object or activity with
the potential of causing injuries to personnel, damage to
equipment or structures, loss or material reduction of ability to
perform a prescribed function.") is a class
        described by topEvent with values of type TOP_EVENT.
TOP_EVENT is a class
        described by cause with values of type CAUSE List
        described by effect with values of type EFFECT List
        described by componentsInvolved with values of type
        COMPONENT List
```

```
        described by initialLikelihood with values of type
        LIKELIHOOD
        described by likelihoodWithPC with values of type
        LIKELIHOOD.
CAUSE is a  class
        described by source with values of type COMPONENT
        described by likelihoodOfCL2TE with values of type
        LIKELIHOOD
        described by preventionControl with values of type
        CONTROL List
        described by likelihoodOfCL2TEWithPC with values of type
        LIKELIHOOD.
EFFECT is a class
   described by initialSeverity with values of type SEVERITY
   described by residualSeverity with values of type SEVERITY
   described by initialLikelihood with values of type LIKELIHOOD
   described by likelihoodOfTEL with values of type LIKELIHOOD
   described by residualLikelihood with values of type LIKELIHOOD
   described by likelihoodOfTELRC with values of type LIKELIHOOD
   described by initialRiskScore with values of type int [1,25]
   described by residualRiskScore with values of type int [1,25].

SEVERITY is a class, must be one of {Negligible, Minor, Major,
Hazarsdous, Catastrophic}.
LIKELIHOOD is a class, must be one of {ExtremelyImprobable,
Improbable, Remote, Occasional, Frequent}.

COMPONENT is a class
   described by allocation with values of type FUNCTION.
FUNCTION is a class.
CONTROL is a class
        described by controlStrength with a single value of type
        int [1,5]
        described by isComposite with values of type boolean
        described by seriesComposition with values of type
        CONTROL List.
CONTROL_TYPE is a class, must be one of {Design Modification,
Safety Feature, Safety Device, Warning Device, Procedures and
Training, Operational Controls, Technical Controls and Management
Controls}.
```

SADL instance of this data model corresponding to the data captured in the excel template (shown in Table 3) is as shown below.

```
uri "http://sadl.org/hiker_rescue_ora.sadl" alias
hiker_rescue_ora.

import "http://sadl.org/ora".
Hazard (note "The drone is performing surveillance of the mapped
area beyond visual line of sight") is a HAZARDOUS_ACTIVITY with
topEvent op_loses_sit_awareness.

COMM_failure is a CAUSE.
preventionControl of COMM_failure is [backup_COMM].
likelihoodOfCL2TE of COMM_failure is Frequent.
likelihoodOfCL2TEWithPC of COMM_failure is ExtremelyImprobable.

UAV_SA_failure is a CAUSE.
preventionControl of UAV_SA_failure is [heterogenous_SA].
likelihoodOfCL2TE of UAV_SA_failure is Remote.
likelihoodOfCL2TEWithPC of UAV_SA_failure is Improbable.

display_failure is a CAUSE.
preventionControl of display_failure is [backup_monitor].
likelihoodOfCL2TE of display_failure is Occasional.
likelihoodOfCL2TEWithPC of display_failure is Remote.

backup_COMM is a CONTROL with controlStrength 5.
heterogenous_SA is a CONTROL with controlStrength 4.
backup_monitor is a CONTROL with controlStrength 3.

op_loses_sit_awareness (note "The drone operator loses
situational awareness") is a TOP_EVENT with cause [COMM_failure,
UAV_SA_failure, display_failure].
initialLikelihood of op_loses_sit_awareness is Frequent.
likelihoodWithPC of op_loses_sit_awareness is Remote.

hover_in_place is a CONTROL with controlStrength 5.
collision_avoidance is a CONTROL with controlStrength 5.

loss_of_UAV is an EFFECT.
recoveryControls of loss_of_UAV is [hover_in_place].
likelihoodOfTEL of loss_of_UAV is Occasional.
likelihoodOfTELRC of loss_of_UAV is ExtremelyImprobable.
initialSeverity of loss_of_UAV is Major.
initialLikelihood of loss_of_UAV is Occasional.
initialRiskScore of loss_of_UAV is 12.
residualSeverity of loss_of_UAV is Major.
residualLikelihood of loss_of_UAV is ExtremelyImprobable.
residualRiskScore of loss_of_UAV is 3.

flight_into_terrain is an EFFECT.
recoveryControls of loss_of_UAV is [collision_avoidance].
likelihoodOfTEL of flight_into_terrain is Frequent.
likelihoodOfTELRC of flight_into_terrain is ExtremelyImprobable.
initialSeverity of flight_into_terrain is Catastrophic.
initialLikelihood of flight_into_terrain is Frequent.
initialRiskScore of flight_into_terrain is 25.
residualSeverity of flight_into_terrain is Catastrophic.
residualLikelihood of flight_into_terrain is ExtremelyImprobable.
residualRiskScore of  flight_into_terrain is 5.
```

Capturing the assessment data in a formally defined data model can enable easy querying of the data to suit the needs of the target audience. For instance one can use the presented data model to define the ontology (elements in ORA and their relationships) in data curation tools like RACK (Rapid Assurance Curation Kit), ingest the ORA data and query to analyze/visualize specific aspects of it.

V. Visualization in AdvoCATE

Assurance Case Automation Toolset (AdvoCATE) was developed by NASA intended to automate the generation of a safety assurance case. AdvoCATE can be used to generate GSN(Goal Structuring Notation) based safety case fragments and Bowtie diagrams. Risk assessment data can be captured in an interface called hazard log editor in AdvoCATE. Data captured in the hazard log editor can be used to generate Bowtie diagrams in AdvoCATE. Figure 3 shows the Bowtie diagram generated using AdvoCATE corresponding to the ORA data captured in the excel spreadsheet as discussed in the previous section. ORA data from the excel spreadsheet was manually entered into the hazard log editor to generate the Bowtie diagram.

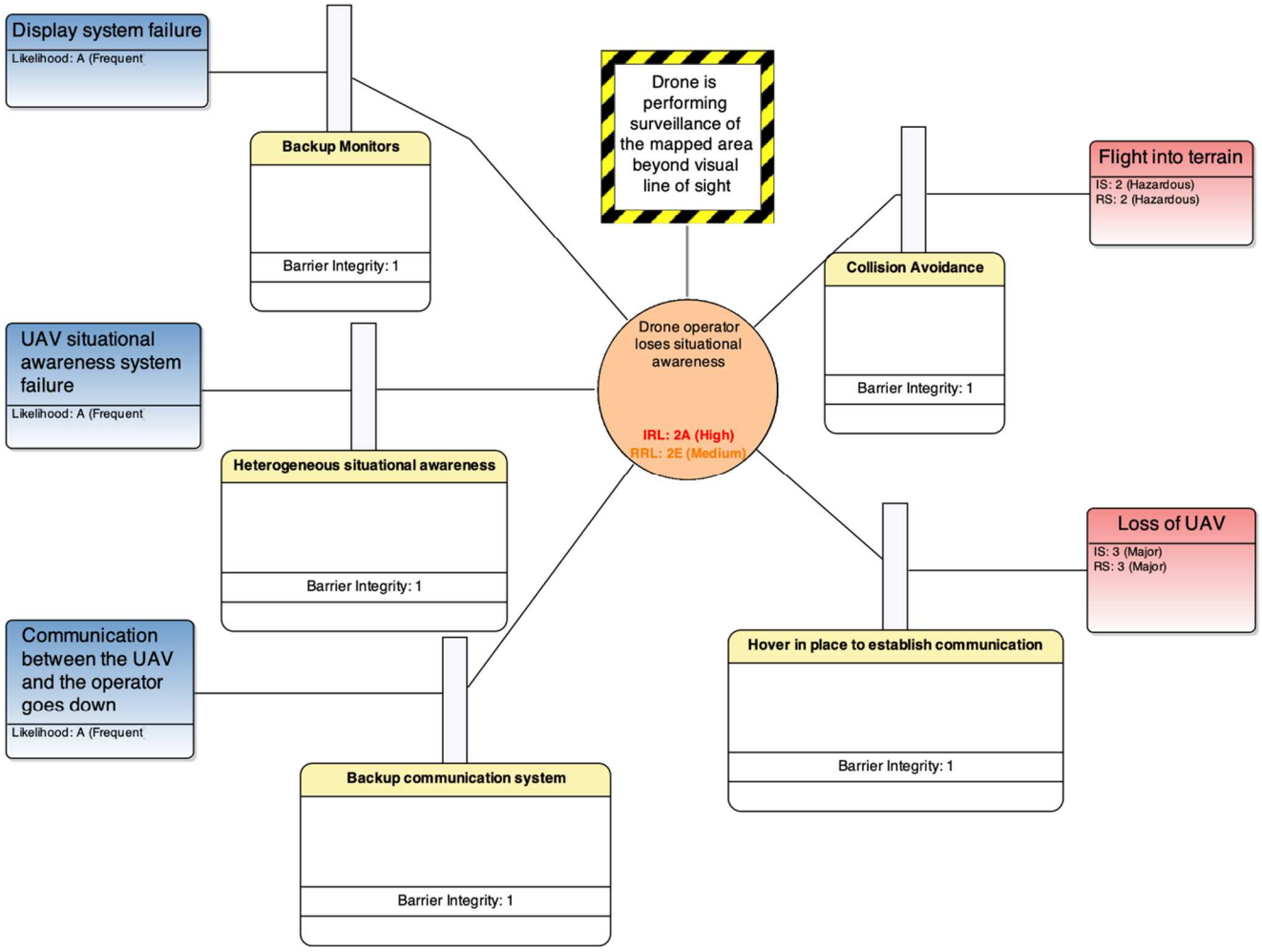

Figure 3: Bowtie diagram generated using AdvoCATE

VI. Conclusion

Visualizing ORA data as Bowtie diagrams can improve the understanding of risk associated with events and impact of mitigations on the identified risks. In this paper we discussed the need for common terminology to map ORA data to Bowtie models. To address this need we proposed a set of terminologies that trace back to standards. We discussed how an excel template containing the normalized terms can be used to capture the ORA data. We also discussed the relationship between the controls (mitigations) and risk scores in our proposed excel template. While diagramatic visualization of the ORA data can be beneficial, manual mapping of ORA data to Bowtie models can be inefficient. As a first step to enabling automatization, we presented a formal data model that captures the relationship between different aspects of the ORA data. This data model can be used to define the ontology in data curation tools like RACK, where once the ontolgoy is defined one can ingest the ORA data and query specific aspects of it. For instance one can query to identify which controls/mitigations can be used to prevent a specific hazardous event. A visualization tool can use the generated query results to generate a Bowtie diagam.

VII. Future Work

To enable automated generation of Bowtie diagrams corresponding to the ORA data we will extend the current work to capture the proposed formal data model in RACK (Rapid Assurance Curation Kit). RACK is a database that uses a structured semantic data model and is a data curation tool that can be used to import and query data. Once the proposed ORA data model is captured as an ontology in RACK, the ORA data captured in excel format can be ingested into RACK. After the ORA data is ingested into RACK, we can query RACK to fetch specific pieces of information in the ORA data by running different queries. To enable generation of Bowtie diagrams, we will create queries to retrieve information corresponding to different Bowtie elements like Top Event, Cause and so on. The fetched information can then be used in Bowtie generation tools like AdvoCATE, where the fetched data can be used to populate loggers or editors like Hazard Log Editors to generate corresponding Bowtie diagrams.

Acknowledgment

This work was supported by NASA System Wide Safety Grant #80NSSC19M0239.

REFERENCES

[1] J. Larrow, "Building Your Operational Risk Assessment," [Online]. Available: https://www.faa.gov/uas/resources/events_calendar/archive/2019_uas_symposium/media/Building_Your_Operational_Risk_Assessment.pdf. [Accessed 8 December 2020].

[2] F. A. Administration, "FAA Safety Management - Safety Risk Management Guidance: SRM Tools," 30 April 2018. [Online]. Available: https://www.faa.gov/regulations_policies/handbooks_manuals/aviation/risk_management/media/20180430_FAASRMGuidanceSRMTools_signed_508.pdf. [Accessed 8 December 2020].

[3] H. Wang, J. Wan and L. Miao, "Research on Controlled Flight Into Terrain Risk Analysis Based on Bow-tie Model and WQAR Data," in *Asia-Pacific Engineering and Technology Conference*, 2017.

[4] L. Cui, J. Zhang, B. Ren and H. Chen, "Research on a new aviation safety index and its solution under uncertainty conditions," *Safety Science,* vol. 107, pp. 55-61, 2018.

[5] J. Aust and D. Pons, "Bowtie Methodology for Risk Analysis of Visual Borescope Inspection during Aircraft Engine Maintenance," *Aerospace ,* 2019.

[6] ASTM, "F3178 Standard Practice for Operational Risk Assessment of Small Unmanned Aircraft Systems (sUAS)," 2018.

[7] SAE, "ARP4754A Guidelines for Development of Civil Aircraft and Systems," 2010.

[8] J. Rushby, "The Interpretation and Evaluation of Assurance Cases," Computer Science Laboratory, SRI International, Menlo Park, CA, 2015.

[9] B. Meng, A. Moitra, A. W. Crapo, S. Paul, K. Siu, M. Durling, D. Prince and H. Herencia-Zapana, "Towards Developing Formalized Assurance Cases," in *AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)*, San Antonio, 2020 .

[10] C. A. Authority, "Introduction-to-bowtie," [Online]. Available: https://www.caa.co.uk/Safety-initiatives-and-resources/Working-with-industry/Bowtie/About-Bowtie/Introduction-to-bowtie/. [Accessed 8 December 2020].

[11] F. Guldenmund and A. d. Ruijter, "The bowtie method: A review," *Safety Science,* vol. 88, no. ISSN 0925-7535, pp. 212-218, 2016.

[12] V. d. Dianousa and C. Fiévezb, "ARAMIS project: A more explicit demonstration of risk control through the use of bow–tie diagrams and the evaluation of safety barrier performance," *Journal of Hazardous Materials,* vol. 130, no. 3, pp. 220-233, 2006.

[13] E. Denney, G. Pai and M. Johnson, "Towards a rigorous basis for specific operations risk assessment of UAS.," in *IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, 2018.

[14] E. Denney, G. Pai and J. Pohl, "AdvoCATE: An assurance case automation toolset," in *International Conference on Computer Safety, Reliability, and Security*, Berlin, Heidelberg., 2012.

[15] E. Denney and G. Pai, "Tool Support for Assurance Case Development," *Automated Software Engg.,* vol. 25, p. 435–499, 2018.

[16] Joint Authorities for Rulemaking of Unmanned Systems, "JARUS guidelines on Specific Operations Risk Assessment (SORA)," 2017. [Online]. Available: http://jarus-rpas.org/sites/jarus-rpas.org/files/jar_doc_06_jarus_sora_v1.0.pdf. [Accessed 14 December 2020].

[17] K. Ellis, P. Krois, M. D. Davirs and J. Koelling, "In-Time System-Wide Safety Assurance (ISSA) Concept of Operations," 2019.

[18] G. Stoneburner, A. Goguen and A. Feringa, *Risk Management Guide for Information Technology Systems - Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-30,,* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, 2002.

[19] E. Denney and G. Pai, "Architecting a Safety Case for UAS Flight Operations," in *Conference: 34th International System Safety Conference (ISSC 2016)*, 2016.

[20] Uschold M., "Ontology and database schema: What's the difference?. Applied Ontology.," pp. 243-58., 2015.