Developing Safety and Mission Assurance Cases with AdvoCATE

Ewen Denney

NASA Ames Research Center

Assurance Case Adoption

- Piper Alpha Report (Cullen Inquiry), 1990
  - Recommended application of safety cases to offshore installations
  - Subsequently adopted by UK Ministry of Defense, Def-Stan-00-56 (MOD), 2004
- Now widely used in many safety-critical industries
  - Offshore Oil & Gas (Cullen 1990), Defense, Medical, Transportation (Road, Rail and Air), Nuclear
- Increasing usage in the U.S.
  - FDA – Infusion pumps
  - FAA – UAS operational approval, performance-based regulation
  - NRC – Nuclear waste disposal
- Defense aviation
  - Military aircraft, largely in UK and Australia
  - NAVAIR
- Civil Aviation
  - By ICAO for RVSM implementation over Africa, Asia
  - EUROCONTROL
  - JARUS – UAS
- Automotive
  - ISO 26262 Functional safety
  - ISO 21448 Safety of the intended functionality
  - UL 4600 Safety of autonomous products
- NASA
  - Objective Hierarchies
  - Risk-informed Safety Cases

Safety (Assurance) Case

- Comprehensive, auditable, safety risk management artifact

- Authoritative record that
  - Safety risks have been identified, are well understood
  - Processes and mechanisms in place for risk reduction
    - Driver for development

- Explicit claims and evidence connected by rationale (argumentation)

- Properties
  - Compelling, comprehensive, convincing, valid, justifiable, defensible, …

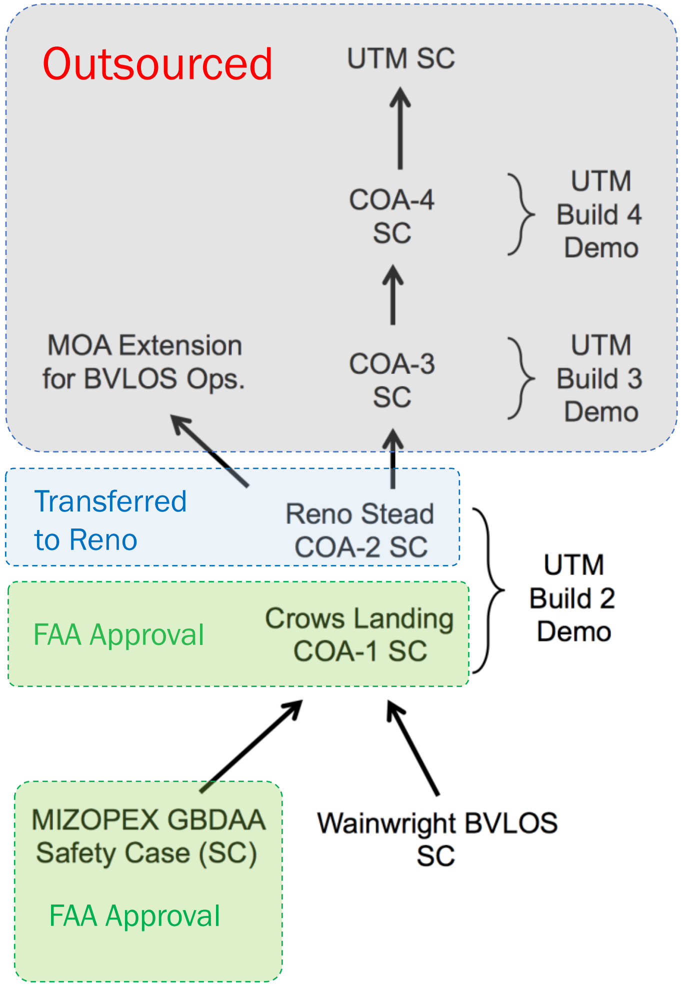
Capturing a Variety of Rationale

- High-level decomposition of assurance objectives
- How specific claims made about the system follows from the evidence supplied
- Verification is appropriate, evidence is relevant, hazard analysis is comprehensive
- Sub-requirements imply parent requirement
- Justification of quantification
- Counterarguments and how they are managed
- Substantiation of assumptions about
  - System, environment, its operations
  - Supporting analysis, design, verification
- Clarification of the context for claims and evidence
- Independence of mitigations
- Single software failures do not lead to system failure
- ALARP / ASARP

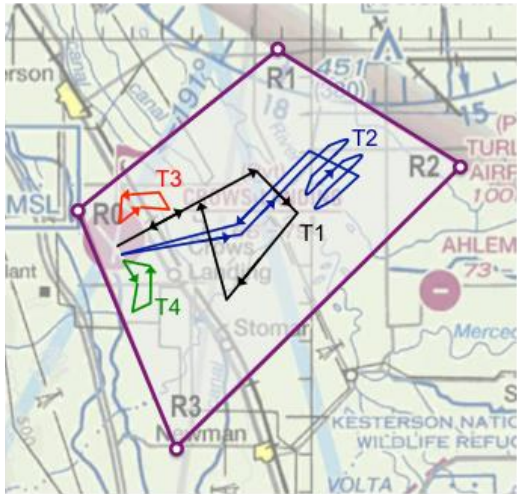
NASA Usage: UTM

- UAS Traffic Management (UTM)
- Series of Beyond Visual Line of Sight (BVLOS) Safety Cases
  - Transit operations
    - Alaska, MIZOPEX / Oliktok for Earth Science Division
    - Alaska, Wainwright for 3rd party in UTM
  - UTM
    - TCL2 (Crows Landing Airfield CA93) – Enabling multiple VLOS and BVLOS UAS flights in a defined operating region with ground-based radar
    - First BVLOS flight approved by FAA in National Airspace System
    - TCL2 (Reno-Stead Airport RTS) – Enabling multiple VLOS and BVLOS UAS flights at non-towered airport with general aviation, using ground-based radar

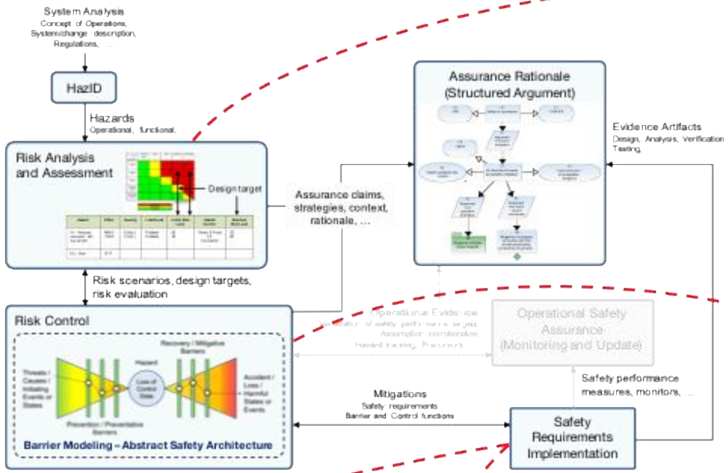
- Risk-based Safety Assurance
  - Safety measures commensurate with risk posed
    - CONOPS, Vehicle, Area



UAS and UTM Safety



Notional CONOPS



System Analysis
Concept of Operations, System/change description, Regulations, …

HazID

Hazards
Operational, functional, …

Risk Analysis and Assessment

Design target

Assurance claims, strategies, context, rationale, …

Assurance Rationale (Structured Argument)

Evidence Artifacts
Design, Analysis, Verification Testing,

Risk scenarios, design targets, risk evaluation

Risk Control

Recovery / Mitigative Barriers

Hazard

Threats / Causes / Initiating Events or States

Loss of Control State

Accident / Loss / Harmful States or Events

Prevention / Preventative Barriers

Barrier Modeling – Abstract Safety Architecture

Operational Evidence
Verification of safety performance targets
Assumption corroboration
Hazard tracking, Precursors

Operational Safety Assurance (Monitoring and Update)

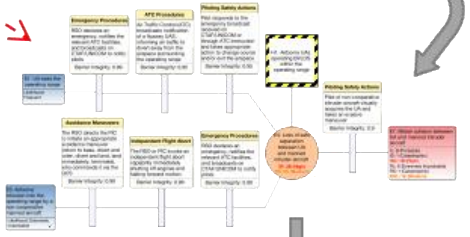
Safety performance measures, monitors, …

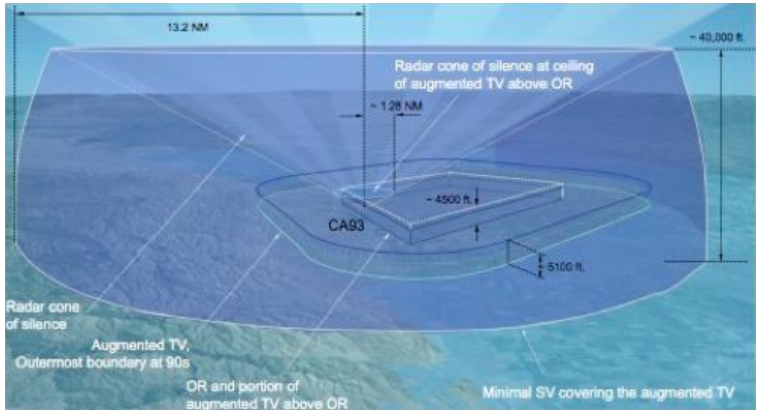
Mitigations
Safety requirements
Barrier and Control functions

Safety Requirements Implementation

Identified Hazards

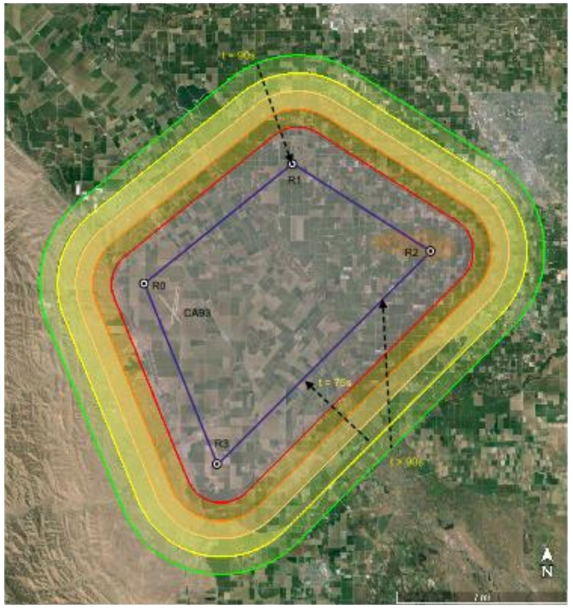
- Primary hazards
  - PH1: NMAC with non-cooperative airborne entities
  - PH2: NMAC between UAs
  - PH3: Collision into ground / structures / people / vehicles
  - PH4: Rapid onset of inclement weather
  - PH5: GPS signal outage
  - PH6: UAs exiting the OR
- Secondary hazards
  - SH1: Lithium fire and/or explosion
- Contributory hazards
  - CH1: Loss of surveillance
  - CH2: Loss of command and control (C2) links
  - CH3: Loss of ground control station (GCS)
  - CH4: Unrecoverable UA failures/malfunction in flight
  - CH5: UA deviation from approved flight path and/or exiting the OR
  - CH6: Human factors
  - CH7: Loss of voice communication links



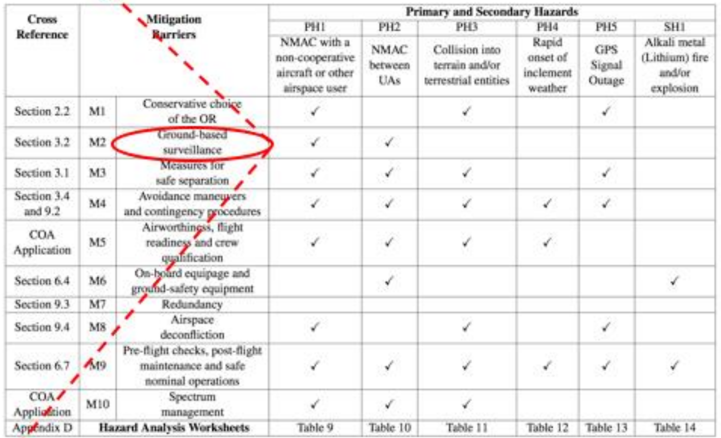


13.2 NM
~ 40,000 ft.
Radar cone of silence at ceiling of augmented TV above OR
~ 1.28 NM
~ 4500 ft.
CA93
5100 ft.
Radar cone of silence
Augmented TV, Outermost boundary at 90s
OR and portion of augmented TV above OR
Minimal SV covering the augmented TV

- Surveillance Requirements
- Avoidance maneuvers, Procedures, etc.
- Justification and Rationale



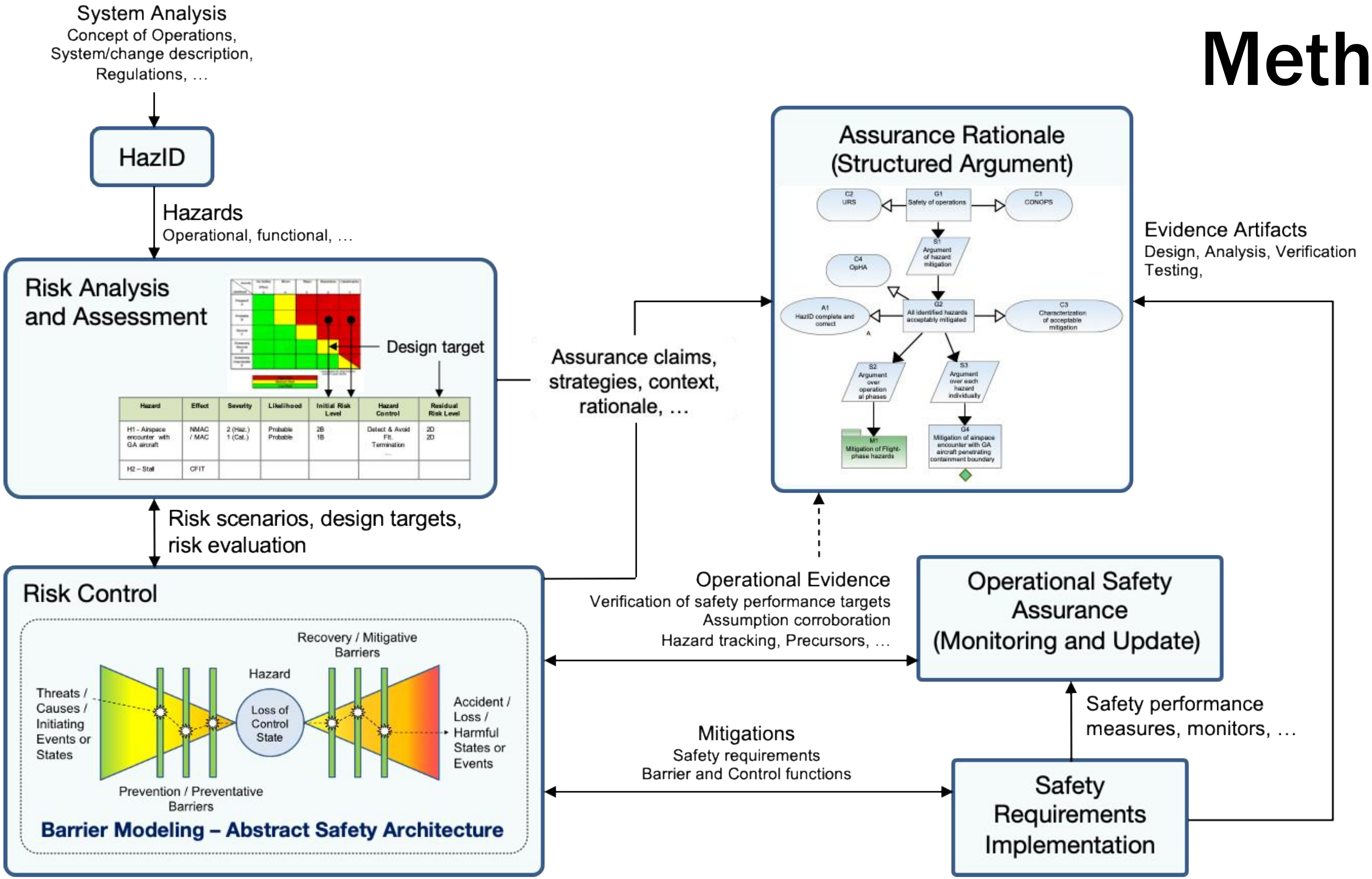
Airspace / Threat Modeling



Cross Reference	Mitigation Barriers		Primary and Secondary Hazards					
			PH1	PH2	PH3	PH4	PH5	SH1
			NMAC with a non-cooperative aircraft or other airspace user	NMAC between UAs	Collision into terrain and/or terrestrial entities	Rapid onset of inclement weather	GPS Signal Outage	Alkali metal (Lithium) fire and/or explosion
Section 2.2	M1	Conservative choice of the OR	✓		✓		✓	
Section 3.2	M2	Ground-based surveillance	✓	✓				
Section 3.1	M3	Measures for safe separation	✓	✓	✓		✓	
Section 3.4 and 9.2	M4	Avoidance maneuvers and contingency procedures	✓	✓	✓	✓	✓	
COA Application	M5	Airworthiness, flight readiness and crew qualification	✓	✓	✓	✓		
Section 6.4	M6	On-board equipage and ground-safety equipment		✓				✓
Section 9.3	M7	Redundancy						
Section 9.4	M8	Airspace deconfliction	✓		✓		✓	
Section 6.7	M9	Pre-flight checks, post-flight maintenance and safe nominal operations	✓	✓	✓	✓	✓	✓
COA Application	M10	Spectrum management	✓	✓	✓			
Appendix D	Hazard Analysis Worksheets		Table 9	Table 10	Table 11	Table 12	Table 13	Table 14

Traceability from Hazards to Mitigation Barriers

Methodology



System Analysis
Concept of Operations,
System/change description,
Regulations, …

HazID

Hazards
Operational, functional, …

Risk Analysis and Assessment

Design target

Hazard	Effect	Severity	Likelihood	Initial Risk Level	Hazard Control	Residual Risk Level
H1 - Airspace encounter with GA aircraft	NMAC / MAC	2 (Haz.) 1 (Cat.)	Probable Probable	2B 1B	Detect & Avoid Flt. Termination …	2D 2D
H2 – Stall	CFIT					

Risk scenarios, design targets, risk evaluation

Assurance claims, strategies, context, rationale, …

Assurance Rationale (Structured Argument)

C2
URS
G1
Safety of operations
C1
CONOPS
S1
Argument of hazard mitigation
C4
OpHA
A1
HazID complete and correct
A
G2
All identified hazards acceptably mitigated
C3
Characterization of acceptable mitigation
S2
Argument over operational phases
S3
Argument over each hazard individually
M1
Mitigation of Flight-phase hazards
G4
Mitigation of airspace encounter with GA aircraft penetrating containment boundary

Evidence Artifacts
Design, Analysis, Verification
Testing,

Risk Control

Recovery / Mitigative Barriers
Hazard
Threats / Causes / Initiating Events or States
Loss of Control State
Accident / Loss / Harmful States or Events
Prevention / Preventative Barriers

Barrier Modeling – Abstract Safety Architecture

Operational Evidence
Verification of safety performance targets
Assumption corroboration
Hazard tracking, Precursors, …

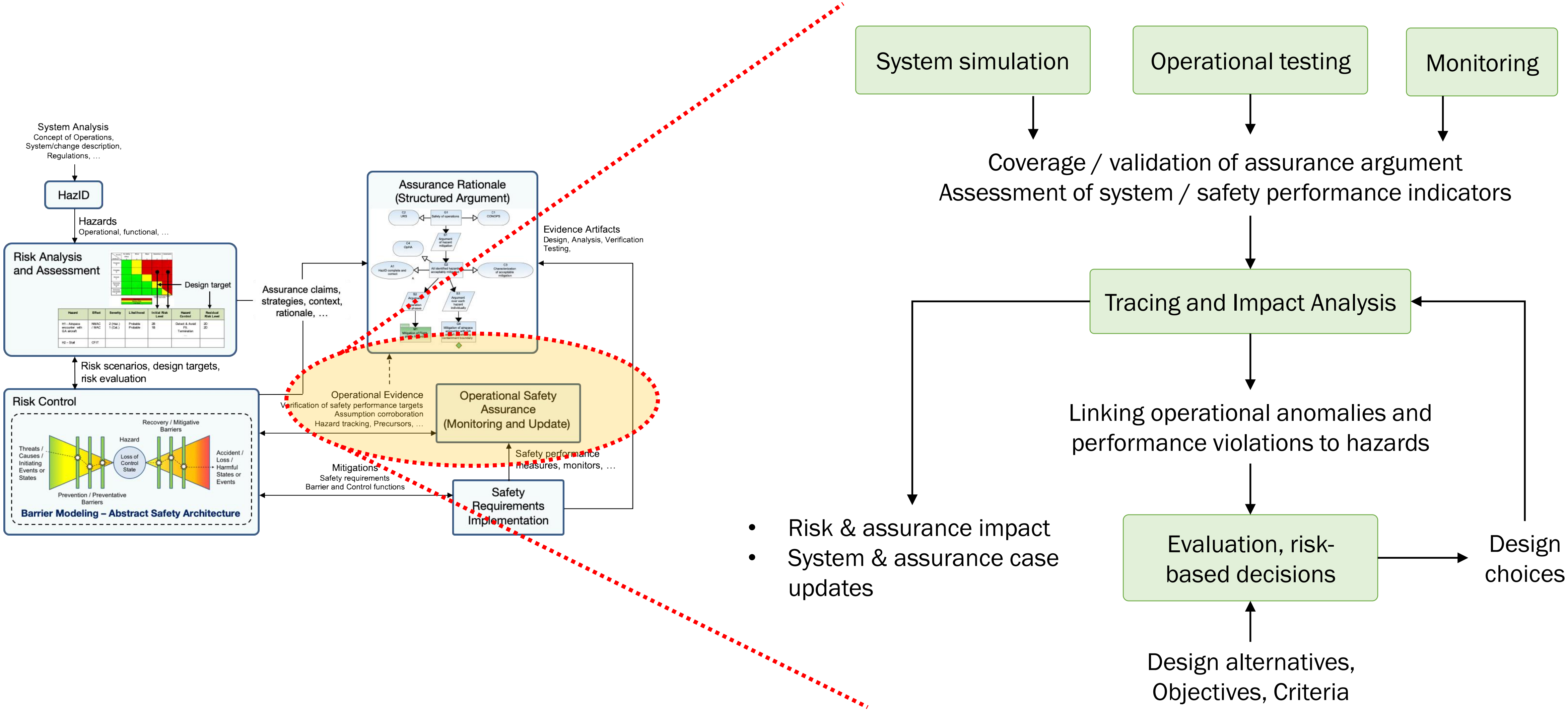
Operational Safety Assurance (Monitoring and Update)

Safety performance measures, monitors, …

Mitigations
Safety requirements
Barrier and Control functions

Safety Requirements Implementation

Methodology



System Analysis
Concept of Operations,
System/change description,
Regulations, …

HazID

Hazards
Operational, functional, …

Risk Analysis and Assessment

Design target

Risk scenarios, design targets, risk evaluation

Risk Control

Barrier Modeling – Abstract Safety Architecture

Assurance claims, strategies, context, rationale, …

Assurance Rationale (Structured Argument)

Evidence Artifacts
Design, Analysis, Verification
Testing,

Operational Evidence
Verification of safety performance targets
Assumption corroboration
Hazard tracking, Precursors, …

Operational Safety Assurance (Monitoring and Update)

Safety performance measures, monitors, …

Mitigations
Safety requirements
Barrier and Control functions

Safety Requirements Implementation

Hazard
Effect
Severity
Likelihood
Initial Risk Level
Hazard Control
Residual Risk Level
H1 - Airspace encounter with GA aircraft
NMAC / MAC
2 (Haz.) 1 (Cat.)
Probable Probable
2B 1B
Detect & Avoid Flt. Termination
2D 2D
H2 – Stall
CFIT
Recovery / Mitigative Barriers
Hazard
Threats / Causes / Initiating Events or States
Loss of Control State
Accident / Loss / Harmful States or Events
Prevention / Preventative Barriers
C2 URS
G1 Safety of operations
C1 CONOPS
S1 Argument of hazard mitigation
C4 OpHA
A1 HazID complete and correct
G2 All identified hazards acceptably mitigated
C3 Characterization of acceptable mitigation
S2 Argument over operational phases
S3 Argument over each hazard individually
M1 Mitigation of Flight phase hazards
G4 Mitigation of airspace encounter with GA aircraft penetrating containment boundary

System simulation

Operational testing

Monitoring

Coverage / validation of assurance argument
Assessment of system / safety performance indicators

Tracing and Impact Analysis

Linking operational anomalies and performance violations to hazards

- Risk & assurance impact
- System & assurance case updates

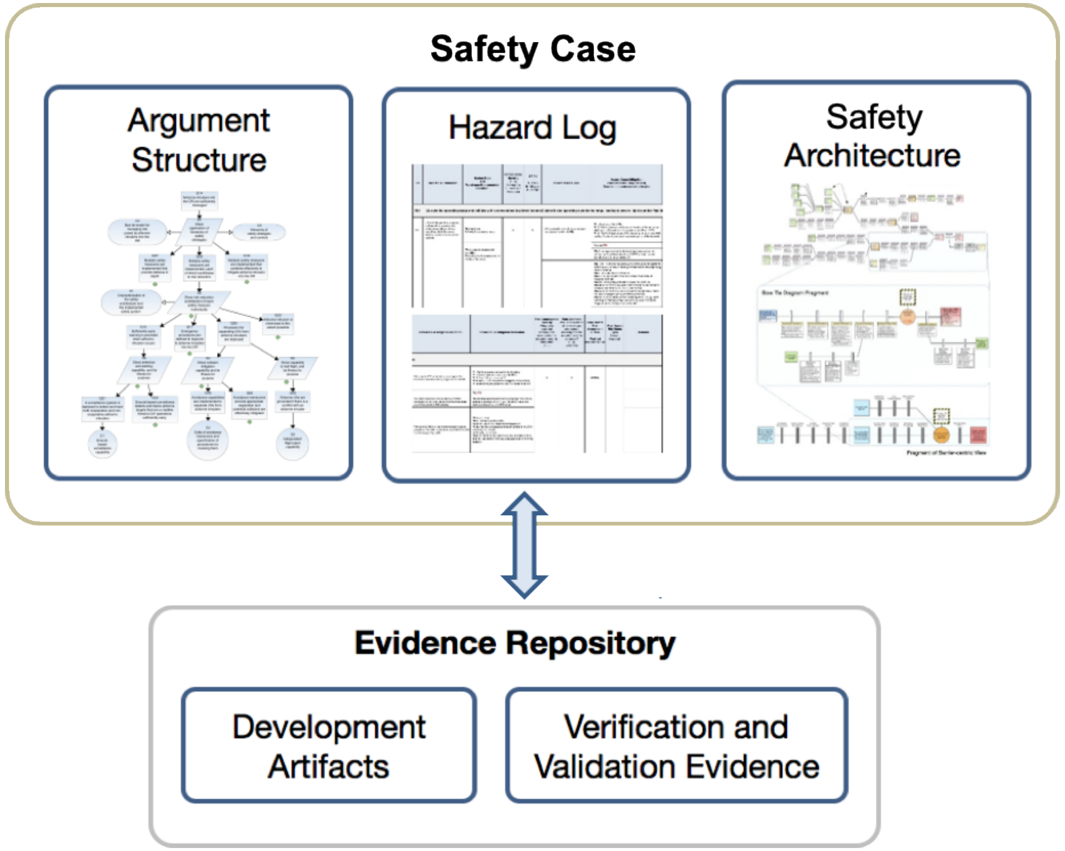
Evaluation, risk-based decisions

Design choices

Design alternatives, Objectives, Criteria

Core Safety Case Components

- Explicit statement of safety assurance objectives
- Heterogeneous evidence
  - Datasheets, design and analysis, verification, operational testing,…
- Structured argument
  - Capturing rationale why evidence supports the claims made
  - Framework to incorporate many standard kinds of evidence and analysis.
- Additionally,
  - Safety architecture providing a risk basis
  - Hazard log and hazard analyses
  - Evidence model



Safety Case

Argument Structure

Hazard Log

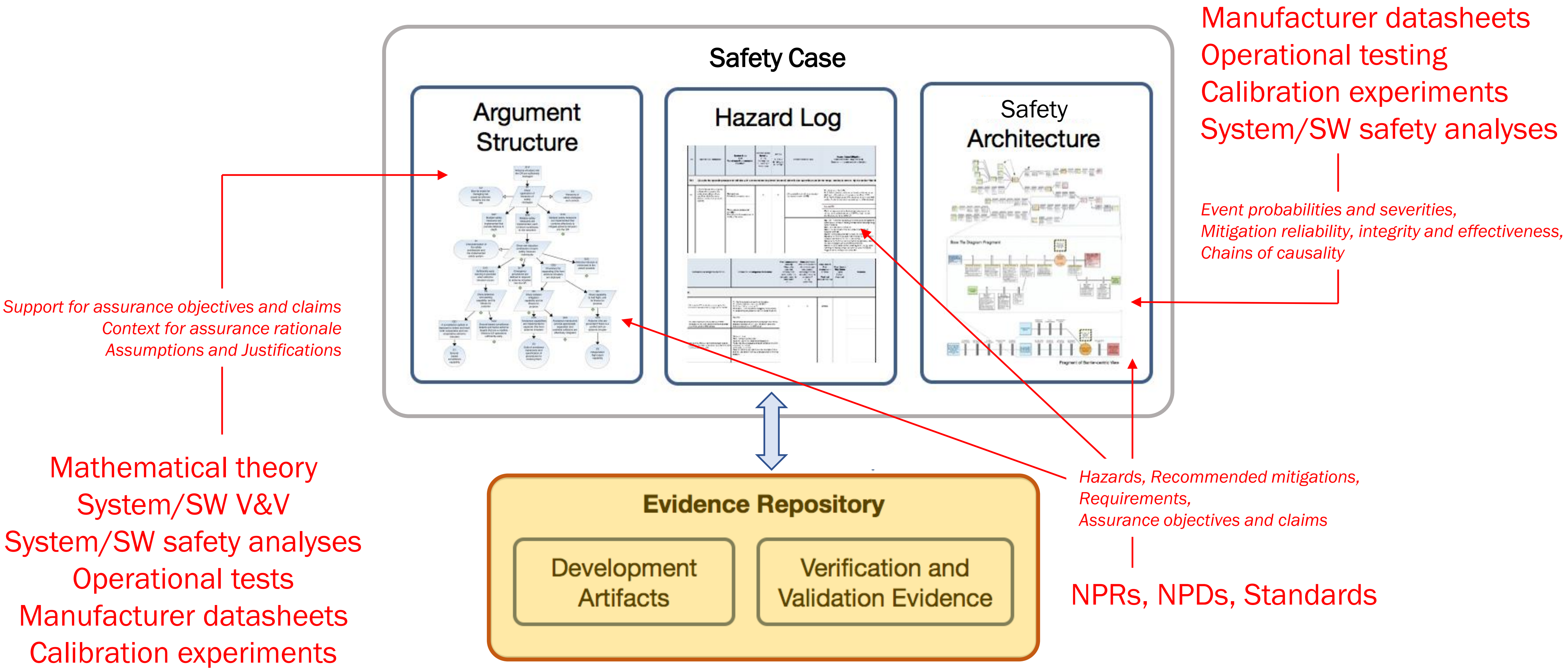
Safety Architecture

Evidence Repository

Development Artifacts

Verification and Validation Evidence

Heterogeneous Evidence



Safety Case

Argument Structure

Hazard Log

Safety Architecture

Evidence Repository

Development Artifacts

Verification and Validation Evidence

Manufacturer datasheets
Operational testing
Calibration experiments
System/SW safety analyses

Event probabilities and severities,
Mitigation reliability, integrity and effectiveness,
Chains of causality

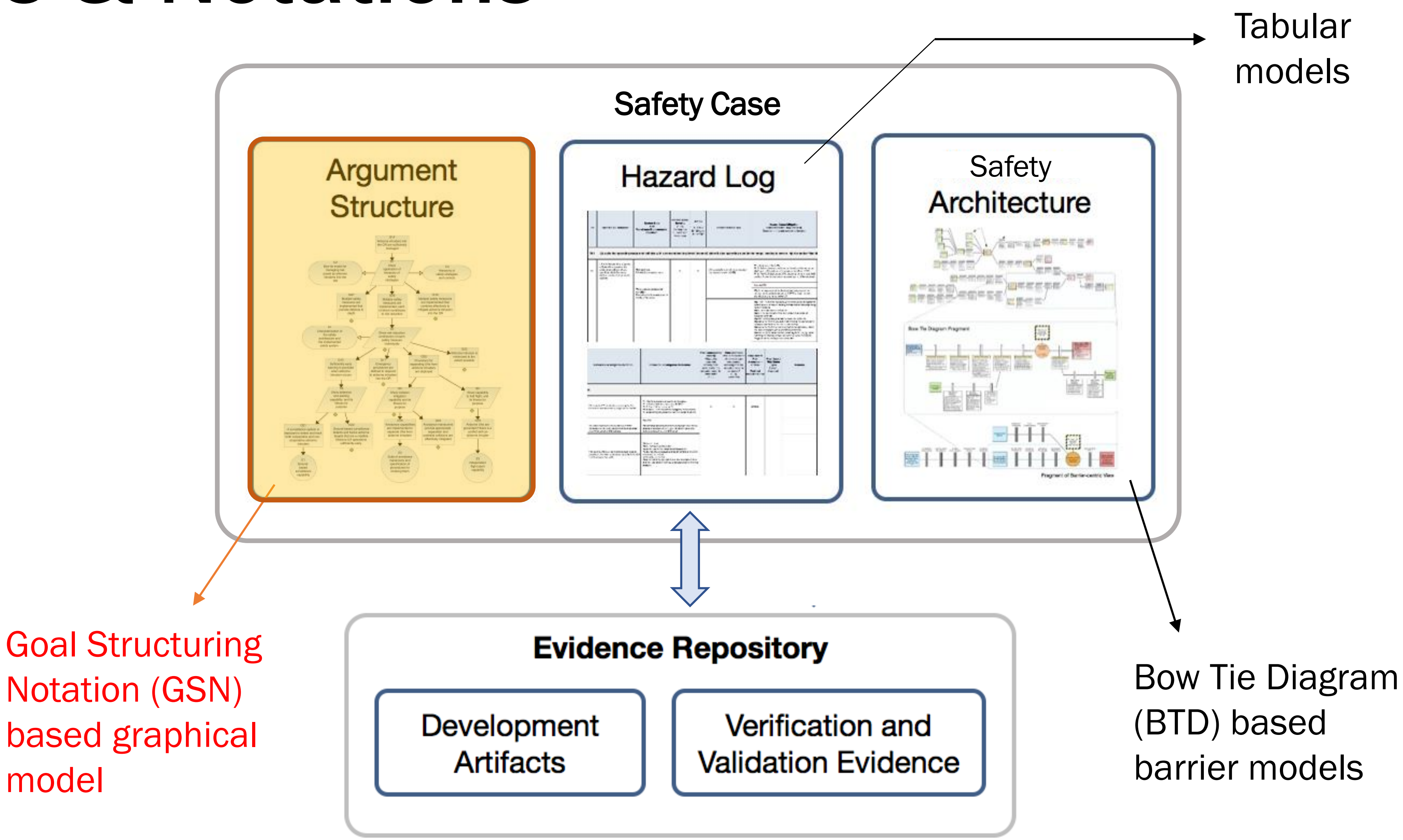
Support for assurance objectives and claims
Context for assurance rationale
Assumptions and Justifications

Mathematical theory
System/SW V&V
System/SW safety analyses
Operational tests
Manufacturer datasheets
Calibration experiments

Hazards, Recommended mitigations,
Requirements,
Assurance objectives and claims

NPRs, NPDs, Standards

Models & Notations



Safety Case

Argument Structure

Hazard Log

Safety Architecture

Evidence Repository

Development Artifacts

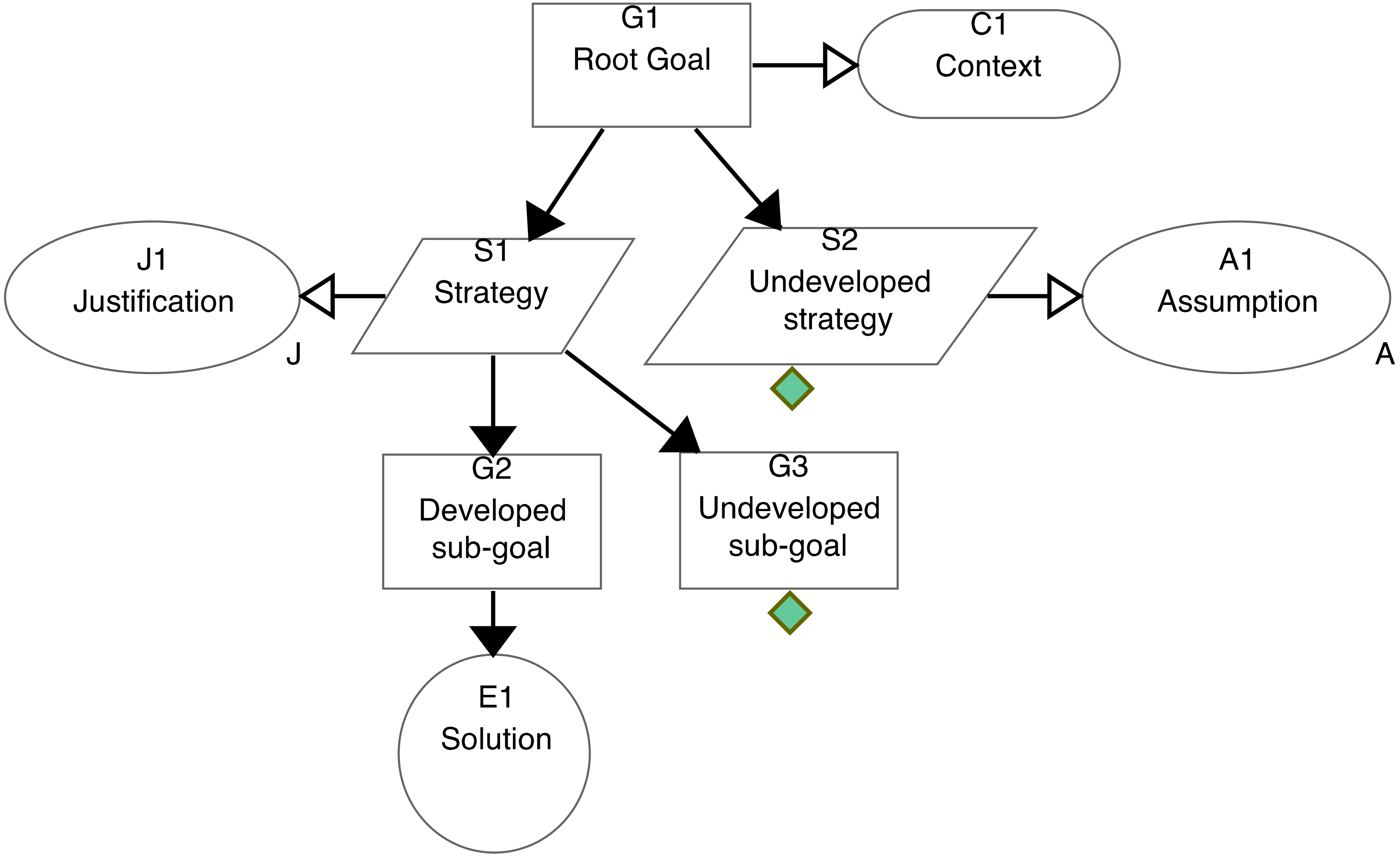
Verification and Validation Evidence

Tabular models

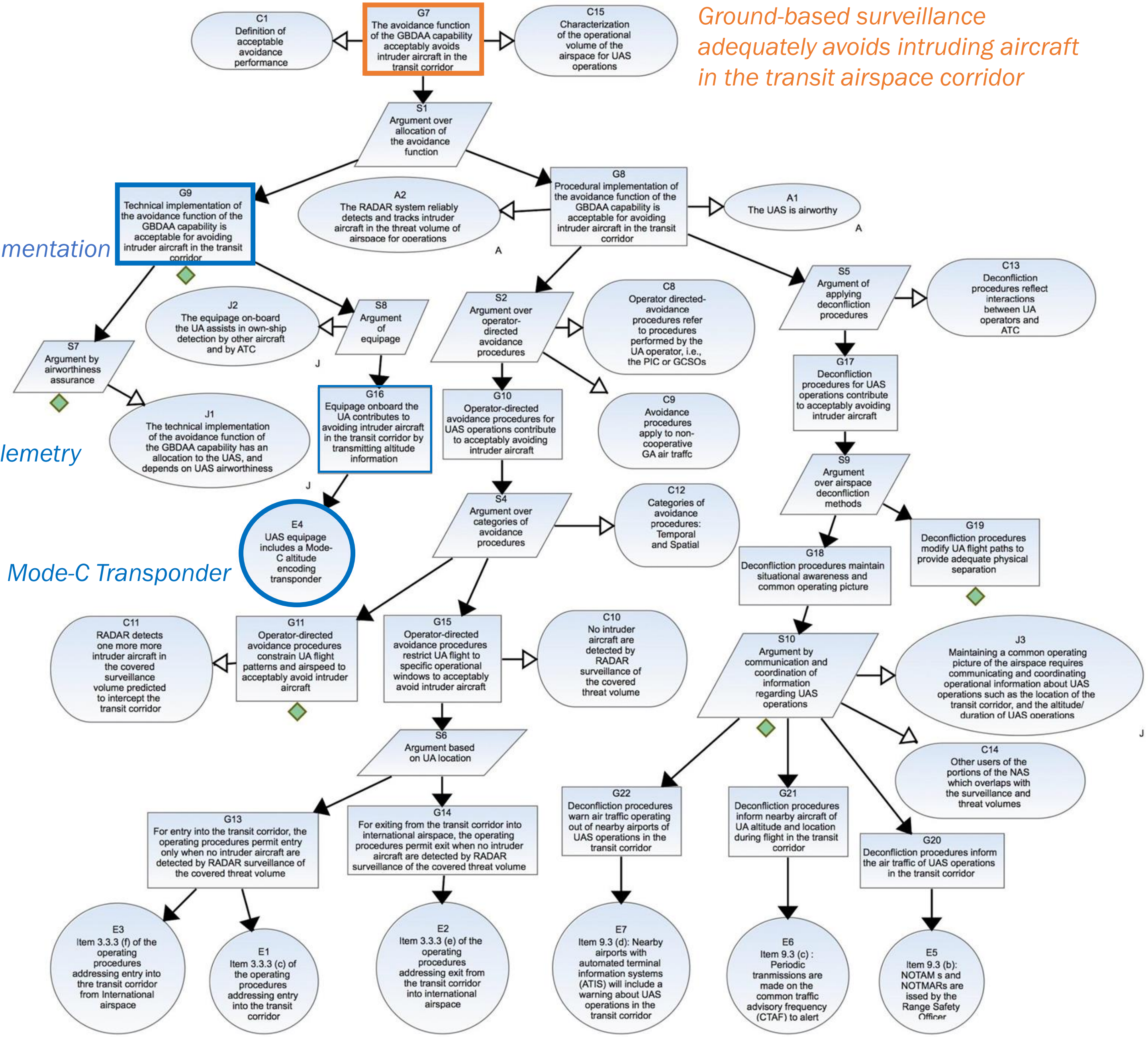
Goal Structuring Notation (GSN) based graphical model

Bow Tie Diagram (BTD) based barrier models

Goal Structuring Notation



Example



Ground-based surveillance adequately avoids intruding aircraft in the transit airspace corridor

Acceptable technical implementation

Equipage for altitude telemetry

Mode-C Transponder

C1
Definition of acceptable avoidance performance

G7
The avoidance function of the GBDAA capability acceptably avoids intruder aircraft in the transit corridor

C15
Characterization of the operational volume of the airspace for UAS operations

S1
Argument over allocation of the avoidance function

G9
Technical implementation of the avoidance function of the GBDAA capability is acceptable for avoiding intruder aircraft in the transit corridor

A2
The RADAR system reliably detects and tracks intruder aircraft in the threat volume of airspace for operations

A

G8
Procedural implementation of the avoidance function of the GBDAA capability is acceptable for avoiding intruder aircraft in the transit corridor

A1
The UAS is airworthy

A

J2
The equipage on-board the UA assists in own-ship detection by other aircraft and by ATC

J

S8
Argument of equipage

S7
Argument by airworthiness assurance

J1
The technical implementation of the avoidance function of the GBDAA capability has an allocation to the UAS, and depends on UAS airworthiness

J

G16
Equipage onboard the UA contributes to avoiding intruder aircraft in the transit corridor by transmitting altitude information

E4
UAS equipage includes a Mode-C altitude encoding transponder

S2
Argument over operator-directed avoidance procedures

C8
Operator directed-avoidance procedures refer to procedures performed by the UA operator, i.e., the PIC or GCSOs

G10
Operator-directed avoidance procedures for UAS operations contribute to acceptably avoiding intruder aircraft

C9
Avoidance procedures apply to non-cooperative GA air traffc

S4
Argument over categories of avoidance procedures

C12
Categories of avoidance procedures: Temporal and Spatial

C11
RADAR detects one more more intruder aircraft in the covered surveillance volume predicted to intercept the transit corridor

G11
Operator-directed avoidance procedures constrain UA flight patterns and airspeed to acceptably avoid intruder aircraft

G15
Operator-directed avoidance procedures restrict UA flight to specific operational windows to acceptably avoid intruder aircraft

C10
No intruder aircraft are detected by RADAR surveillance of the covered threat volume

S6
Argument based on UA location

G13
For entry into the transit corridor, the operating procedures permit entry only when no intruder aircraft are detected by RADAR surveillance of the covered threat volume

G14
For exiting from the transit corridor into international airspace, the operating procedures permit exit when no intruder aircraft are detected by RADAR surveillance of the covered threat volume

E3
Item 3.3.3 (f) of the operating procedures addressing entry into thre transit corridor from International airspace

E1
Item 3.3.3 (c) of the operating procedures addressing entry into the transit corridor

E2
Item 3.3.3 (e) of the operating procedures addressing exit from the transit corridor into international airspace

S5
Argument of applying deconfliction procedures

C13
Deconfliction procedures reflect interactions between UA operators and ATC

G17
Deconfliction procedures for UAS operations contribute to acceptably avoiding intruder aircraft

S9
Argument over airspace deconfliction methods

G18
Deconfliction procedures maintain situational awareness and common operating picture

G19
Deconfliction procedures modify UA flight paths to provide adequate physical separation

S10
Argument by communication and coordination of information regarding UAS operations

J3
Maintaining a common operating picture of the airspace requires communicating and coordinating operational information about UAS operations such as the location of the transit corridor, and the altitude/ duration of UAS operations

J

C14
Other users of the portions of the NAS which overlaps with the surveillance and threat volumes

G22
Deconfliction procedures warn air traffic operating out of nearby airports of UAS operations in the transit corridor

G21
Deconfliction procedures inform nearby aircraft of UA altitude and location during flight in the transit corridor

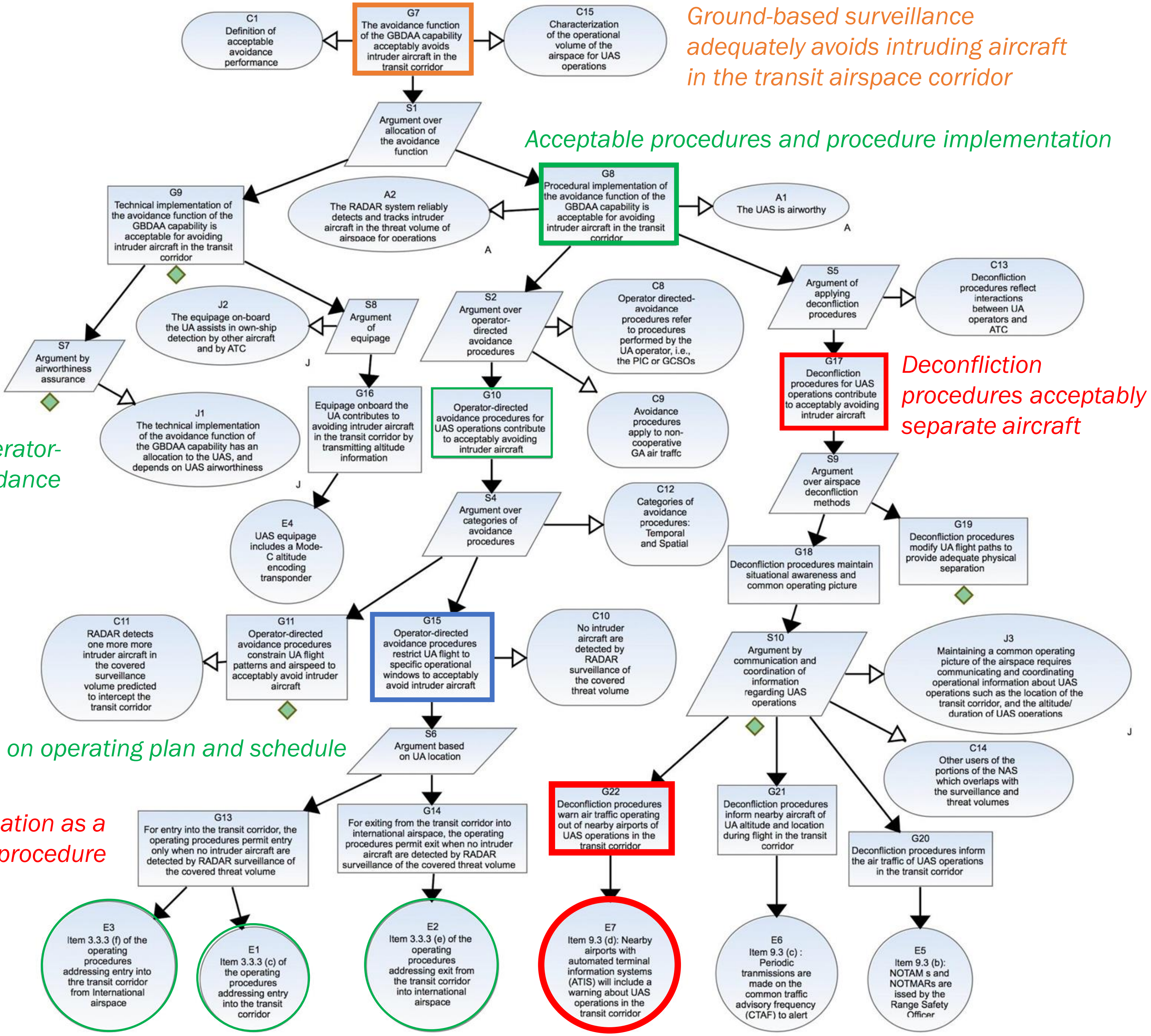
G20
Deconfliction procedures inform the air traffic of UAS operations in the transit corridor

E7
Item 9.3 (d): Nearby airports with automated terminal information systems (ATIS) will include a warning about UAS operations in the transit corridor

E6
Item 9.3 (c) : Periodic tranmissions are made on the common traffic advisory frequency (CTAF) to alert

E5
Item 9.3 (b): NOTAM s and NOTMARs are issed by the Range Safety Officer

Example



Ground-based surveillance adequately avoids intruding aircraft in the transit airspace corridor

C1
Definition of acceptable avoidance performance

G7
The avoidance function of the GBDAA capability acceptably avoids intruder aircraft in the transit corridor

C15
Characterization of the operational volume of the airspace for UAS operations

S1
Argument over allocation of the avoidance function

Acceptable procedures and procedure implementation

G9
Technical implementation of the avoidance function of the GBDAA capability is acceptable for avoiding intruder aircraft in the transit corridor

A2
The RADAR system reliably detects and tracks intruder aircraft in the threat volume of airspace for operations

A

G8
Procedural implementation of the avoidance function of the GBDAA capability is acceptable for avoiding intruder aircraft in the transit corridor

A1
The UAS is airworthy

A

J2
The equipage on-board the UA assists in own-ship detection by other aircraft and by ATC

J

S8
Argument of equipage

S2
Argument over operator-directed avoidance procedures

C8
Operator directed-avoidance procedures refer to procedures performed by the UA operator, i.e., the PIC or GCSOs

S5
Argument of applying deconfliction procedures

C13
Deconfliction procedures reflect interactions between UA operators and ATC

S7
Argument by airworthiness assurance

J1
The technical implementation of the avoidance function of the GBDAA capability has an allocation to the UAS, and depends on UAS airworthiness

J

G16
Equipage onboard the UA contributes to avoiding intruder aircraft in the transit corridor by transmitting altitude information

G10
Operator-directed avoidance procedures for UAS operations contribute to acceptably avoiding intruder aircraft

C9
Avoidance procedures apply to non-cooperative GA air traffc

G17
Deconfliction procedures for UAS operations contribute to acceptably avoiding intruder aircraft

Deconfliction procedures acceptably separate aircraft

Acceptable operator-directed avoidance

E4
UAS equipage includes a Mode-C altitude encoding transponder

S4
Argument over categories of avoidance procedures

C12
Categories of avoidance procedures: Temporal and Spatial

S9
Argument over airspace deconfliction methods

G18
Deconfliction procedures maintain situational awareness and common operating picture

G19
Deconfliction procedures modify UA flight paths to provide adequate physical separation

C11
RADAR detects one more more intruder aircraft in the covered surveillance volume predicted to intercept the transit corridor

G11
Operator-directed avoidance procedures constrain UA flight patterns and airspeed to acceptably avoid intruder aircraft

G15
Operator-directed avoidance procedures restrict UA flight to specific operational windows to acceptably avoid intruder aircraft

C10
No intruder aircraft are detected by RADAR surveillance of the covered threat volume

S10
Argument by communication and coordination of information regarding UAS operations

J3
Maintaining a common operating picture of the airspace requires communicating and coordinating operational information about UAS operations such as the location of the transit corridor, and the altitude/ duration of UAS operations

J

Constraints on operating plan and schedule

S6
Argument based on UA location

C14
Other users of the portions of the NAS which overlaps with the surveillance and threat volumes

Air traffic radio communication as a deconfliction procedure

G13
For entry into the transit corridor, the operating procedures permit entry only when no intruder aircraft are detected by RADAR surveillance of the covered threat volume

G14
For exiting from the transit corridor into international airspace, the operating procedures permit exit when no intruder aircraft are detected by RADAR surveillance of the covered threat volume

G22
Deconfliction procedures warn air traffic operating out of nearby airports of UAS operations in the transit corridor

G21
Deconfliction procedures inform nearby aircraft of UA altitude and location during flight in the transit corridor

G20
Deconfliction procedures inform the air traffic of UAS operations in the transit corridor

E3
Item 3.3.3 (f) of the operating procedures addressing entry into thre transit corridor from International airspace

E1
Item 3.3.3 (c) of the operating procedures addressing entry into the transit corridor

E2
Item 3.3.3 (e) of the operating procedures addressing exit from the transit corridor into international airspace

E7
Item 9.3 (d): Nearby airports with automated terminal information systems (ATIS) will include a warning about UAS operations in the transit corridor

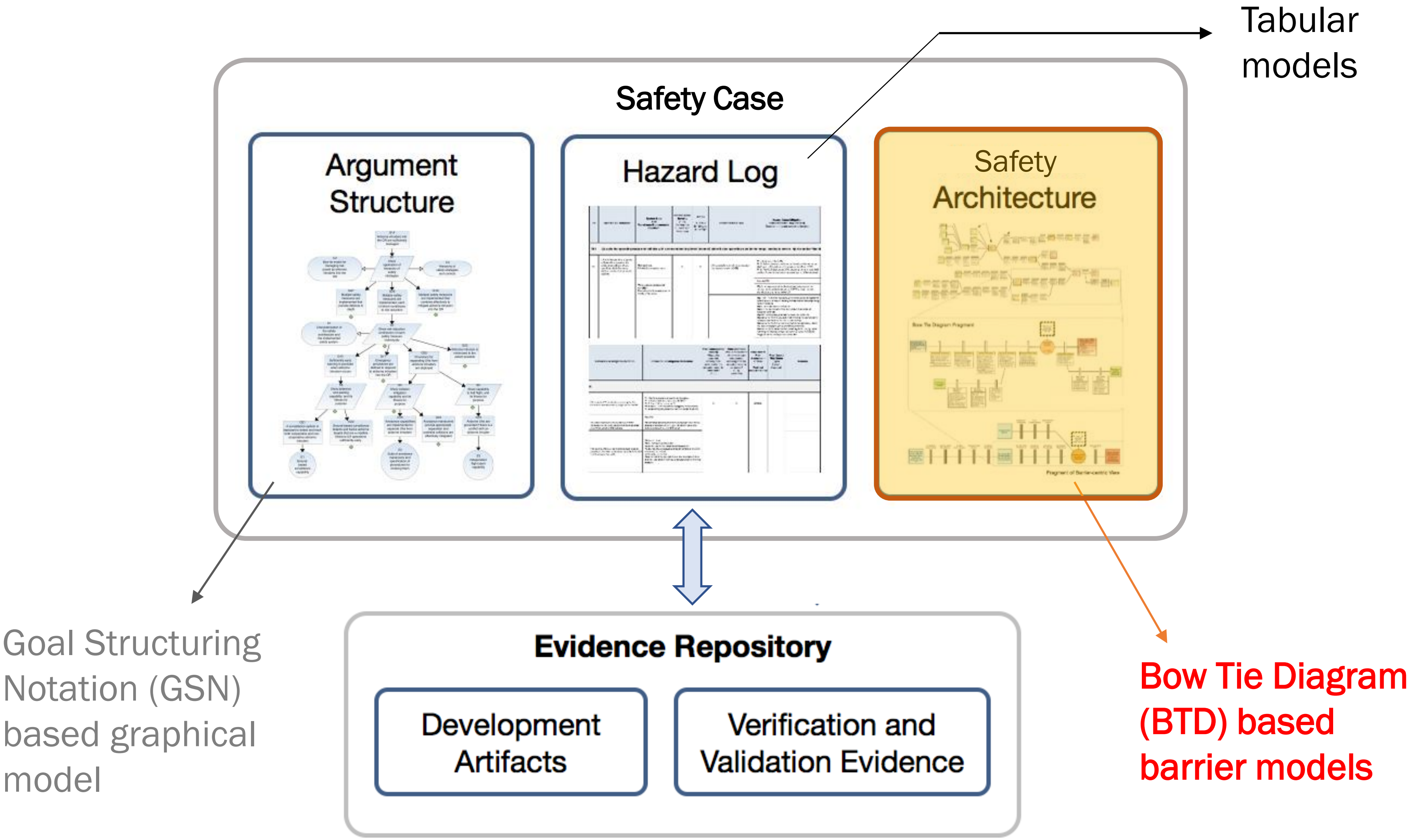
E6
Item 9.3 (c) : Periodic tranmissions are made on the common traffic advisory frequency (CTAF) to alert

E5
Item 9.3 (b): NOTAM s and NOTMARs are issed by the Range Safety Officer

Concrete operating procedures

ATIS system

Models & Notations



Tabular models

Safety Case

Argument Structure

Hazard Log

Safety Architecture

Goal Structuring Notation (GSN) based graphical model

Evidence Repository

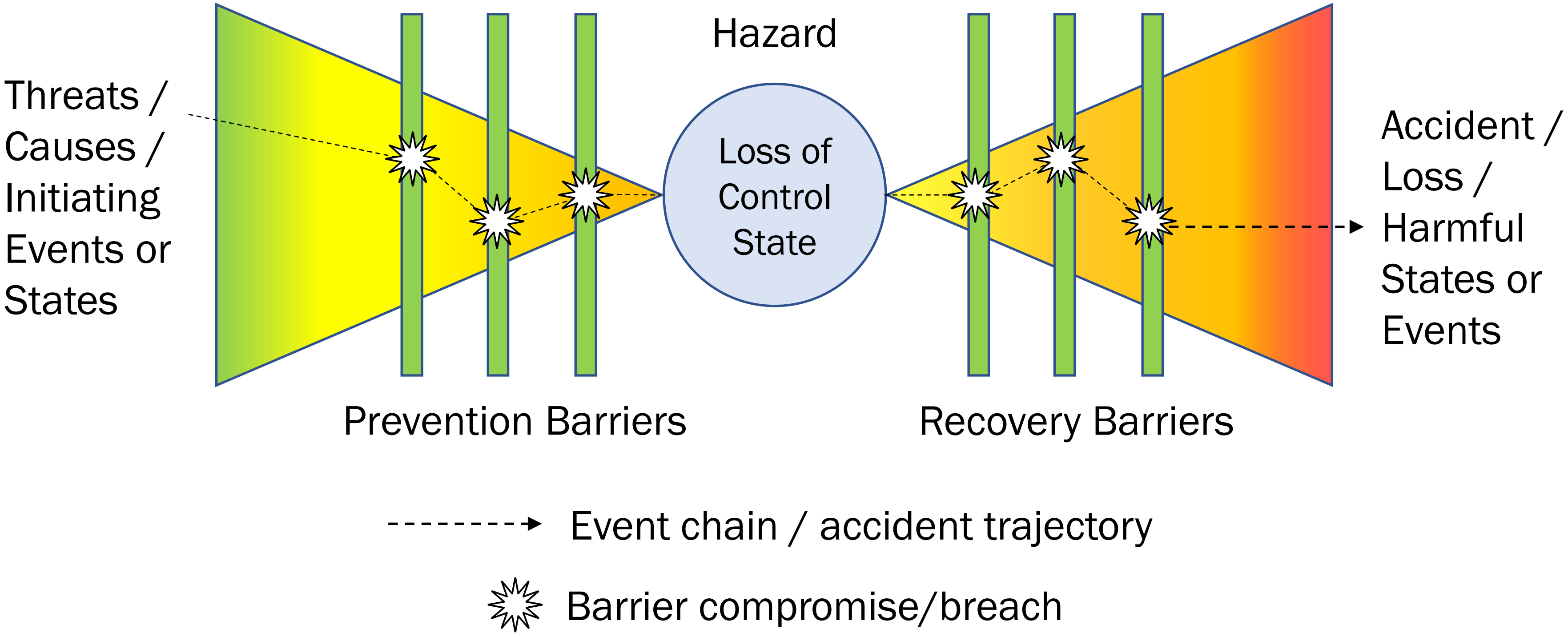
Development Artifacts

Verification and Validation Evidence

Bow Tie Diagram (BTD) based barrier models

Barrier Models

- Scenario-based, event-chain model of risk



Threats / Causes / Initiating Events or States

Hazard

Loss of Control State

Accident / Loss / Harmful States or Events

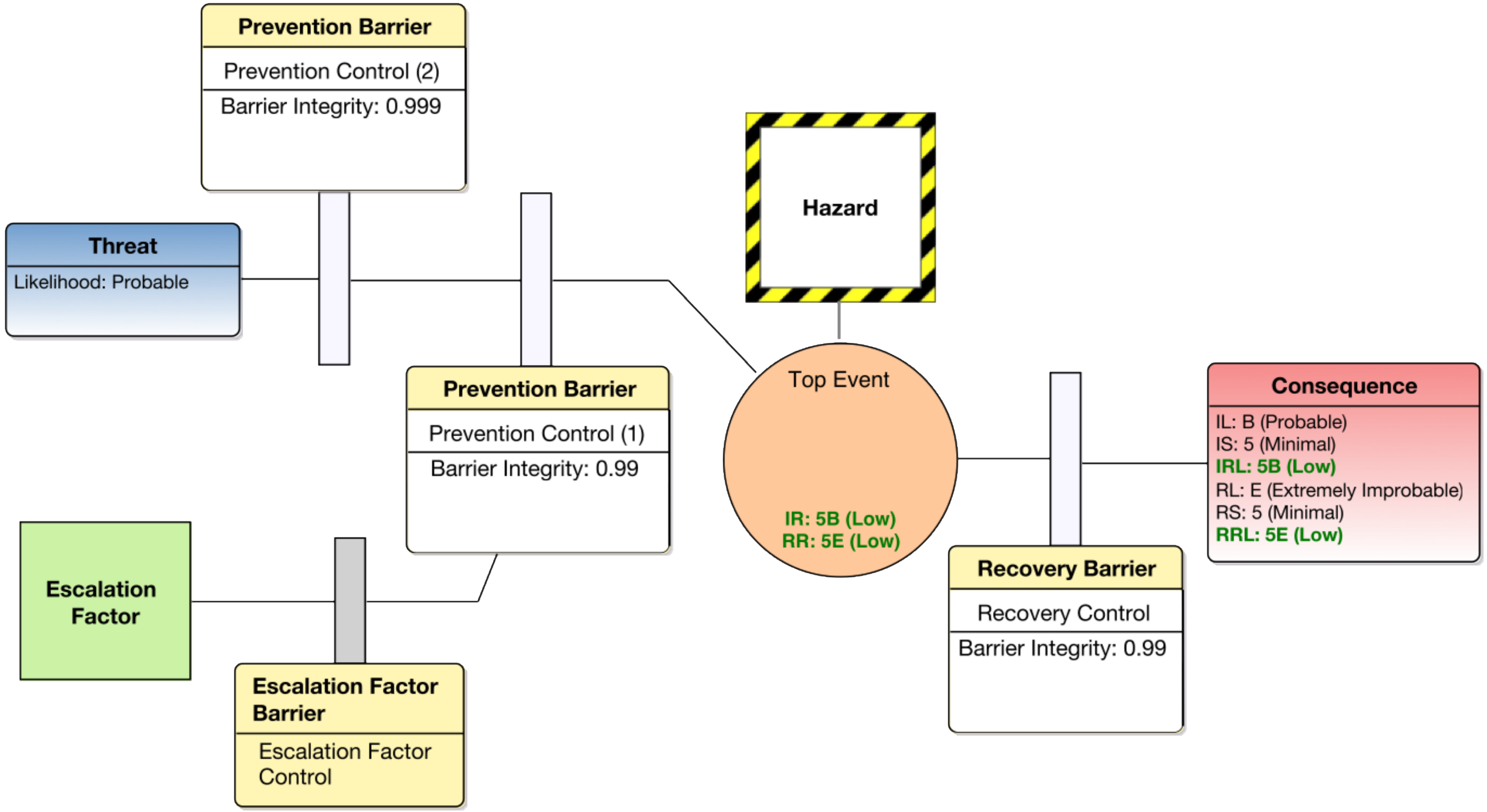
Prevention Barriers

Recovery Barriers

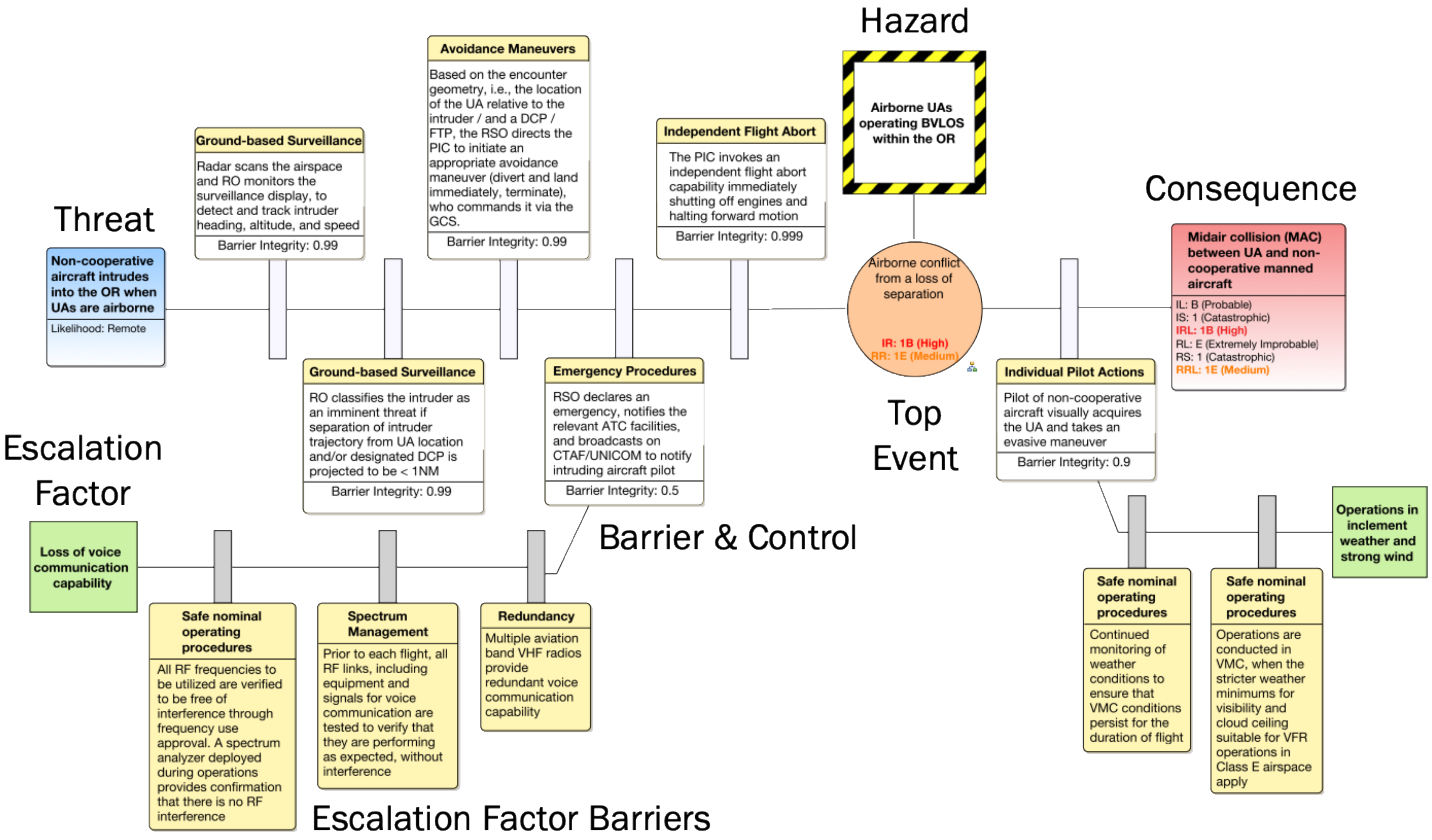
- - - - - - - -→ Event chain / accident trajectory

✸ Barrier compromise/breach

Bow Tie Diagrams



Example Bow Tie Diagram – Loss of Separation



Hazard

Airborne UAs operating BVLOS within the OR

Threat

Non-cooperative aircraft intrudes into the OR when UAs are airborne

Likelihood: Remote

Ground-based Surveillance

Radar scans the airspace and RO monitors the surveillance display, to detect and track intruder heading, altitude, and speed

Barrier Integrity: 0.99

Ground-based Surveillance

RO classifies the intruder as an imminent threat if separation of intruder trajectory from UA location and/or designated DCP is projected to be < 1NM

Barrier Integrity: 0.99

Avoidance Maneuvers

Based on the encounter geometry, i.e., the location of the UA relative to the intruder / and a DCP / FTP, the RSO directs the PIC to initiate an appropriate avoidance maneuver (divert and land immediately, terminate), who commands it via the GCS.

Barrier Integrity: 0.99

Emergency Procedures

RSO declares an emergency, notifies the relevant ATC facilities, and broadcasts on CTAF/UNICOM to notify intruding aircraft pilot

Barrier Integrity: 0.5

Independent Flight Abort

The PIC invokes an independent flight abort capability immediately shutting off engines and halting forward motion

Barrier Integrity: 0.999

Airborne conflict from a loss of separation

IR: 1B (High)
RR: 1E (Medium)

Top Event

Individual Pilot Actions

Pilot of non-cooperative aircraft visually acquires the UA and takes an evasive maneuver

Barrier Integrity: 0.9

Consequence

Midair collision (MAC) between UA and non-cooperative manned aircraft

IL: B (Probable)
IS: 1 (Catastrophic)
IRL: 1B (High)
RL: E (Extremely Improbable)
RS: 1 (Catastrophic)
RRL: 1E (Medium)

Escalation Factor

Loss of voice communication capability

Safe nominal operating procedures

All RF frequencies to be utilized are verified to be free of interference through frequency use approval. A spectrum analyzer deployed during operations provides confirmation that there is no RF interference

Spectrum Management

Prior to each flight, all RF links, including equipment and signals for voice communication are tested to verify that they are performing as expected, without interference

Redundancy

Multiple aviation band VHF radios provide redundant voice communication capability

Barrier & Control

Escalation Factor Barriers

Safe nominal operating procedures

Continued monitoring of weather conditions to ensure that VMC conditions persist for the duration of flight

Safe nominal operating procedures

Operations are conducted in VMC, when the stricter weather minimums for visibility and cloud ceiling suitable for VFR operations in Class E airspace apply

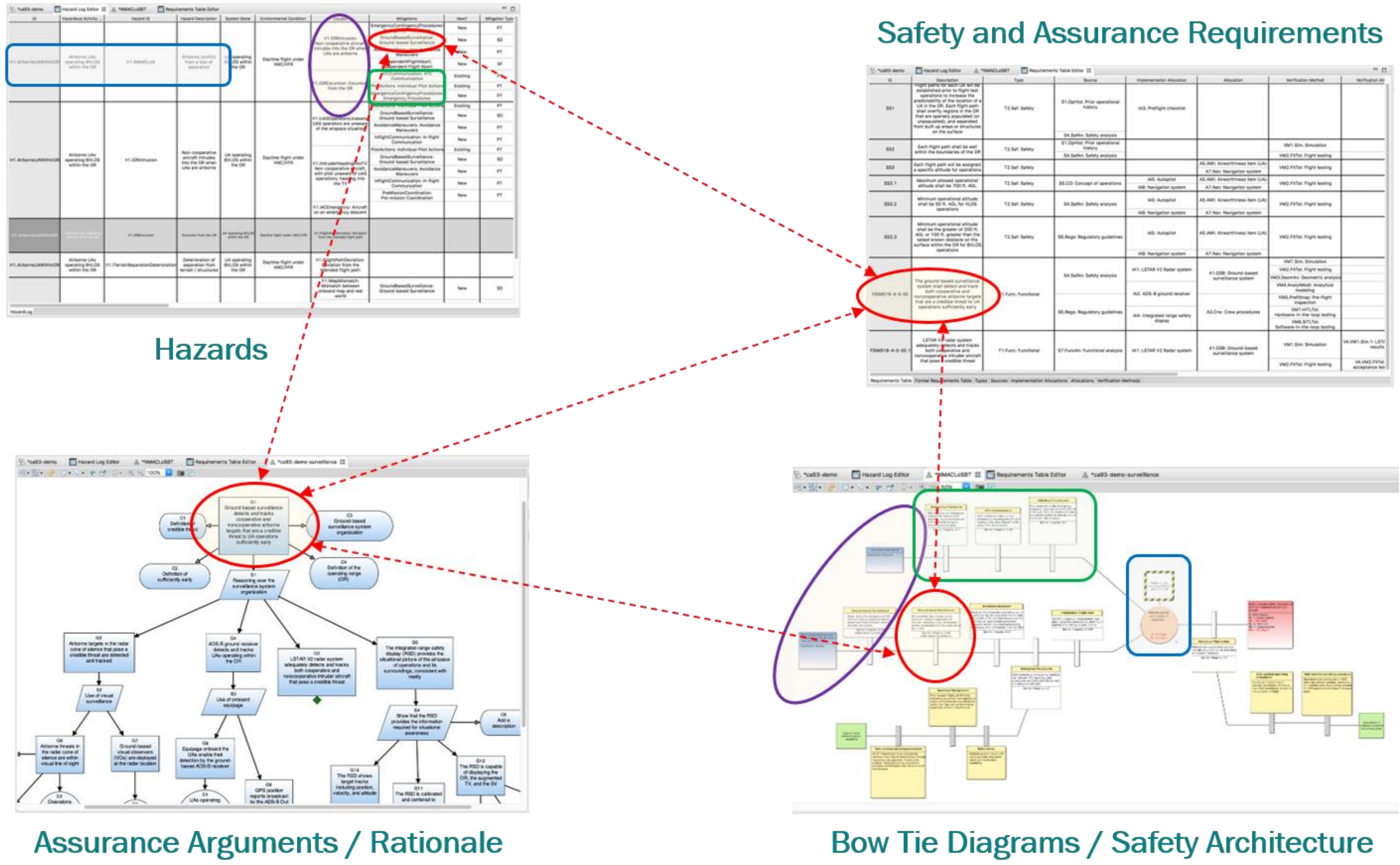
Operations in inclement weather and strong wind

Risk Analysis with Barrier Models

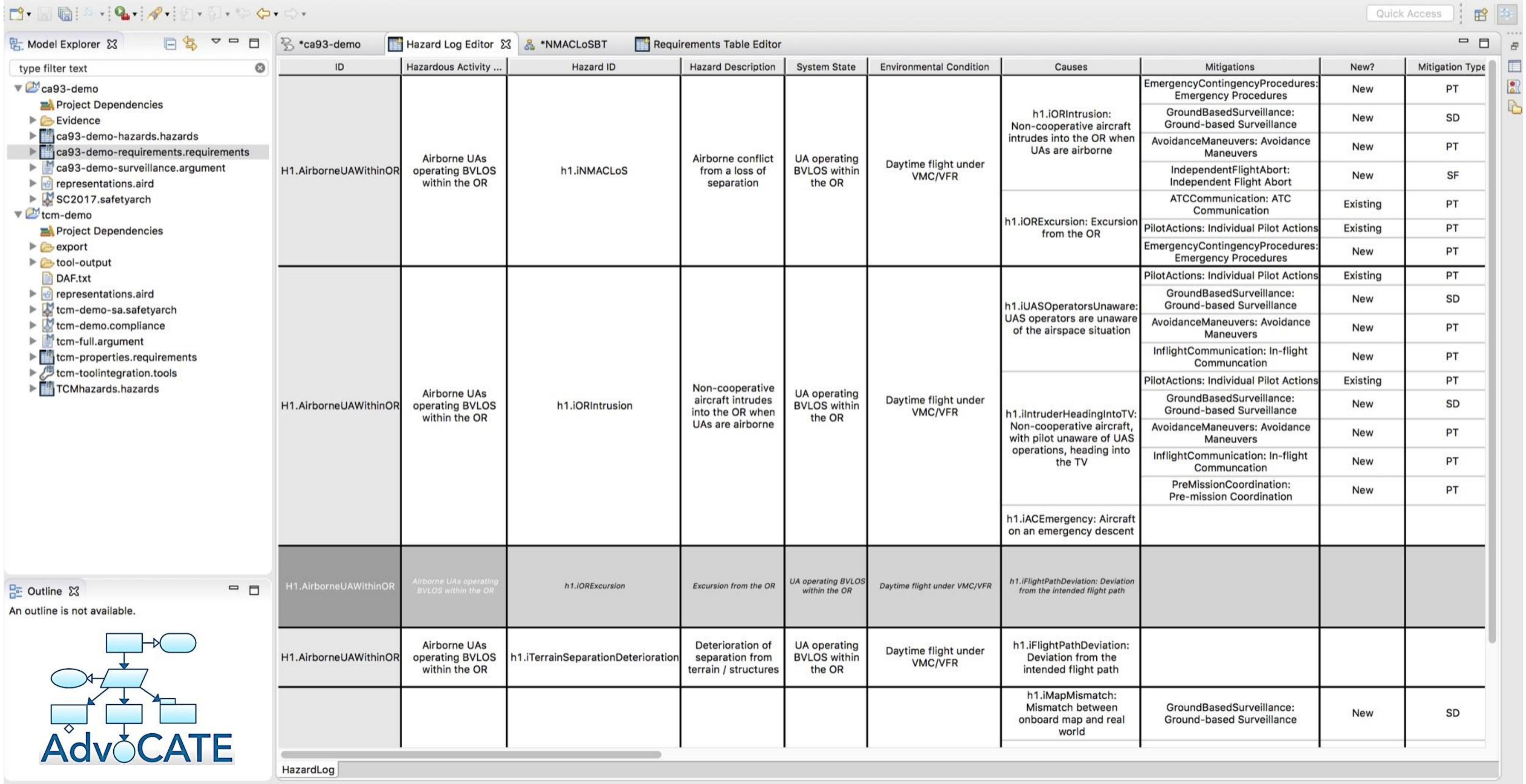
- Concepts of barrier and control *integrity*
  - Probability that barrier performs the required safety function (under all stated conditions, within a stated time)
  - Equivalent to reliability if all barrier/control functionality impacts safety
- Risk computation
  - Path probability as joint probability of events on a path
    - Threats, barrier breach events
  - Probability of an event with multiple source paths using inclusion-exclusion principle
  - Probability propagation from threat to consequence
- Assumptions
  - Both barriers and constituent controls assumed (designed) to be independent (in their failures)
  - Threats are independent
  - P(Top event | Threat, No Barrier) = 1
- Severity propagation from consequence to threat
  - Worst-case severity considered
- Risk as a combination of probability and severity → Risk Matrix
  - Risk levels for events selected from risk matrix

AdvoCATE: Assurance Case Automation Toolset

- Hazard analysis and risk assessment
- Safety and assurance requirements capture
- Structured argument development
- Safety architecture development
- Evidence management
- Measures, metrics, indicators
- Traceability and consistency


Safety and Assurance Requirements
Hazards
Assurance Arguments / Rationale
Bow Tie Diagrams / Safety Architecture

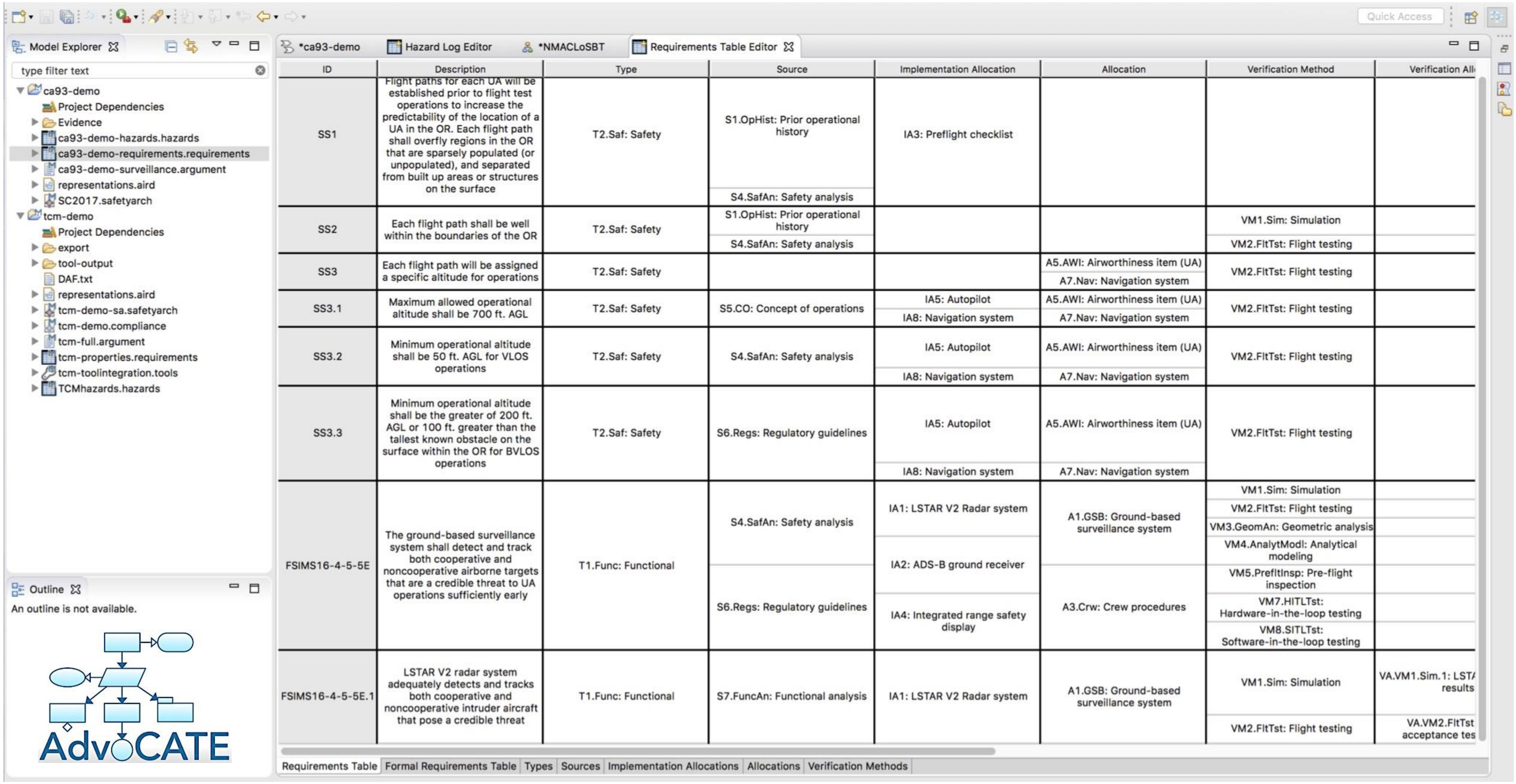
Hazard Log



An outline is not available.

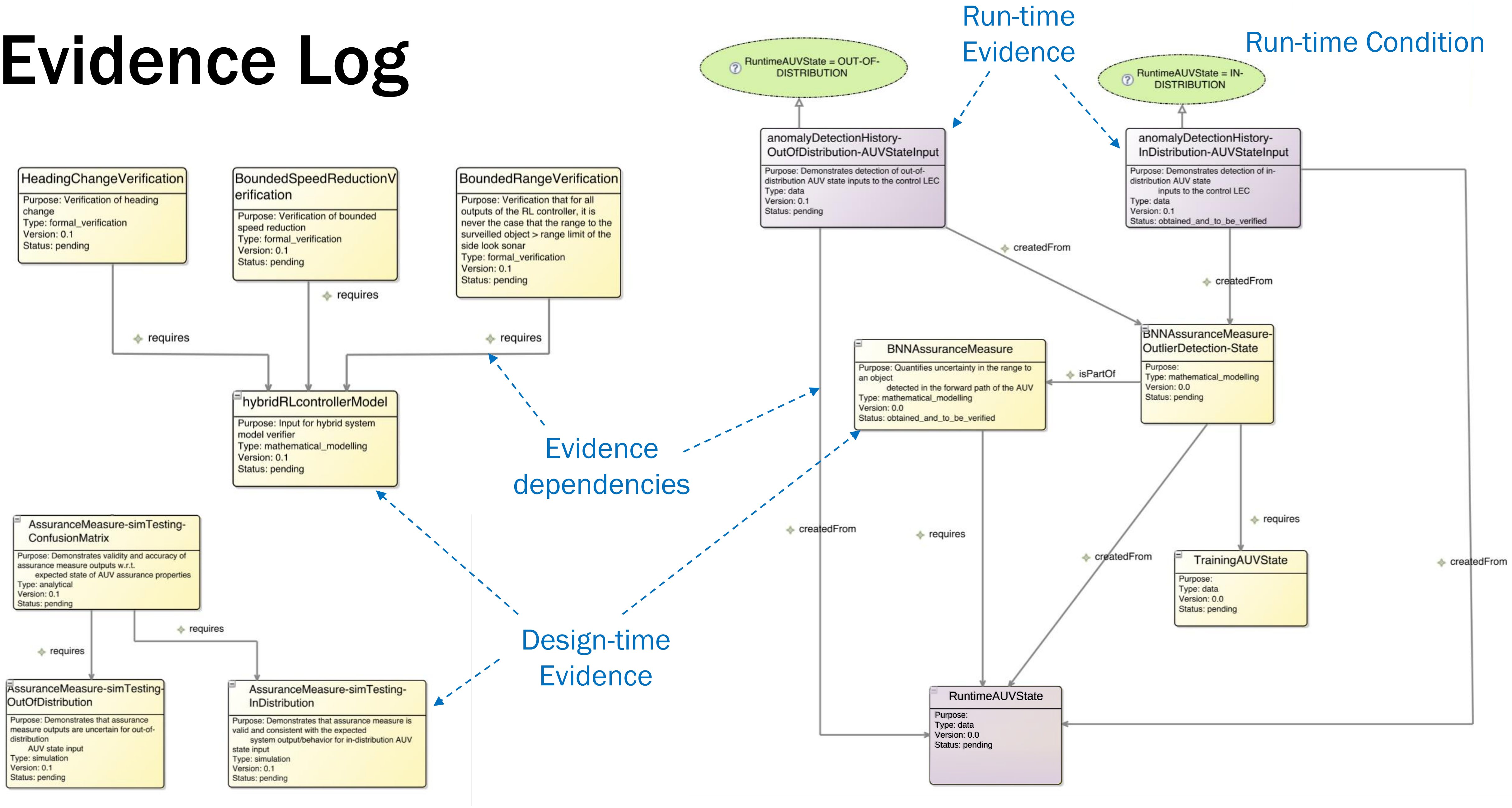
ID	Hazardous Activity ...	Hazard ID	Hazard Description	System State	Environmental Condition	Causes	Mitigations	New?	Mitigation Type
H1.AirborneUAWithinOR	Airborne UAs operating BVLOS within the OR	h1.iNMACLoS	Airborne conflict from a loss of separation	UA operating BVLOS within the OR	Daytime flight under VMC/VFR	h1.iORIntrusion: Non-cooperative aircraft intrudes into the OR when UAs are airborne	EmergencyContingencyProcedures: Emergency Procedures	New	PT
							GroundBasedSurveillance: Ground-based Surveillance	New	SD
							AvoidanceManeuvers: Avoidance Maneuvers	New	PT
							IndependentFlightAbort: Independent Flight Abort	New	SF
						h1.iORExcursion: Excursion from the OR	ATCCommunication: ATC Communication	Existing	PT
							PilotActions: Individual Pilot Actions	Existing	PT
							EmergencyContingencyProcedures: Emergency Procedures	New	PT
H1.AirborneUAWithinOR	Airborne UAs operating BVLOS within the OR	h1.iORIntrusion	Non-cooperative aircraft intrudes into the OR when UAs are airborne	UA operating BVLOS within the OR	Daytime flight under VMC/VFR	h1.iUASOperatorsUnaware: UAS operators are unaware of the airspace situation	PilotActions: Individual Pilot Actions	Existing	PT
							GroundBasedSurveillance: Ground-based Surveillance	New	SD
							AvoidanceManeuvers: Avoidance Maneuvers	New	PT
							InflightCommunication: In-flight Communication	New	PT
						h1.iIntruderHeadingIntoTV: Non-cooperative aircraft, with pilot unaware of UAS operations, heading into the TV	PilotActions: Individual Pilot Actions	Existing	PT
							GroundBasedSurveillance: Ground-based Surveillance	New	SD
							AvoidanceManeuvers: Avoidance Maneuvers	New	PT
							InflightCommunication: In-flight Communication	New	PT
							PreMissionCoordination: Pre-mission Coordination	New	PT
						h1.iACEmergency: Aircraft on an emergency descent			
H1.AirborneUAWithinOR	*Airborne UAs operating BVLOS within the OR*	*h1.iORExcursion*	*Excursion from the OR*	*UA operating BVLOS within the OR*	*Daytime flight under VMC/VFR*	*h1.iFlightPathDeviation: Deviation from the intended flight path*			
H1.AirborneUAWithinOR	Airborne UAs operating BVLOS within the OR	h1.iTerrainSeparationDeterioration	Deterioration of separation from terrain / structures	UA operating BVLOS within the OR	Daytime flight under VMC/VFR	h1.iFlightPathDeviation: Deviation from the intended flight path			
						h1.iMapMismatch: Mismatch between onboard map and real world	GroundBasedSurveillance: Ground-based Surveillance	New	SD

Requirements Log



ID	Description	Type	Source	Implementation Allocation	Allocation	Verification Method	Verification All
SS1	Flight paths for each UA will be established prior to flight test operations to increase the predictability of the location of a UA in the OR. Each flight path shall overfly regions in the OR that are sparsely populated (or unpopulated), and separated from built up areas or structures on the surface	T2.Saf: Safety	S1.OpHist: Prior operational history S4.SafAn: Safety analysis	IA3: Preflight checklist			
SS2	Each flight path shall be well within the boundaries of the OR	T2.Saf: Safety	S1.OpHist: Prior operational history S4.SafAn: Safety analysis			VM1.Sim: Simulation VM2.FltTst: Flight testing	
SS3	Each flight path will be assigned a specific altitude for operations	T2.Saf: Safety			A5.AWI: Airworthiness item (UA) A7.Nav: Navigation system	VM2.FltTst: Flight testing	
SS3.1	Maximum allowed operational altitude shall be 700 ft. AGL	T2.Saf: Safety	S5.CO: Concept of operations	IA5: Autopilot IA8: Navigation system	A5.AWI: Airworthiness item (UA) A7.Nav: Navigation system	VM2.FltTst: Flight testing	
SS3.2	Minimum operational altitude shall be 50 ft. AGL for VLOS operations	T2.Saf: Safety	S4.SafAn: Safety analysis	IA5: Autopilot IA8: Navigation system	A5.AWI: Airworthiness item (UA) A7.Nav: Navigation system	VM2.FltTst: Flight testing	
SS3.3	Minimum operational altitude shall be the greater of 200 ft. AGL or 100 ft. greater than the tallest known obstacle on the surface within the OR for BVLOS operations	T2.Saf: Safety	S6.Regs: Regulatory guidelines	IA5: Autopilot IA8: Navigation system	A5.AWI: Airworthiness item (UA) A7.Nav: Navigation system	VM2.FltTst: Flight testing	
FSIMS16-4-5-5E	The ground-based surveillance system shall detect and track both cooperative and noncooperative airborne targets that are a credible threat to UA operations sufficiently early	T1.Func: Functional	S4.SafAn: Safety analysis S6.Regs: Regulatory guidelines	IA1: LSTAR V2 Radar system IA2: ADS-B ground receiver IA4: Integrated range safety display	A1.GSB: Ground-based surveillance system A3.Crw: Crew procedures	VM1.Sim: Simulation VM2.FltTst: Flight testing VM3.GeomAn: Geometric analysis VM4.AnalytModl: Analytical modeling VM5.PrefltInsp: Pre-flight inspection VM7.HITLTst: Hardware-in-the-loop testing VM8.SITLTst: Software-in-the-loop testing	
FSIMS16-4-5-5E.1	LSTAR V2 radar system adequately detects and tracks both cooperative and noncooperative intruder aircraft that pose a credible threat	T1.Func: Functional	S7.FuncAn: Functional analysis	IA1: LSTAR V2 Radar system	A1.GSB: Ground-based surveillance system	VM1.Sim: Simulation VM2.FltTst: Flight testing	VA.VM1.Sim.1: LST results VA.VM2.FltTst acceptance tes

Evidence Log



Run-time Evidence

Run-time Condition

RuntimeAUVState = OUT-OF-DISTRIBUTION

RuntimeAUVState = IN-DISTRIBUTION

anomalyDetectionHistory-OutOfDistribution-AUVStateInput
Purpose: Demonstrates detection of out-of-distribution AUV state inputs to the control LEC
Type: data
Version: 0.1
Status: pending

anomalyDetectionHistory-InDistribution-AUVStateInput
Purpose: Demonstrates detection of in-distribution AUV state inputs to the control LEC
Type: data
Version: 0.1
Status: obtained_and_to_be_verified

HeadingChangeVerification
Purpose: Verification of heading change
Type: formal_verification
Version: 0.1
Status: pending

BoundedSpeedReductionVerification
Purpose: Verification of bounded speed reduction
Type: formal_verification
Version: 0.1
Status: pending

BoundedRangeVerification
Purpose: Verification that for all outputs of the RL controller, it is never the case that the range to the surveilled object > range limit of the side look sonar
Type: formal_verification
Version: 0.1
Status: pending

hybridRLcontrollerModel
Purpose: Input for hybrid system model verifier
Type: mathematical_modelling
Version: 0.1
Status: pending

BNNAssuranceMeasure
Purpose: Quantifies uncertainty in the range to an object detected in the forward path of the AUV
Type: mathematical_modelling
Version: 0.0
Status: obtained_and_to_be_verified

BNNAssuranceMeasure-OutlierDetection-State
Purpose:
Type: mathematical_modelling
Version: 0.0
Status: pending

TrainingAUVState
Purpose:
Type: data
Version: 0.0
Status: pending

RuntimeAUVState
Purpose:
Type: data
Version: 0.0
Status: pending

AssuranceMeasure-simTesting-ConfusionMatrix
Purpose: Demonstrates validity and accuracy of assurance measure outputs w.r.t. expected state of AUV assurance properties
Type: analytical
Version: 0.1
Status: pending

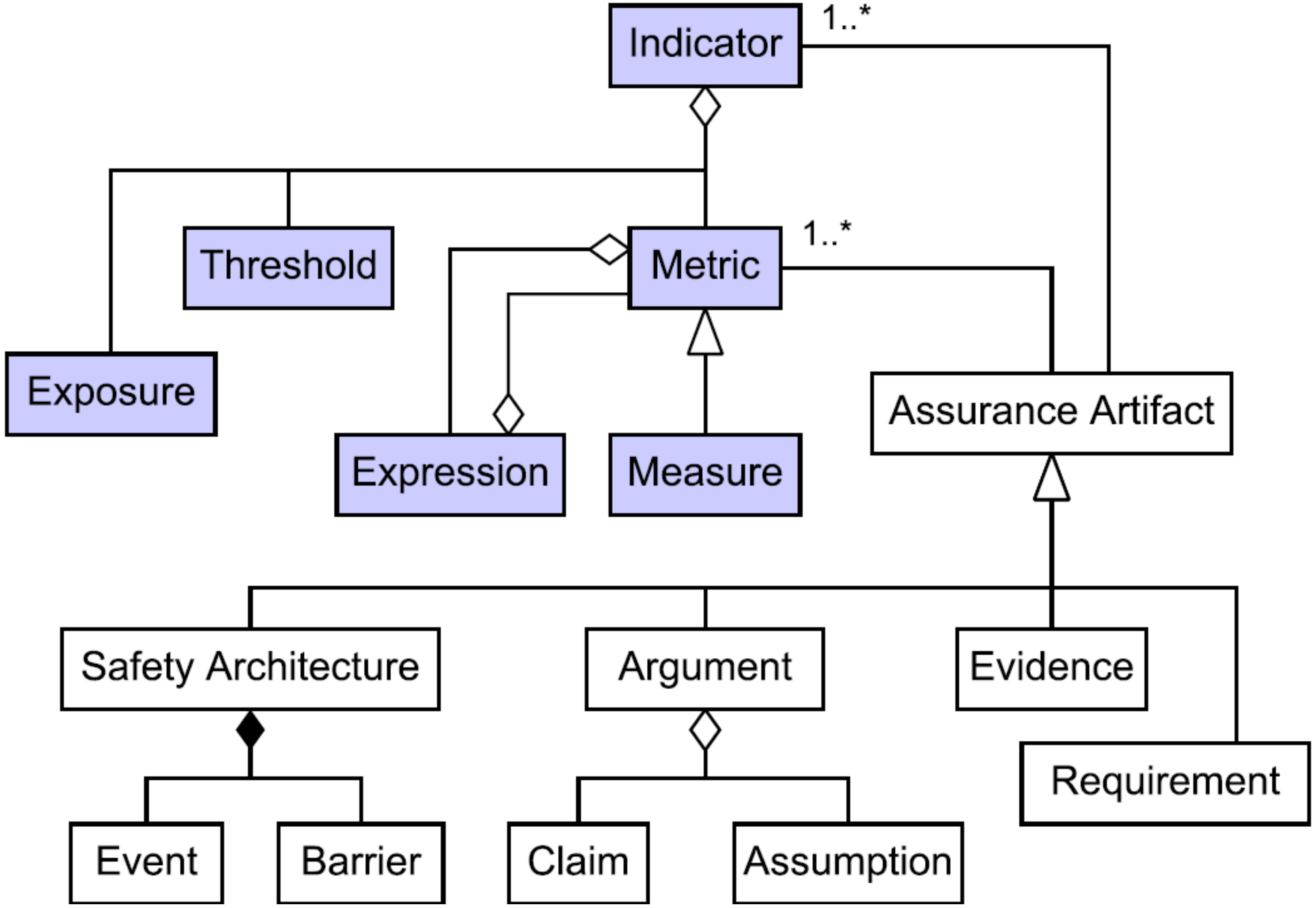
AssuranceMeasure-simTesting-OutOfDistribution
Purpose: Demonstrates that assurance measure outputs are uncertain for out-of-distribution AUV state input
Type: simulation
Version: 0.1
Status: pending

AssuranceMeasure-simTesting-InDistribution
Purpose: Demonstrates that assurance measure is valid and consistent with the expected system output/behavior for in-distribution AUV state input
Type: simulation
Version: 0.1
Status: pending

Evidence dependencies

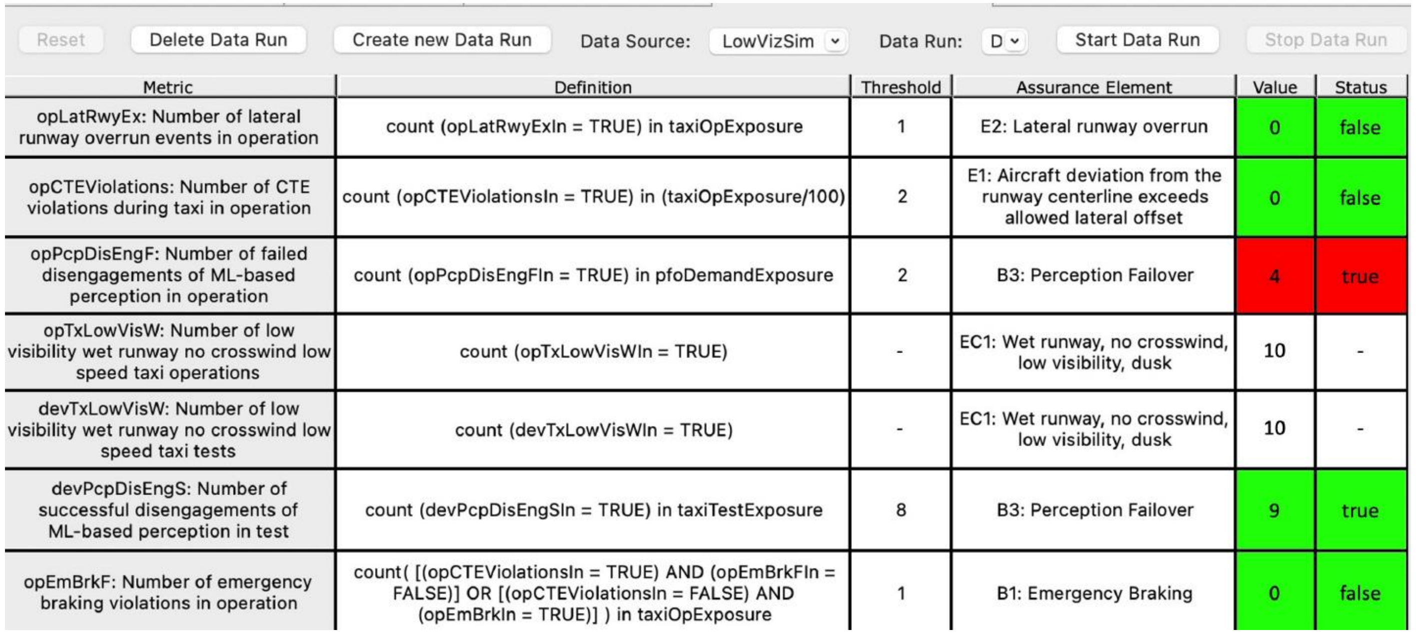
Design-time Evidence

Measures, Metrics, and Performance Indicators



- Measures: Directly observable parameters of the system or environment
- Metrics: Computed value based on measures and other metrics
- Indicator: Target value that a metric reaches in a given duration
  - Safety performance indicators

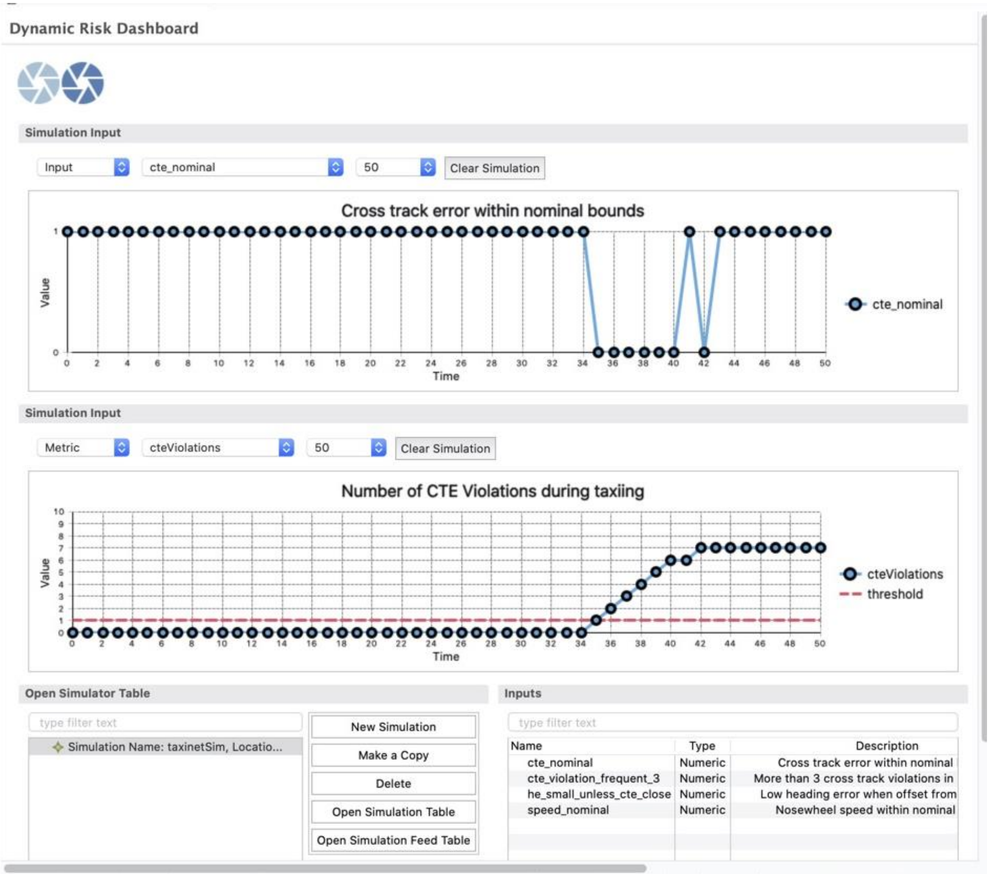
Visualization of Metrics and Indicators



Reset | Delete Data Run | Create new Data Run | Data Source: LowVizSim | Data Run: D | Start Data Run | Stop Data Run

Metric	Definition	Threshold	Assurance Element	Value	Status
opLatRwyEx: Number of lateral runway overrun events in operation	count (opLatRwyExIn = TRUE) in taxiOpExposure	1	E2: Lateral runway overrun	0	false
opCTEViolations: Number of CTE violations during taxi in operation	count (opCTEViolationsIn = TRUE) in (taxiOpExposure/100)	2	E1: Aircraft deviation from the runway centerline exceeds allowed lateral offset	0	false
opPcpDisEngF: Number of failed disengagements of ML-based perception in operation	count (opPcpDisEngFIn = TRUE) in pfoDemandExposure	2	B3: Perception Failover	4	true
opTxLowVisW: Number of low visibility wet runway no crosswind low speed taxi operations	count (opTxLowVisWIn = TRUE)	-	EC1: Wet runway, no crosswind, low visibility, dusk	10	-
devTxLowVisW: Number of low visibility wet runway no crosswind low speed taxi tests	count (devTxLowVisWIn = TRUE)	-	EC1: Wet runway, no crosswind, low visibility, dusk	10	-
devPcpDisEngS: Number of successful disengagements of ML-based perception in test	count (devPcpDisEngSIn = TRUE) in taxiTestExposure	8	B3: Perception Failover	9	true
opEmBrkF: Number of emergency braking violations in operation	count([(opCTEViolationsIn = TRUE) AND (opEmBrkFIn = FALSE)] OR [(opCTEViolationsIn = FALSE) AND (opEmBrkIn = TRUE)]) in taxiOpExposure	1	B1: Emergency Braking	0	false

Performance indicators table



Dynamic Risk Dashboard

Simulation Input

Input | cte_nominal | 50 | Clear Simulation

Simulation Input

Metric | cteViolations | 50 | Clear Simulation

Open Simulator Table

type filter text

Simulation Name: taxinetSim, Locatio...

Inputs

type filter text

Name	Type	Description
cte_nominal	Numeric	Cross track error within nominal
cte_violation_frequent_3	Numeric	More than 3 cross track violations in
he_small_unless_cte_close	Numeric	Low heading error when offset from
speed_nominal	Numeric	Nosewheel speed within nominal

Metrics Visualization, connected to Simulations

Conclusions

- Development of end-to-end assurance methodology and tool support
- Core assurance case concepts
  - Argumentation
  - Hazard analysis
  - Requirements
  - Barrier models
- Closing the loop between design and operations
  - Monitor indicators during design and operations
  - Maintain consistency of (dynamic) indicators and (static) arguments
  - Generate tasks: update/review

- Advanced assurance case concepts
  - Ontology integration
  - Queries, views
  - Pattern instantiation and composition
  - Round-trip engineering
- Model-based mission assurance
  - Collaborative development and review
  - Version control
  - RESTful API: add, modify, query
    - ▸ Synchronization with evidence/external artifacts
    - ▸ External tool integration: import/export