STINGER GHAFFARIAN TECHNOLOGIES

Technology and Tool Development to Support Safety and Mission Assurance

Ewen Denney and **Ganesh Pai**

ISRDS 2
SGT Technology Day, Houston, TX
Oct. 30, 2017

Summary

STINGER GHAFFARIAN TECHNOLOGIES

- How we are (and have been)
  - Defining the state of the art
    - Foundational research in assurance technology
  - Pushing the state of the practice
    - Application of research to enable application of emerging technologies
    - Unmanned aircraft systems (UAS) missions
  - Developing supporting tools and technologies
    - AdvoCATE (Assurance Case Automation Toolset)
    - Proven application in unmanned aircraft systems (UAS) missions

Outline

STINGER GHAFFARIAN TECHNOLOGIES

- Motivation
- Assurance Cases
- Example
- Tool support
- Outlook

Outline

STINGER GHAFFARIAN TECHNOLOGIES

- **Motivation**
- Assurance Cases
- Example
- Tool Support
- Outlook

Research Motivation

STINGER GHAFFARIAN TECHNOLOGIES

- High-hazard industries are moving to *active safety management*
  - Safety management system (SMS) in aviation
  - Need to
    - Unify reasoning about technical aspects of safety
    - Support safety-related decision making

- *Goals-based* regulation is attractive for novel applications
  - When performance standards are absent
    - Unmanned aircraft systems (UAS), Autonomous systems, …
  - Increases flexibility for regulated entity
  - Evidence-based assurance → *safety case*

Foundational research in languages, methodology, and automation support

Practical Motivation

STINGER GHAFFARIAN TECHNOLOGIES

- MIZOPEX (2013)
  - NASA Earth science mission with Sierra UAS off Alaska coast
  - Flight in combination of US National Airspace + Oceanic Airspace
  - Use of air defense radar for detect and avoid
  - Project needed FAA approval through submission of *safety case* – a detailed safety justification
- UTM (2016 – Ongoing)
  - Fleet of small UAS demonstrating low-altitude traffic management system
  - Flight in US national airspace, over sparsely populated land
  - Use of ground-based radar for detect and avoid
  - Project needed FAA approval through submission of *safety case*

Practical application of our research solutions
in response to customer needs

Outline

STINGER GHAFFARIAN TECHNOLOGIES

- Motivation
- **Assurance Cases**
- Example
- Tool support
- Outlook

Safety Case

STINGER GHAFFARIAN TECHNOLOGIES

‘A safety case is a structured argument, supported by a body of evidence, that provides a compelling, comprehensible and valid case that a system is safe for a given application in a given operating environment’

- *UK MOD, DS-00-56 Issue 4* (*2007*)

- Essentially, a *safety risk management artifact*
  - Other compatible definitions and guidance on content
    - Based on application domain, standard, regulatory paradigm, etc.
      - FAA: Order 8900.1, FSIMS, vol. 16, UAS
      - NAVAIR: Instruction 13034.4
      - ICAO and Eurocontrol: Safety case development manual
      - Automotive: ISO 26262
      - FDA: Infusion pumps total product lifecycle guidance

Safety Case Content

STINGER GHAFFARIAN TECHNOLOGIES

- FAA (8900.1, FSIMS, vol. 16, UAS)
  - Core content
    - Environment (airspace system) description
    - System description and system change description
    - Airworthiness description of affected items
    - Aircraft capabilities and flight data
    - Accident / incident data
    - Pilot / crew roles and responsibilities
    - Hazard analysis and details of risk analysis, risk assessment, and risk control
    - Emergency and contingency procedures
  - Safety risk management plan
    - Hazard tracking and treatment
    - Safety performance monitoring

Safety Case Content

STINGER GHAFFARIAN TECHNOLOGIES

- In general,
  - 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
- Additionally,
  - *Safety architecture* providing a *risk basis*
  - Hazard log and hazard analyses
  - Evidence model
  - Monitoring and update

Assurance Cases

STINGER GHAFFARIAN TECHNOLOGIES

‘A documented body of evidence that provides a convincing and valid argument that a specified set of **critical claims regarding a system’s properties** are adequately justified for a given application in a given environment’

- *MITRE* (*2005*)

‘A reasoned and compelling argument, supported by a body of evidence, that a **system, service, or organization, will operate as intended** for a defined application, in a defined environment’

- *Goal Structuring Notation Standard* (*2011*)

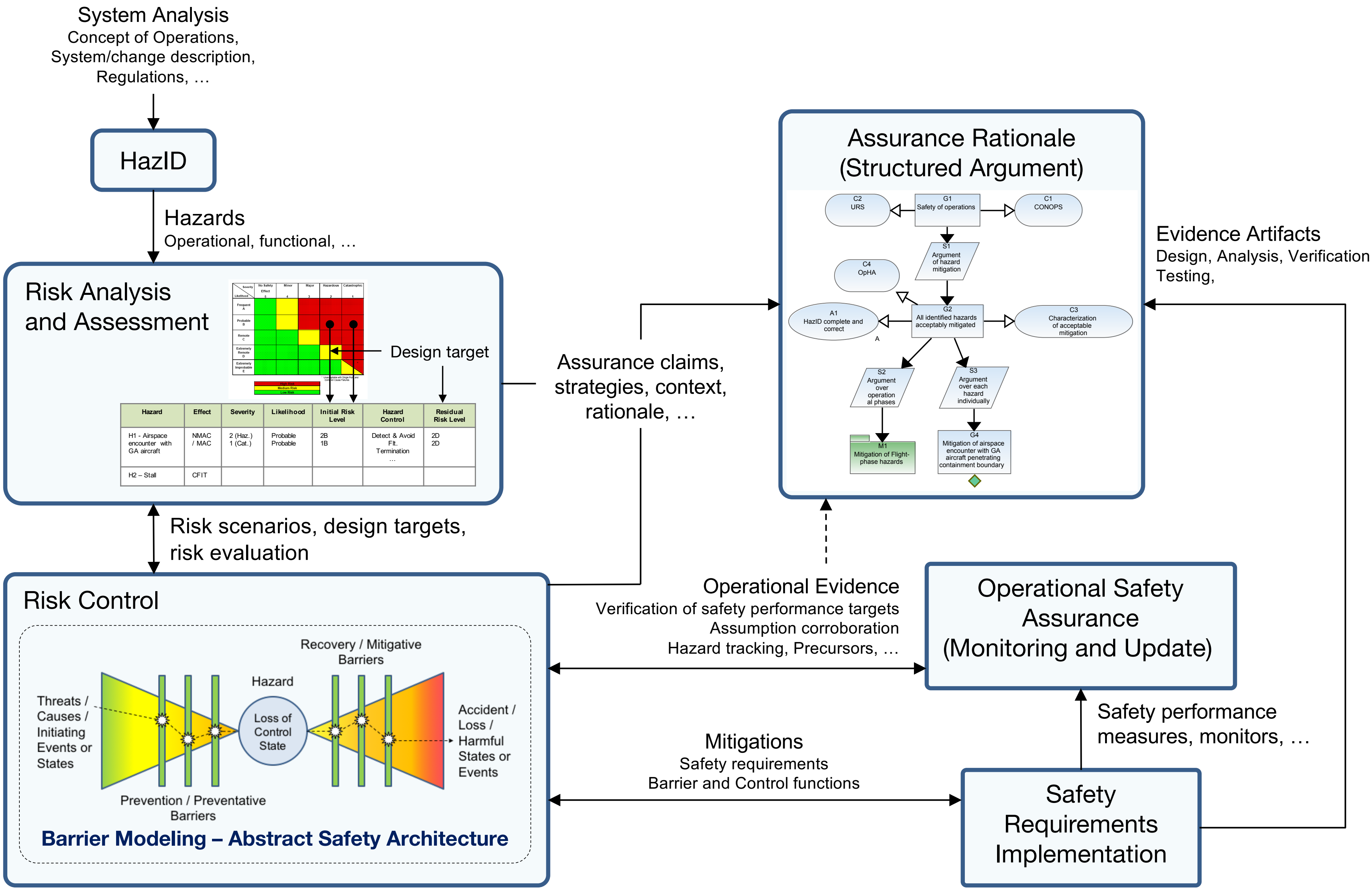
‘A structured set of arguments and a body of evidence showing that an (information) system **satisfies specific claims with respect to a given quality attribute**’

- *National Institute of Standards and Technology* (*2013*)

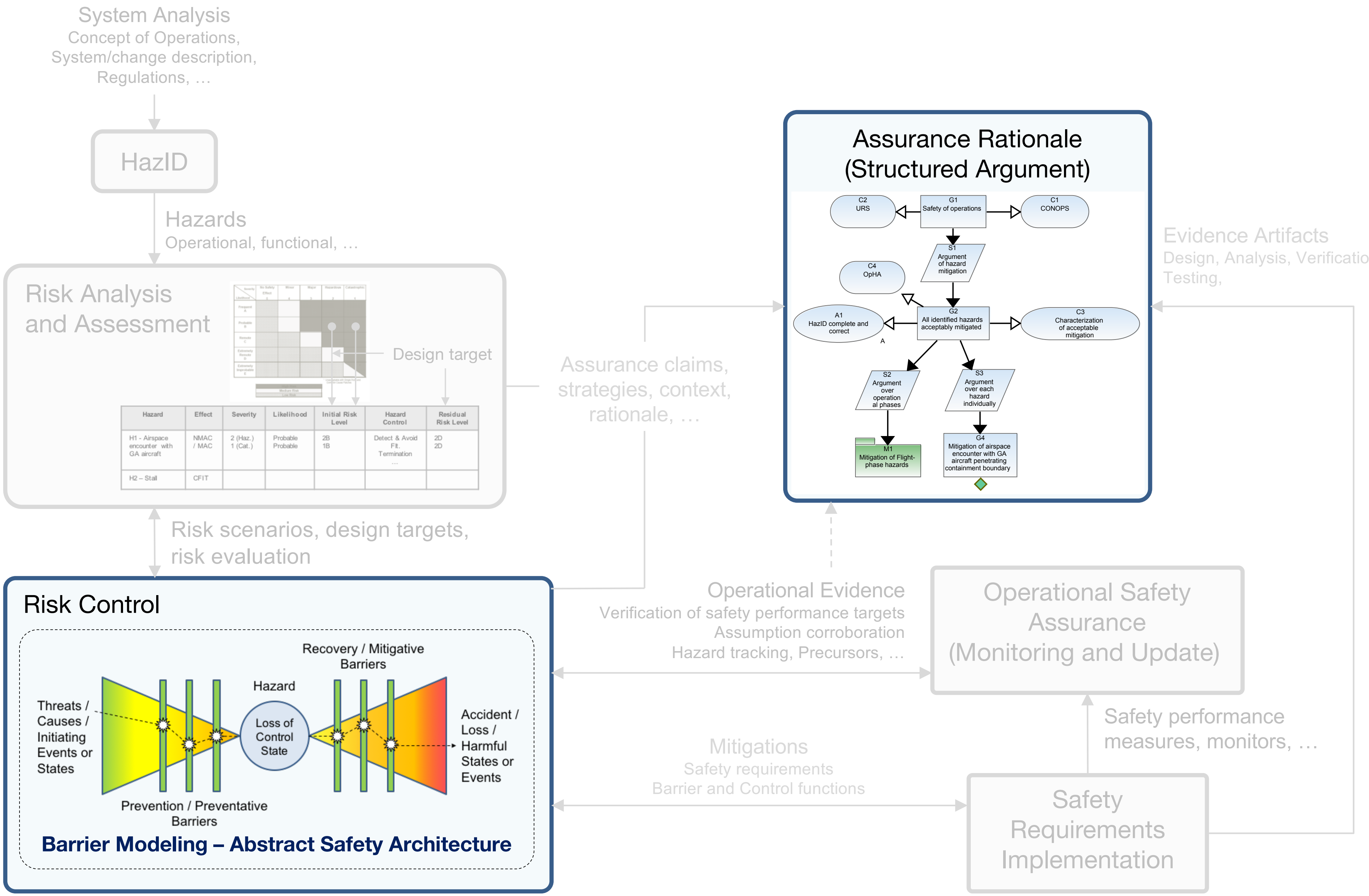
Generalization of safety cases to other assurance properties: security, dependability, …

Safety Risk Management Approach

STINGER GHAFFARIAN TECHNOLOGIES



This Talk

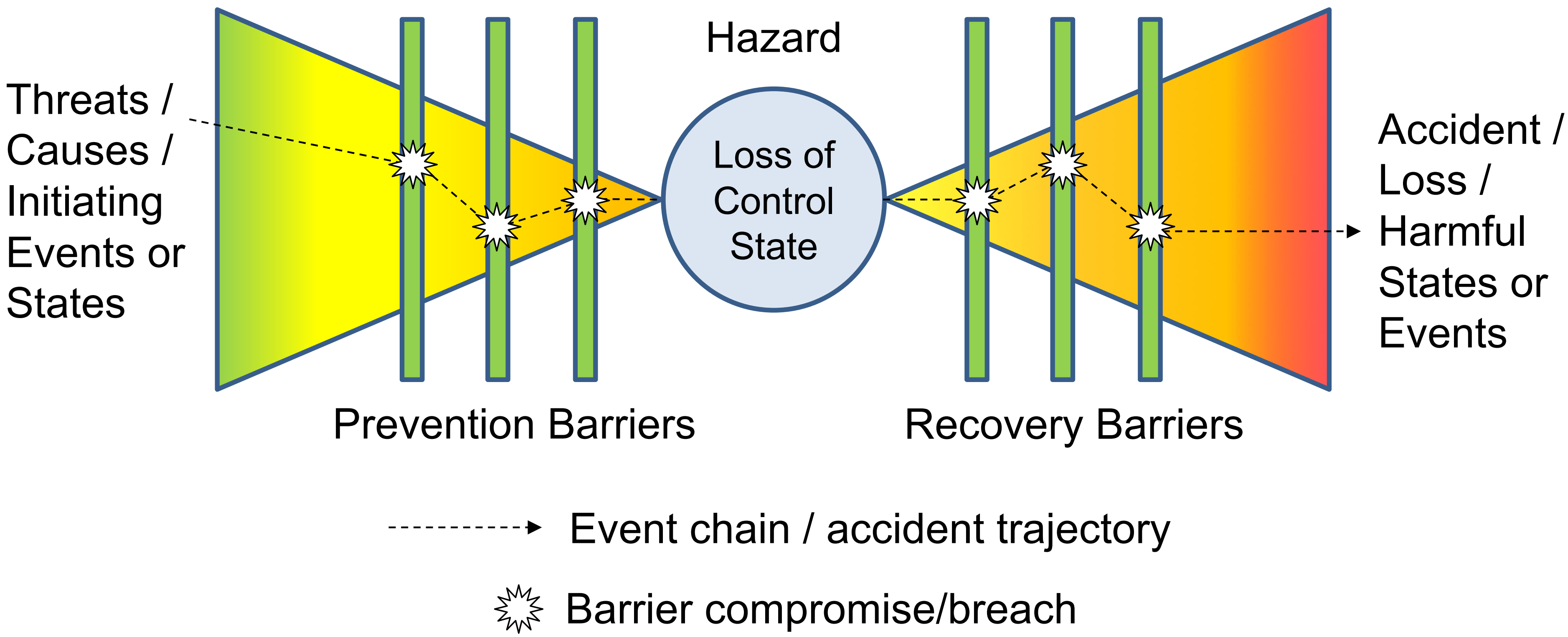


System Analysis
Concept of Operations, System/change description, Regulations, …
HazID
Hazards
Operational, functional, …
Risk Analysis and Assessment
Design target
Hazard | Effect | Severity | Likelihood | Initial Risk Level | Hazard Control | Residual Risk Level
H1 - Airspace encounter with GA aircraft | 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
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

Barrier Modeling

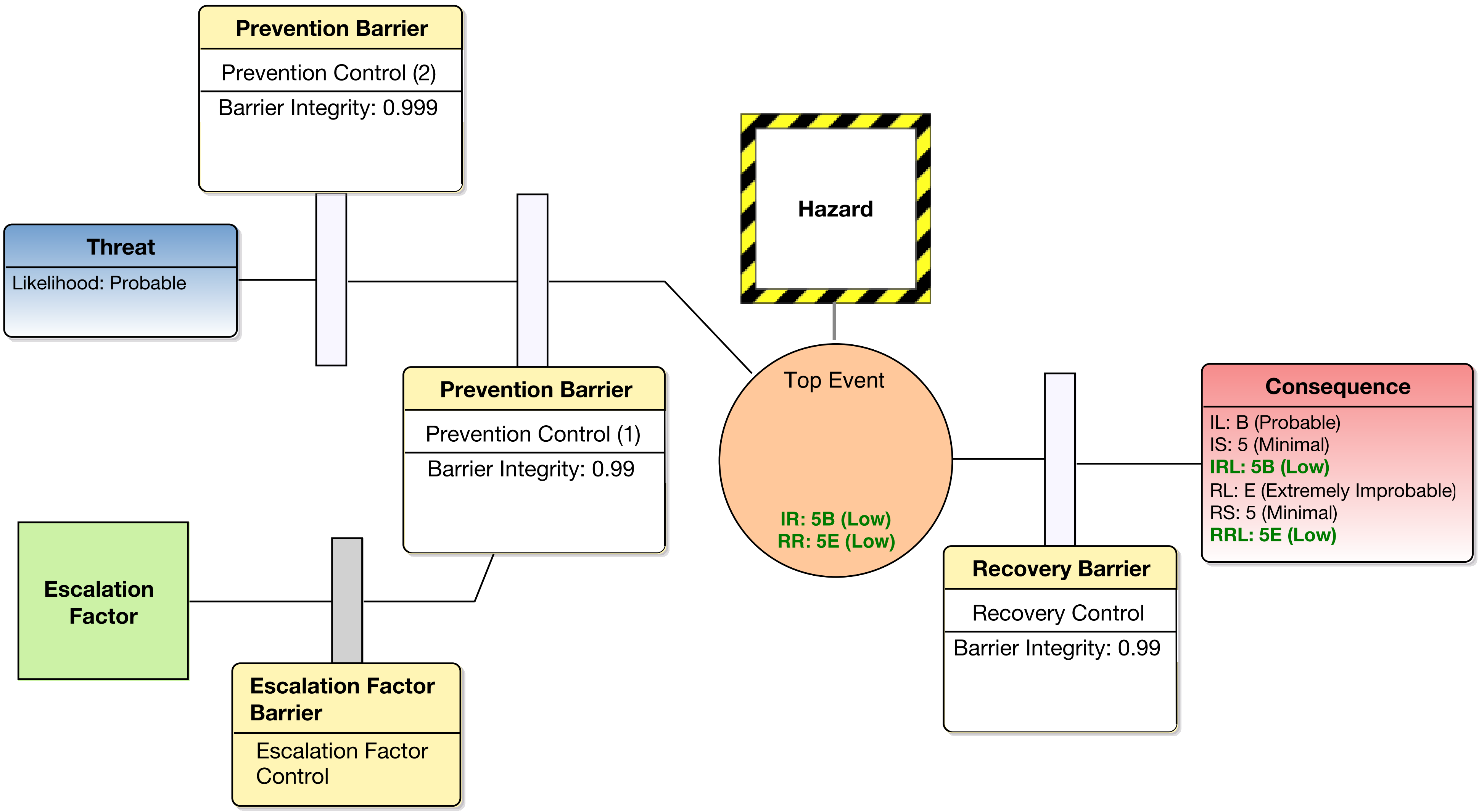
STINGER GHAFFARIAN TECHNOLOGIES

- Collection of barrier models providing a *risk basis*
  - Collection of all factors affecting risk
  - Model for risk qualification/quantification



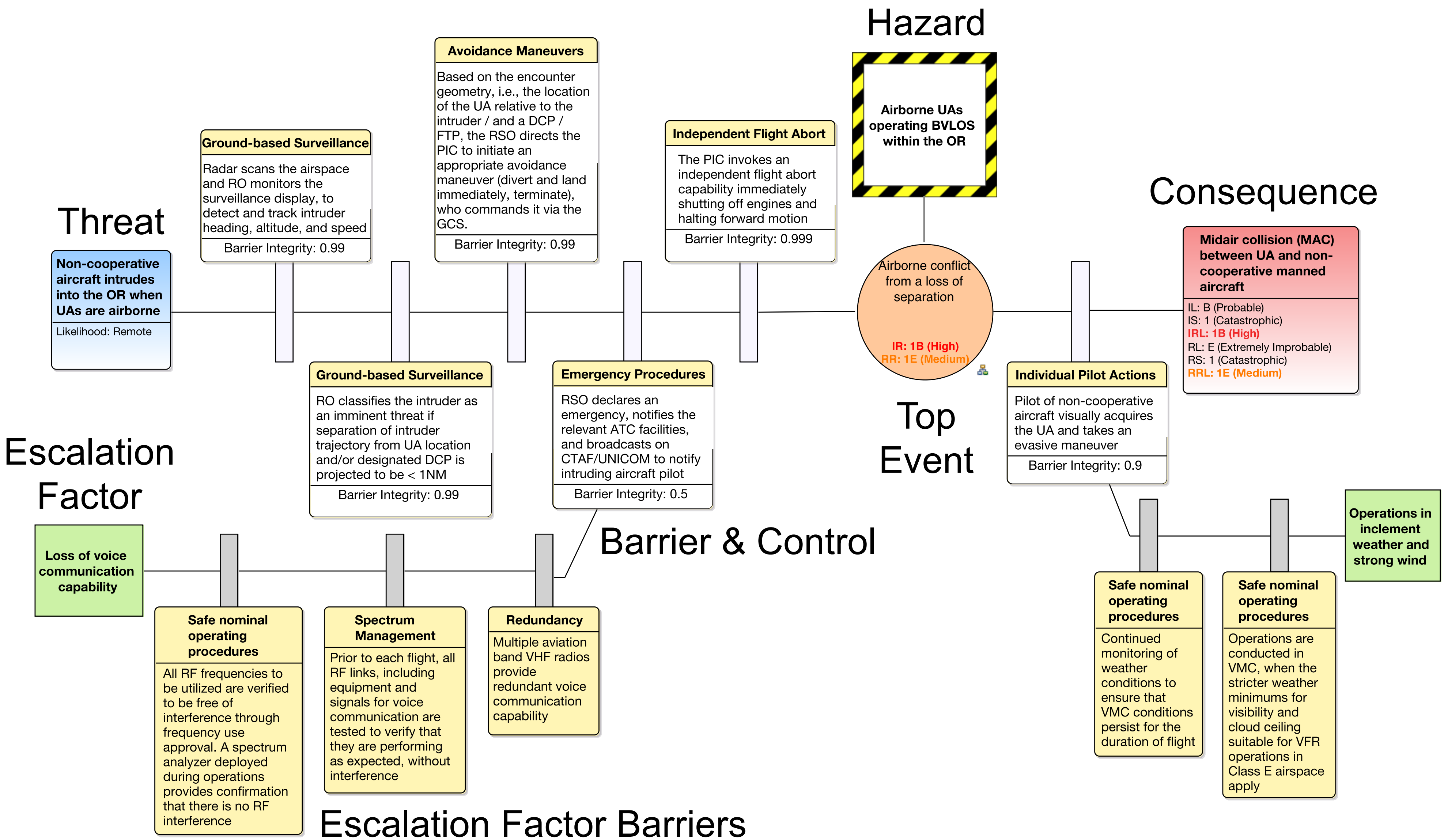
Bow Tie Diagram (BTD)

STINGER GHAFFARIAN TECHNOLOGIES



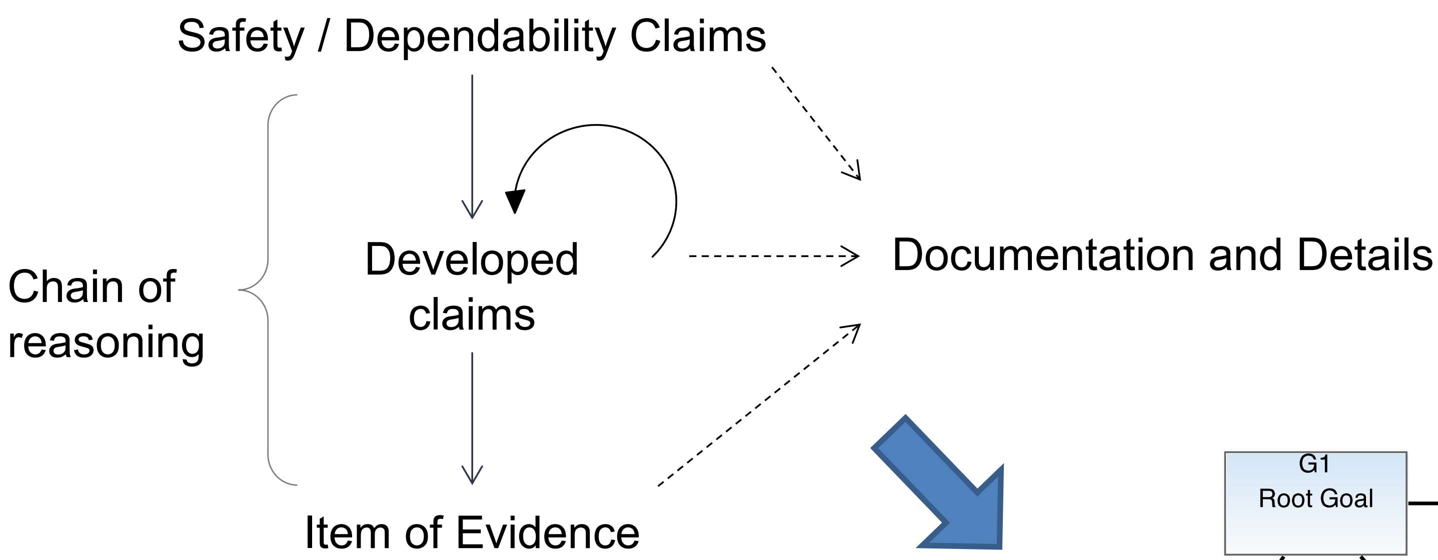
Example: Loss of Separation

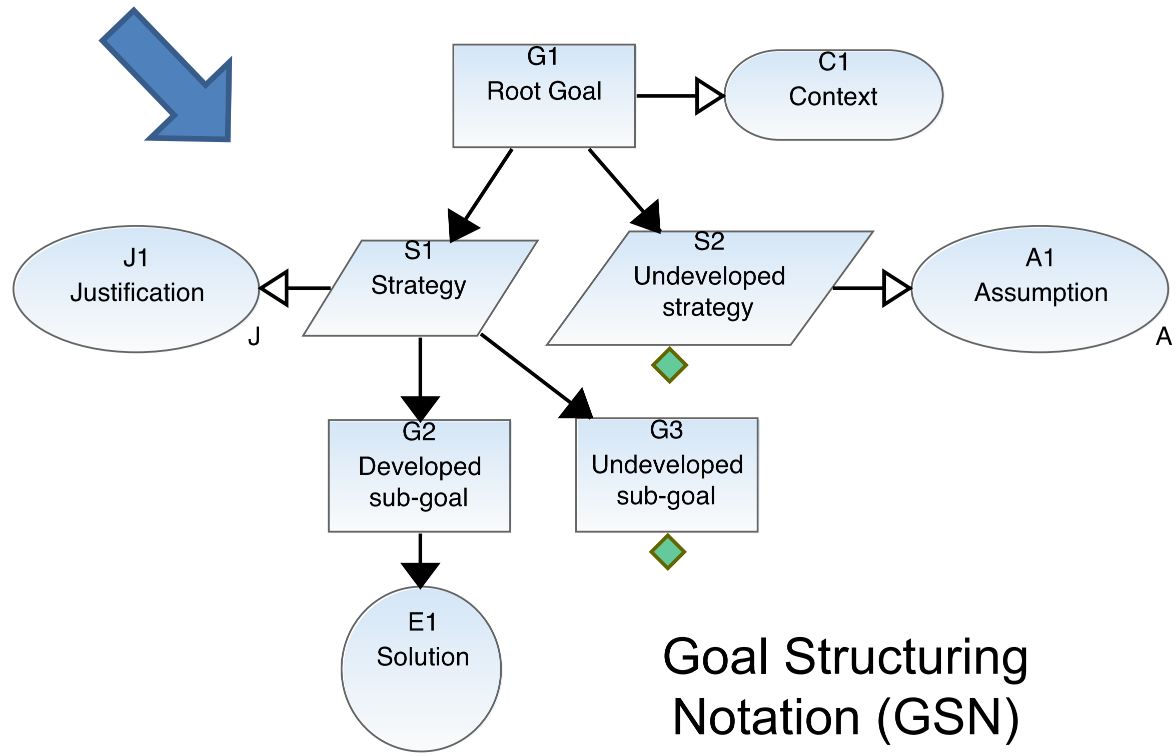
STINGER GHAFFARIAN TECHNOLOGIES



Rationale Capture

STINGER GHAFFARIAN TECHNOLOGIES

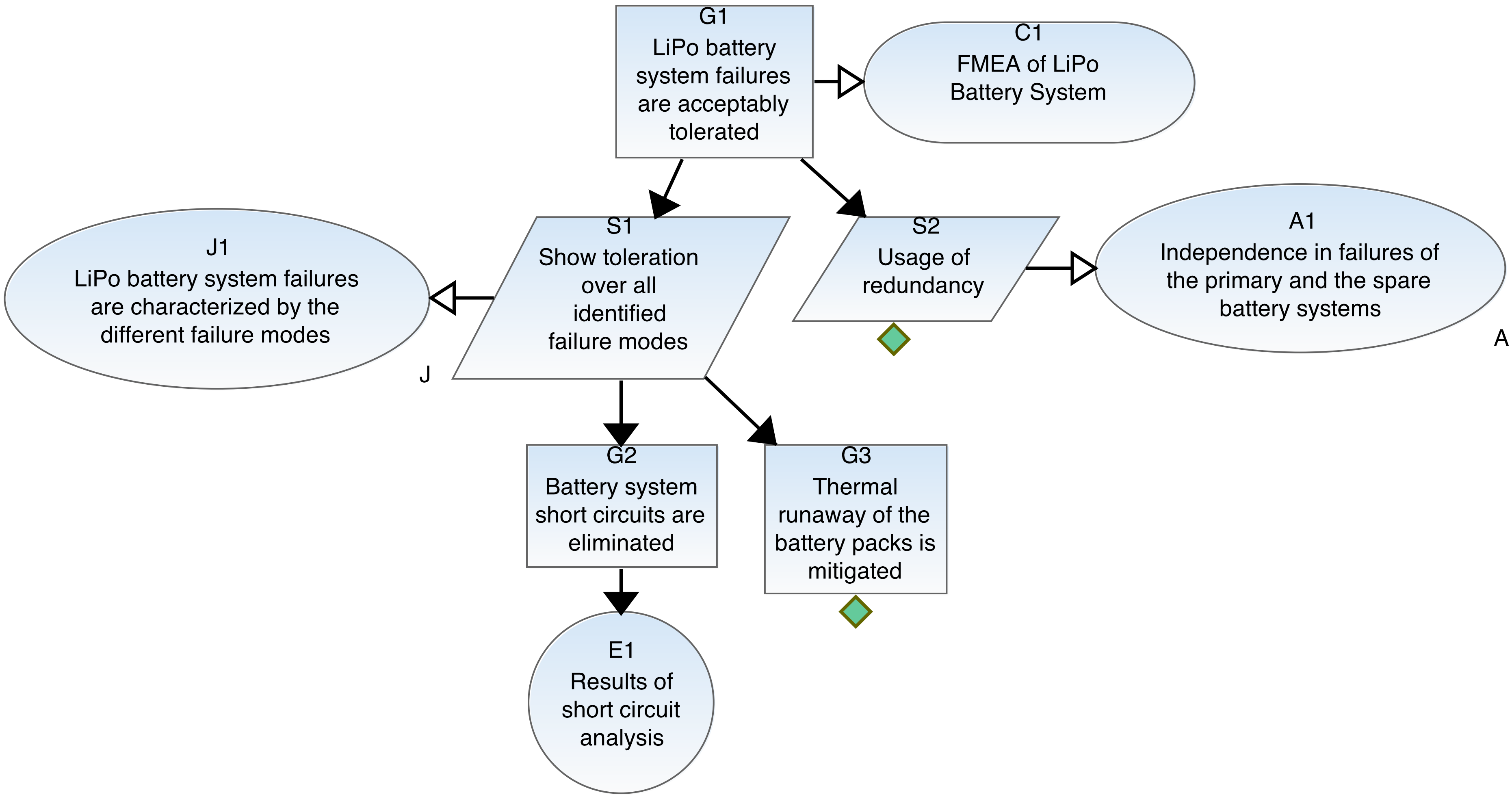




Goal Structuring Notation (GSN)

Example Structured Argument

STINGER GHAFFARIAN TECHNOLOGIES



Tiered Assurance Framework

STINGER GHAFFARIAN TECHNOLOGIES

Tier	Core Assurance Concerns and Scope			Additional Assurance Qualities
Safety Objectives	**System Safety** – Safe concept (safety designed-in) – Safety in design – Safety in implementation – Safe transition into service **– Safety in operations** **– TLOS / Acceptable level of risk** – Safe disposal	Due diligence Reduction of risk – ALARP – SFAIRP – ASARP	Compliance with Aviation Regulations	Processes; – Maturity, … Input data; People; – Competence, … Method and Tools; – Qualification, … Safety management system; Lifecycle
1	**Overall Assurance** All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release. **All relevant consequences** across all BTDs.		All applicable regulatory requirements	Coverage; Independence of threats; Effectiveness; ….
2	**Profile of Risks** For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, … **Specific consequence,** e.g., **midair collision** All causal chains, threats, and dangerous interactions across all hazards.			Coverage (function, environment, interactions, scenarios, …); Independence; …
3	**Individual Risks** **Specific risk scenario,** i.e., causal chain of consequence, top event, threats, causes/precursors **Applicable system of barriers / safety measures**			Depth; **Independence;** Proactiveness: Prevention vs. Recovery; …
4	**Barriers** Functional safety / **fitness for purpose** Delivery of required service			Depth; Independence; Common causes/modes, …
5	**Controls** Functional safety / fitness for purpose Delivery of required service			Reliability and effectiveness; Availability; Functional / safety integrity; Resilience; Fail safety; Data integrity; **Verifiability**; …

Outline

STINGER GHAFFARIAN TECHNOLOGIES

- Motivation
- Assurance Cases
- **Example**
- Tool support
- Outlook

Factors Affecting UAS Safety

STINGER GHAFFARIAN TECHNOLOGIES

Diverse environment
- Populated / urban / built-up areas
- Uncontrolled / controlled airspace
- Low / high density airspace

Different configurations
- Airborne sensors (Lidar, sonar, FPV camera, Radar)
- Ground sensors (Radar)
- Multiple GCS, Roaming GCS, …

Varying mission concepts
- Package delivery
- Surveillance
- Aerial inspection
- Mapping, …

Increasing complexity in mission and operations

Combination of operating modes
- Visual line of sight (VLOS)
- Beyond visual line of sight (BVLOS)
- Beyond radio line of sight (BRLOS)

Varying *access profiles*
- Operating range
- Terminal airspace
- Transit (vertical / lateral)

UAS Safety Assurance

STINGER GHAFFARIAN TECHNOLOGIES

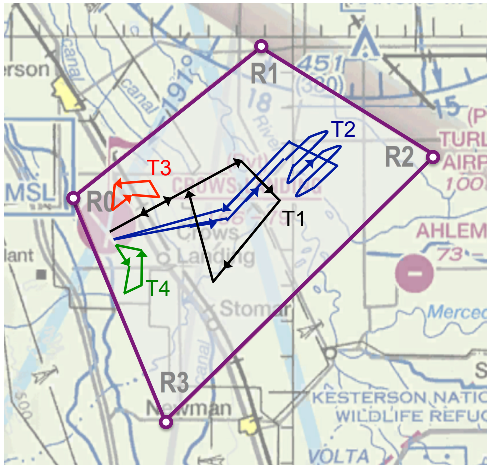
- Scope of UAS safety
  - Design assurance
  - Prior to deployment
  - Engineering evidence from development of fitness for purpose
- Operational assurance
  - Post-deployment, runtime evidence
  - Corroboration of expected safety performance

- Safety measures should be commensurate with the risk posed by the intended operations
  - Level of risk posed dictates safety measures employed and the extent of assurance provided

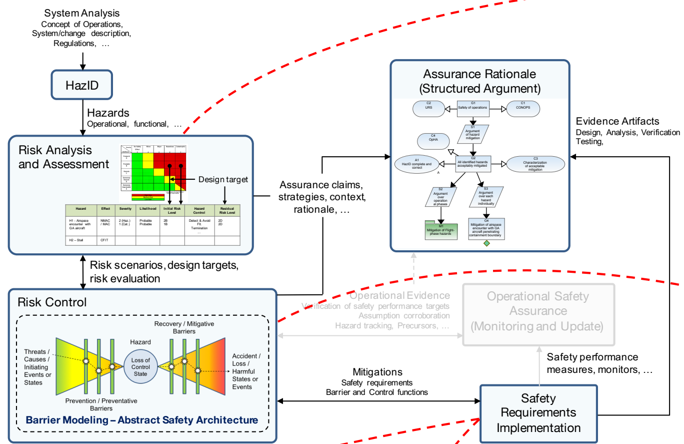
- Preferred form of safety justification (FAA Order 8900.1)
  - Safety Case
  - Assessment of Acceptable Level of Safety (ALoS)

UTM / UAS Safety

STINGER GHAFFARIAN TECHNOLOGIES

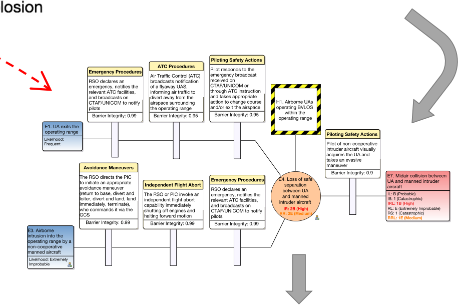


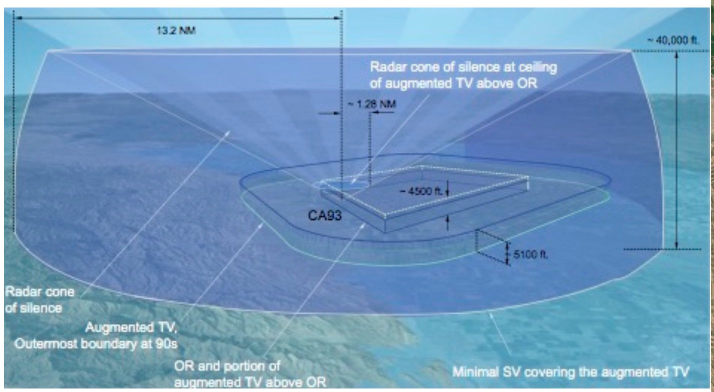
Notional CONOPS



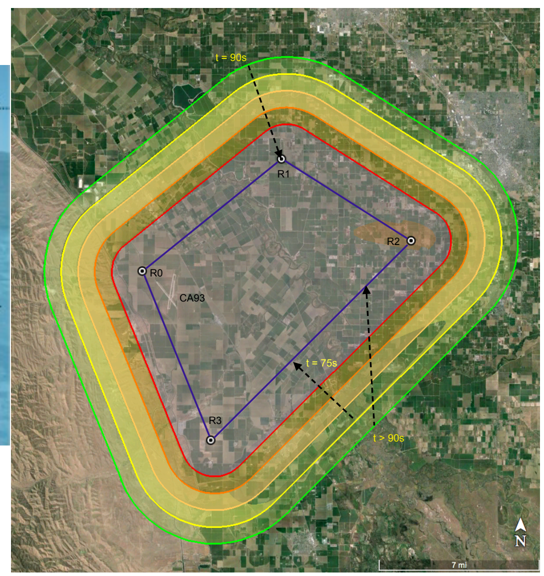
Identified Hazards

- 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





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



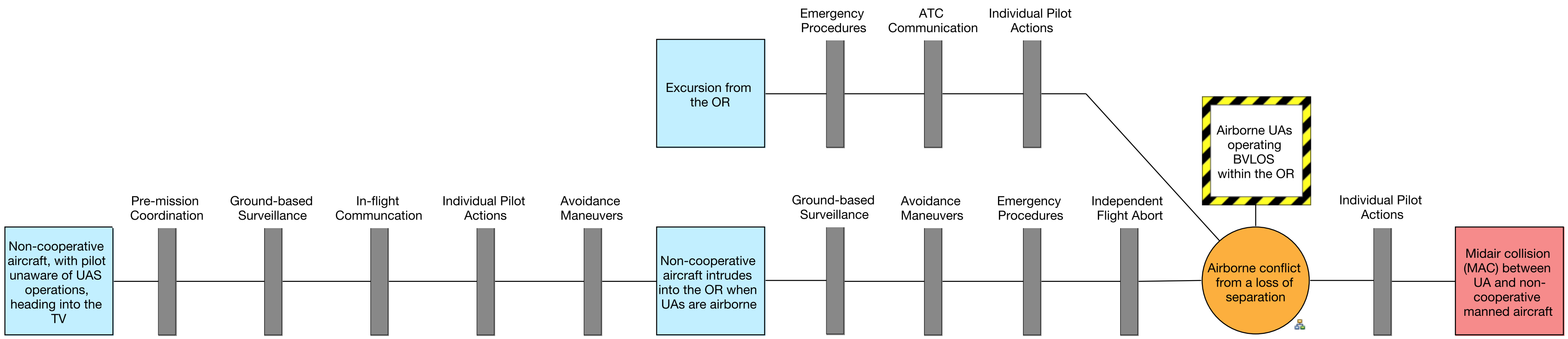
Airspace / Threat Modeling

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

Risk Assessment

STINGER GHAFFARIAN TECHNOLOGIES



- Residual risk = Consequence probability x severity
  - Probability of disjunction of all paths leading to consequence
    - Inclusion exclusion principle
  - Path probability = Joint probability of all events on path
    - Barrier *integrity*, threat event probability
  - Assumptions and data

Recall Tiered Assurance

STINGER GHAFFARIAN TECHNOLOGIES

Tier	Core Assurance Concerns and Scope			Additional Assurance Qualities
Safety Objectives	**System Safety** – Safe concept (safety designed-in) – Safety in design – Safety in implementation – Safe transition into service **– Safety in operations** **– TLOS / Acceptable level of risk** – Safe disposal	Due diligence Reduction of risk – ALARP – SFAIRP – ASARP	Compliance with Aviation Regulations	Processes; – Maturity, … Input data; People; – Competence, … Method and Tools; – Qualification, … Safety management system; Lifecycle
1	**Overall Assurance** All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release. **All relevant consequences** across all BTDs.		All applicable regulatory requirements	Coverage; Independence of threats; Effectiveness; ….
2	**Profile of Risks** For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, … **Specific consequence,** e.g., **midair collision** All causal chains, threats, and dangerous interactions across all hazards.			Coverage (function, environment, interactions, scenarios, …); Independence; …
3	**Individual Risks** **Specific risk scenario,** i.e., causal chain of consequence, top event, threats, causes/precursors **Applicable system of barriers / safety measures**			Depth; **Independence;** Proactiveness: Prevention vs. Recovery; …
4	**Barriers** Functional safety / **fitness for purpose** Delivery of required service			Depth; Independence; Common causes/modes, …
5	**Controls** Functional safety / fitness for purpose Delivery of required service			Reliability and effectiveness; Availability; Functional / safety integrity; Resilience; Fail safety; Data integrity; **Verifiability**; …

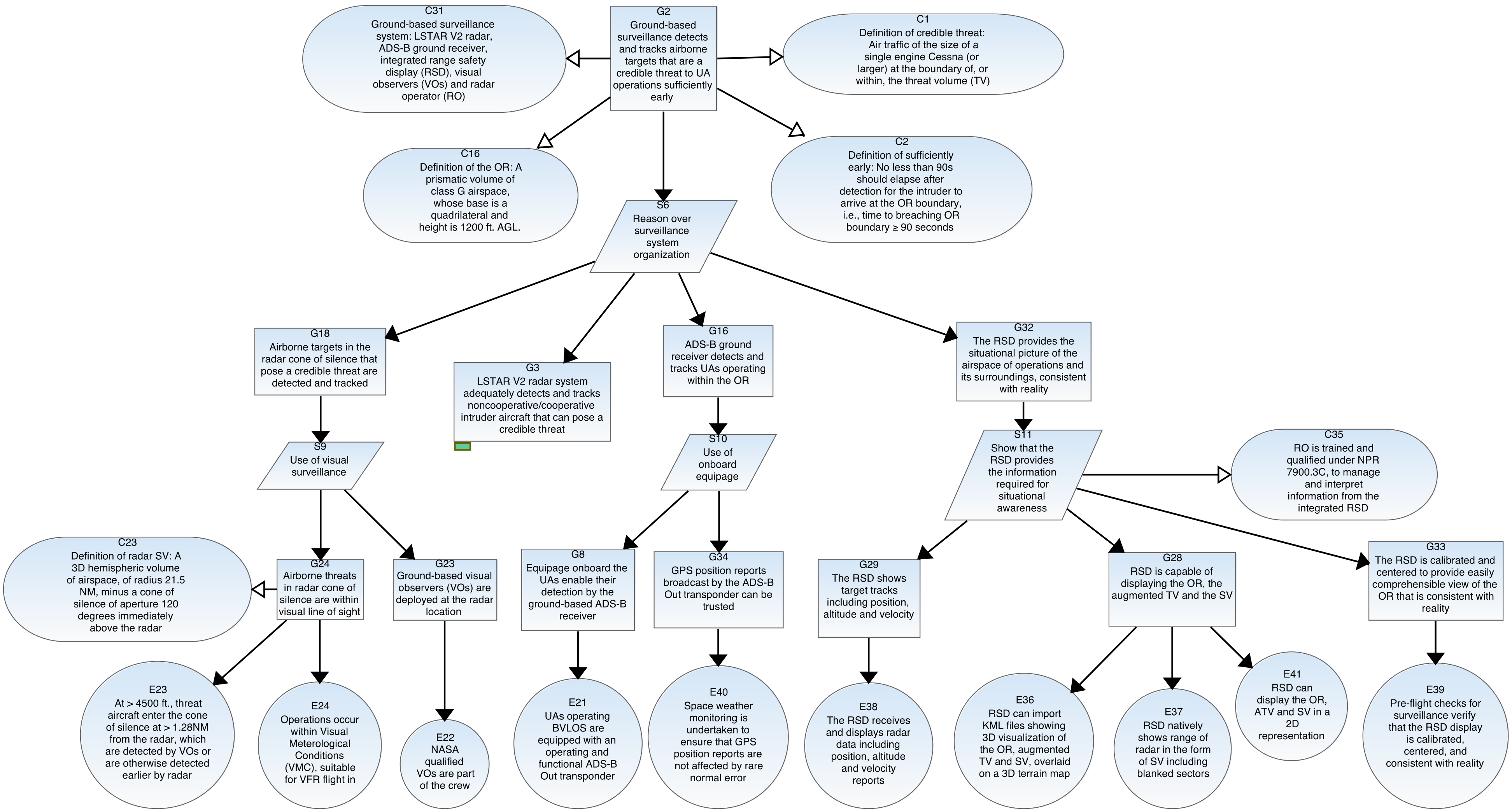
Argument-based Assurance

STINGER GHAFFARIAN TECHNOLOGIES

Tier	Core Assurance Concerns and Scope			Additional Assurance Qualities
Safety Objectives	**System Safety** – Safe concept (safety designed-in) – Safety in design – Safety in implementation – Safe transition into service – **Safety in operations** – **TLOS / Acceptable level of risk** – Safe disposal	Due diligence Reduction of risk – ALARP – SFAIRP – ASARP	Compliance with Aviation Regulations	Processes; – Maturity, … Input data; People; – Competence, … Method and Tools; – Qualification, … Safety management system; Lifecycle
1	**Overall Assurance** All hazards / hazard risk statements, i.e., combination of hazardous situation, hazard release. **All relevant consequences** across all BTDs.		All applicable regulatory requirements	Coverage; Independence of threats; Effectiveness; ….
2	**Profile of Risks** For each hazard, all risk scenarios (consequences), e.g., midair collision, near midair collision, ground collision, … **Specific consequence,** e.g., **midair collision** All causal chains, threats, and dangerous interactions across all hazards.			Coverage (function, environment, interactions, scenarios, …); Independence; …
3	**Individual Risks** **Specific risk scenario,** i.e., causal chain of consequence, top event, threats, causes/precursors **Applicable system of barriers / safety measures**			Depth; **Independence;** Proactiveness: Prevention vs. Recovery; …
4	**Barriers** Functional safety / **fitness for purpose** Delivery of required service			Depth; Independence; Common causes/modes, …
5	**Controls** Functional safety / fitness for purpose Delivery of required service			Reliability and effectiveness; Availability; Functional / safety integrity; Resilience; Fail safety; Data integrity; **Verifiability**; …

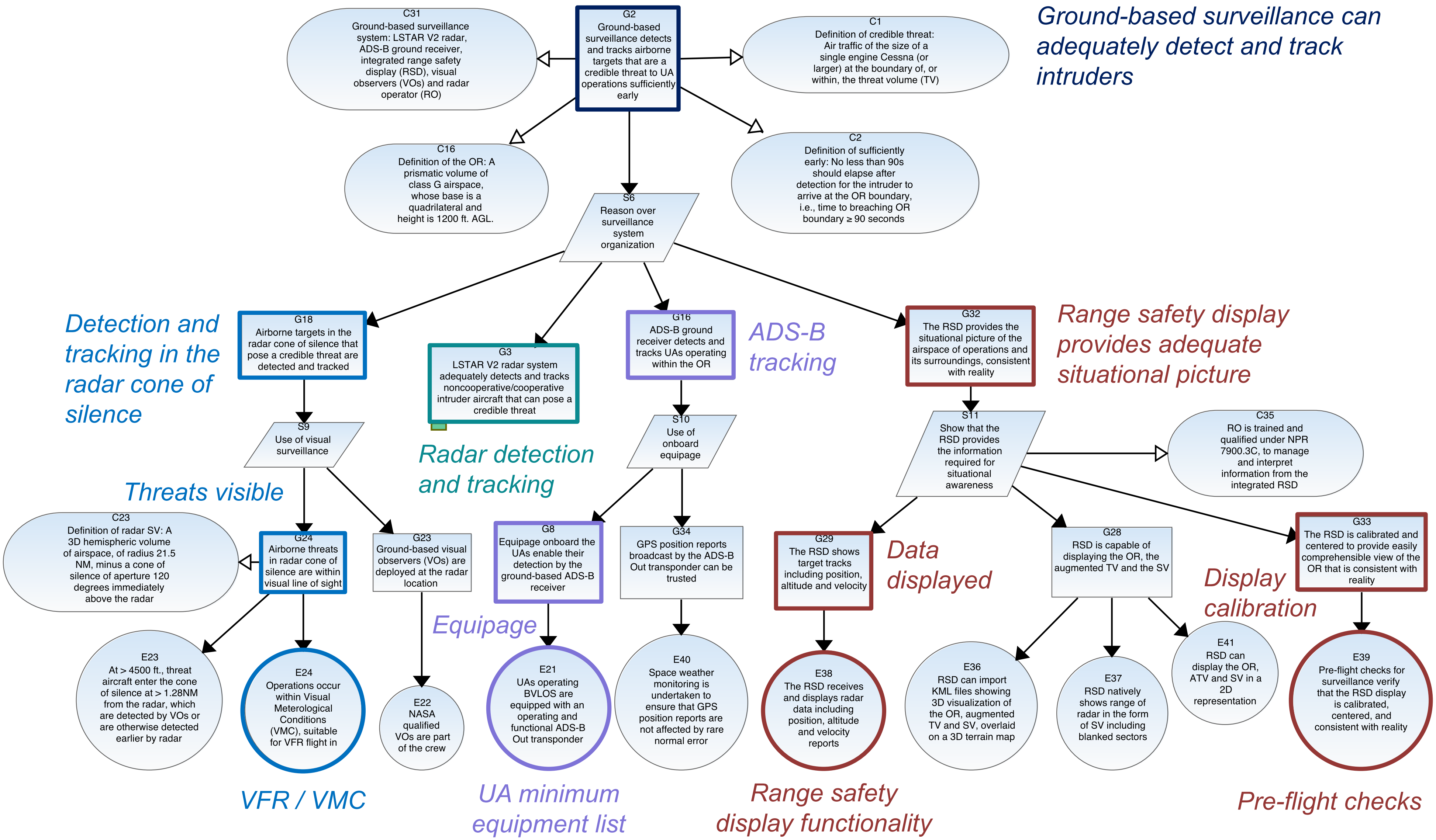
Barrier Fitness for Purpose

STINGER GHAFFARIAN TECHNOLOGIES



Barrier Fitness for Purpose

STINGER GHAFFARIAN TECHNOLOGIES



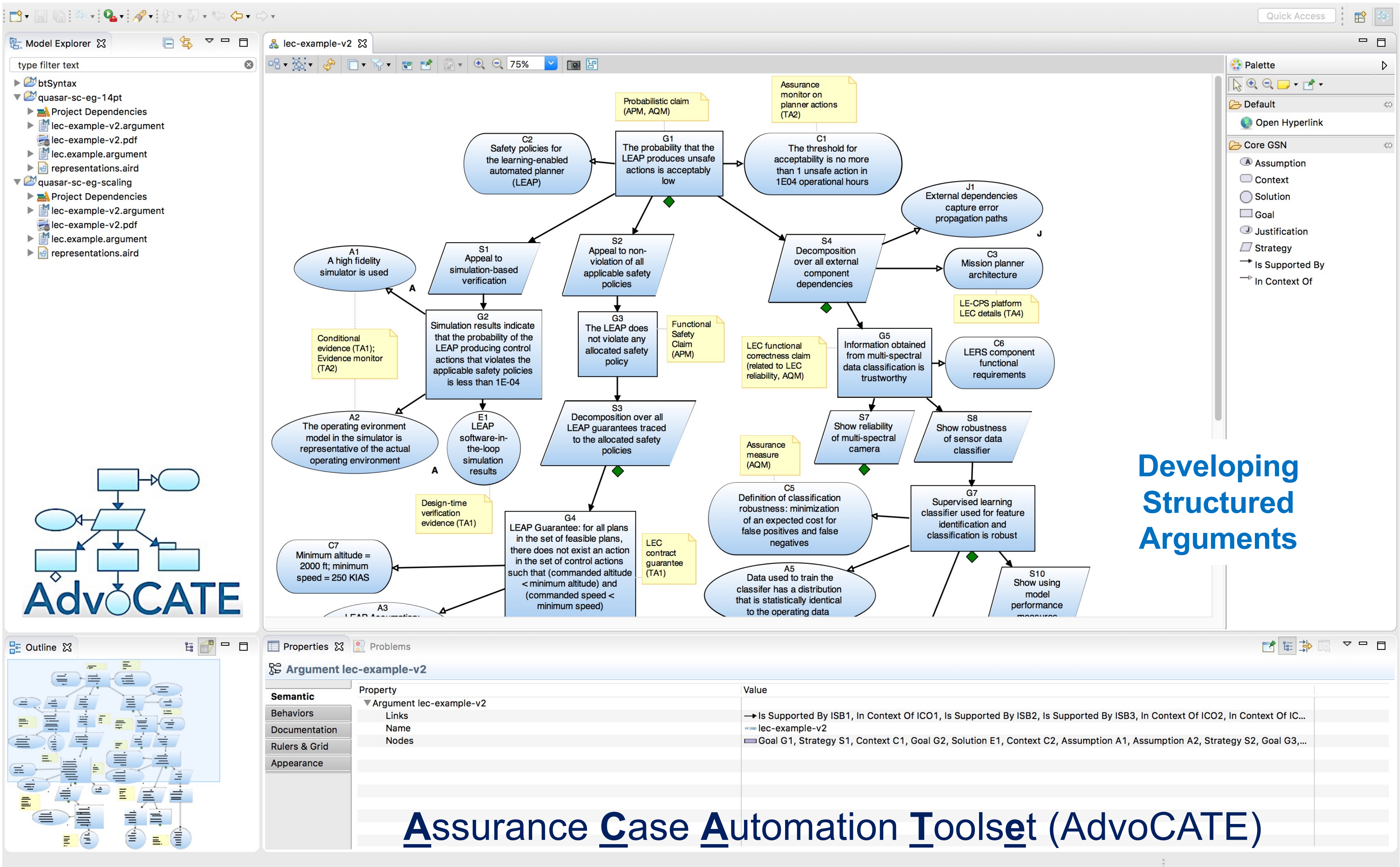
Outline

STINGER GHAFFARIAN TECHNOLOGIES

- Motivation
- Assurance Cases
- Example
- **Tool support**
- Outlook

AdvoCATE

STINGER GHAFFARIAN TECHNOLOGIES

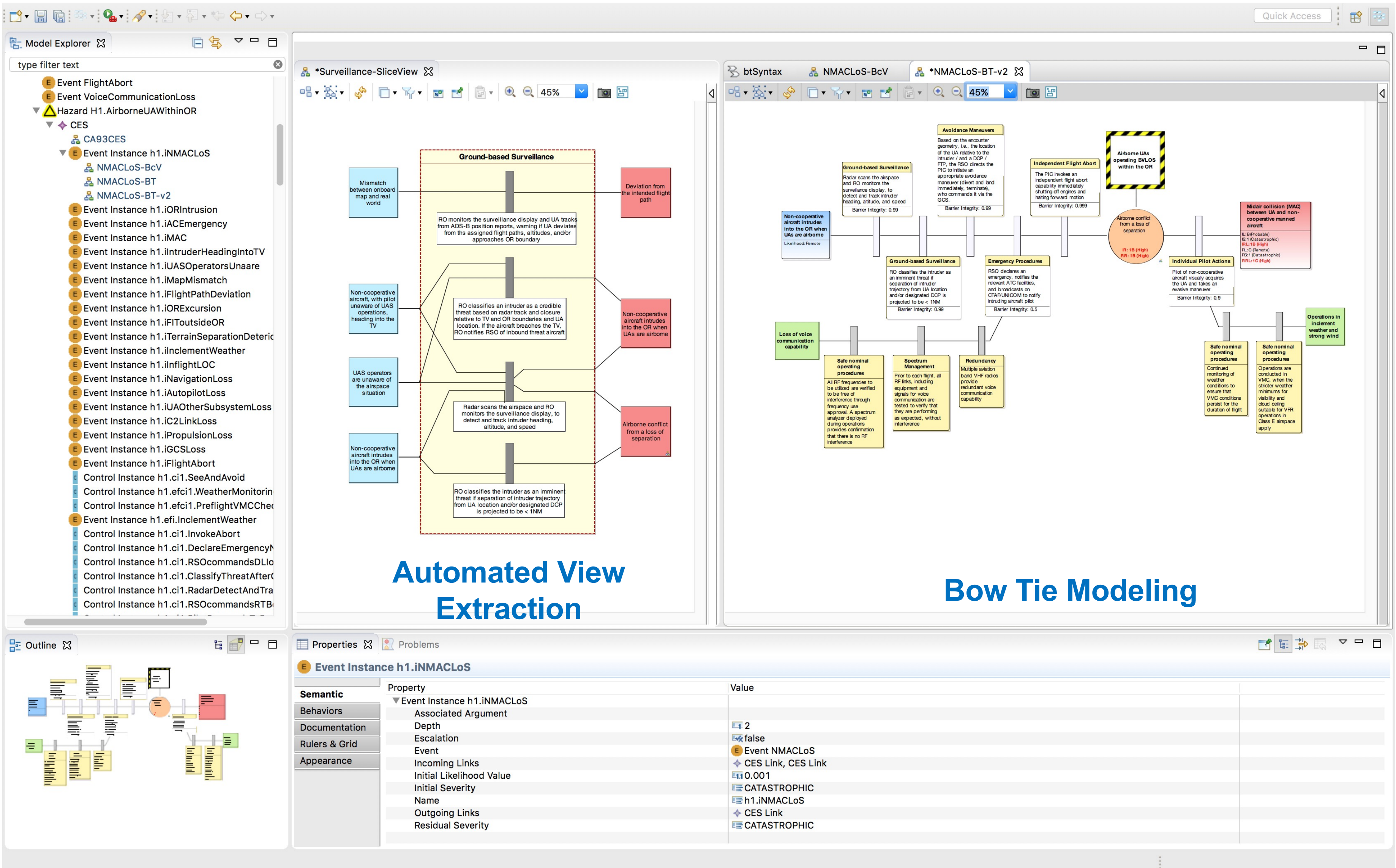


Developing Structured Arguments

Assurance **C**ase **A**utomation **T**ools**e**t (AdvoCATE)

AdvoCATE

STINGER GHAFFARIAN TECHNOLOGIES



AdvoCATE

STINGER GHAFFARIAN TECHNOLOGIES

- Hazard analysis and safety requirements capture
- Structured arguments
  - *Pattern* specification and automated pattern *instantiation*
  - Integration of formal methods and formal tool-based evidence
  - *Hierarchical* and *Modular* refactoring
  - Argument *queries* and *views*
  - Argument *verification*
  - Metrics
  - Report generation
- Safety architectures
  - Bow tie modeling
  - Views
  - Transformations (event and barrier split / merge)
- Evidence management
- <u>**S**</u>afety, <u>**M**</u>ission <u>**A**</u>ssurance, and <u>**R**</u>isk managemen<u>**t**</u> (SMART) Dashboard

Outline

STINGER GHAFFARIAN TECHNOLOGIES

- Motivation
- Assurance Cases
- Example
- Tool support
- **Outlook**

RISC and OHs

STINGER GHAFFARIAN TECHNOLOGIES

- NASA adoption of *safety case* paradigm
- Promulgated by Office of Safety and Mission Assurance (OSMA)
  - *Objective hierarchies* (OHs)
    - Decomposition of assurance objectives
      - Safety, reliability and maintainability, software assurance, range safety, …
  - *Risk informed safety case* (RISC)
    - System Safety Handbook, vols. 1 & 2
    - Elaborates
      - NASA acquisition process based on safety performance
      - Supplier requirements for justification of safety performance
      - Argumentation for rationale capture
      - Risk assessment and cost-benefit analysis for decision making

RISC and OHs

- Software assurance research program funding (FY18)
  - Retrospective characterization of assurance afforded by RISC and Software OH against an *assurance baseline*
  - Assurance baseline from NASA ARC BioSentinel mission
    - CFS/CFE
    - V&V artifacts
    - Current NASA assurance standards and guidelines
  - Mapping to RISC and OH to assurance artifacts
    - Analysis of potential gaps and assurance deficits
  - Tool support via AdvoCATE

Conclusions and Future Work

STINGER GHAFFARIAN TECHNOLOGIES

- Development of end-to-end assurance methodology and tool support
- Foundational research, informed by and corroborated in practical application
- Safety cases created were the first of their kind
  - MIZOPEX: First civil safety case to be approved
    - NASA Honor Award
  - UTM Safety Case: First civil safety case to be approved for using ground-based detect and avoid to conduct BVLOS operations in the NAS

Conclusions and Future Work

STINGER GHAFFARIAN TECHNOLOGIES

- Ongoing focus on design-time assurance
  - Artifacts and rationale from development, prior to release-into-service
- Outlook towards operational assurance through lifecycle
  - In-service safety performance monitoring
- Dashboard for stakeholder-specific assurance
- Current focus on safety
  - Expansion in focus to mission assurance
  - Expansion in application domain to spaceflight
    - Initially robotic
    - Eventually, human spaceflight

Looking for opportunities to infuse our technology into other SGT customer projects

Abstract

STINGER GHAFFARIAN TECHNOLOGIES

The *Assurance Case* approach is being adopted in a number of safety-/mission-critical application domains in the U.S., e.g., medical devices, defense aviation, automotive systems, and, lately, civil aviation. This paradigm refocuses traditional, process-based approaches to assurance on demonstrating explicitly stated assurance goals, emphasizing the use of *structured rationale*, and concrete *product-based evidence* as the means for providing justified confidence that systems and software are fit for purpose in safely achieving mission objectives. NASA has also been embracing assurance cases through the concepts of *Risk Informed Safety Cases* (RISCs), as documented in the NASA System Safety Handbook*, and Objective Hierarchies* (OHs), as put forth by the Agency's Office of Safety and Mission Assurance (OSMA). This talk will give an overview of the work being performed by the SGT team located at NASA Ames Research Center, in developing technologies and tools to engineer and apply assurance cases in customer projects pertaining to aviation safety. We elaborate how our **A**ssurance **C**ase **A**utomation **T**ools**e**t (AdvoCATE) has not only extended the state-of-the-art in assurance case research, but also demonstrated its practical utility. We have successfully developed safety assurance cases for a number of Unmanned Aircraft Systems (UAS) operations, which underwent, and passed, scrutiny both by the aviation regulator, i.e., the FAA, as well as the applicable NASA boards for airworthiness and flight safety, flight readiness, and mission readiness. We discuss our efforts in expanding AdvoCATE capabilities to support RISCs and OHs under a project recently funded by OSMA under its Software Assurance Research Program. Finally, we speculate on the applicability of our innovations beyond aviation safety to such endeavors as robotic, and human spaceflight.