Barrier Analysis of an Aviation Safety Assessment Model

John Shortle
Seungwon Noh
George Mason University

July 10, 2018

GEORGE MASON UNIVERSITY

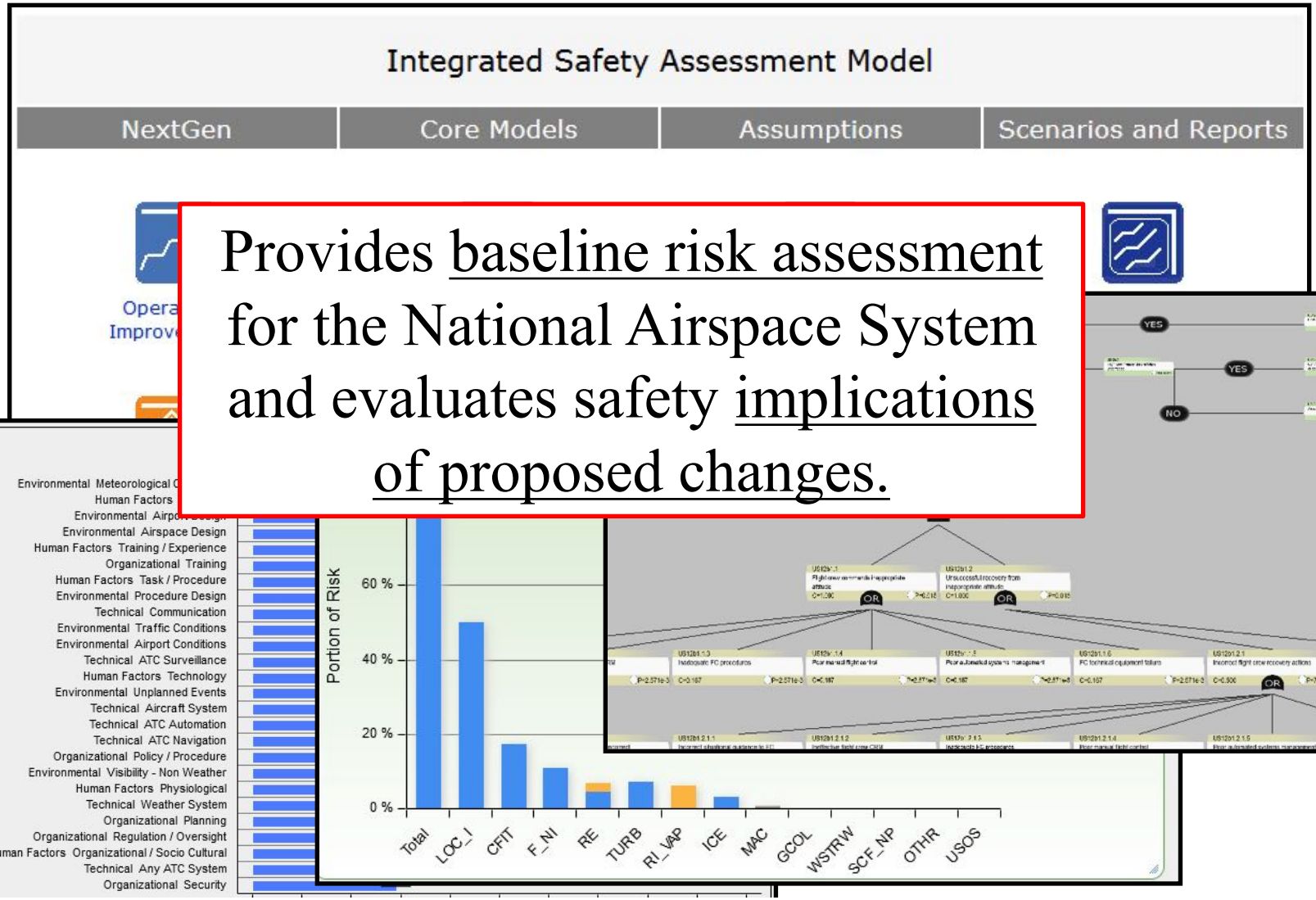
Acknowledgments

- Aleta Best, FAA
- Alan Durston, Brian Hjelle, Poornima Balakrishna, Saab-Sensis

Disclaimer

- The opinions expressed in this talk are those of the authors

Integrated Safety Assessment Model

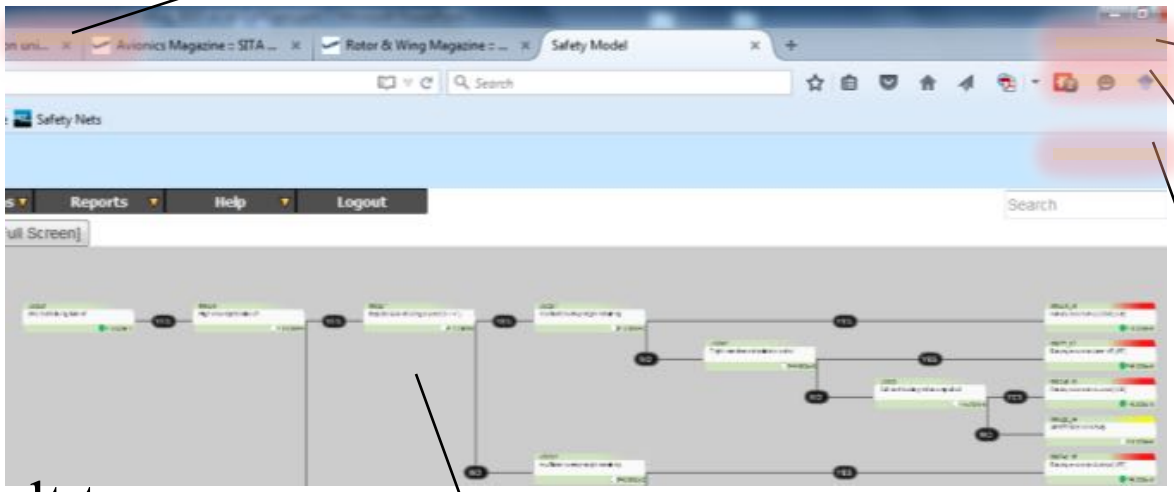


Borener, S., S. Trajkov, P. Balakrishna. 2012. Design and development of an Integrated Safety Assessment Model for NextGen, International Annual Conference of the American Society for Engineering Management.

ISAM Safety Model

Event sequence diagrams

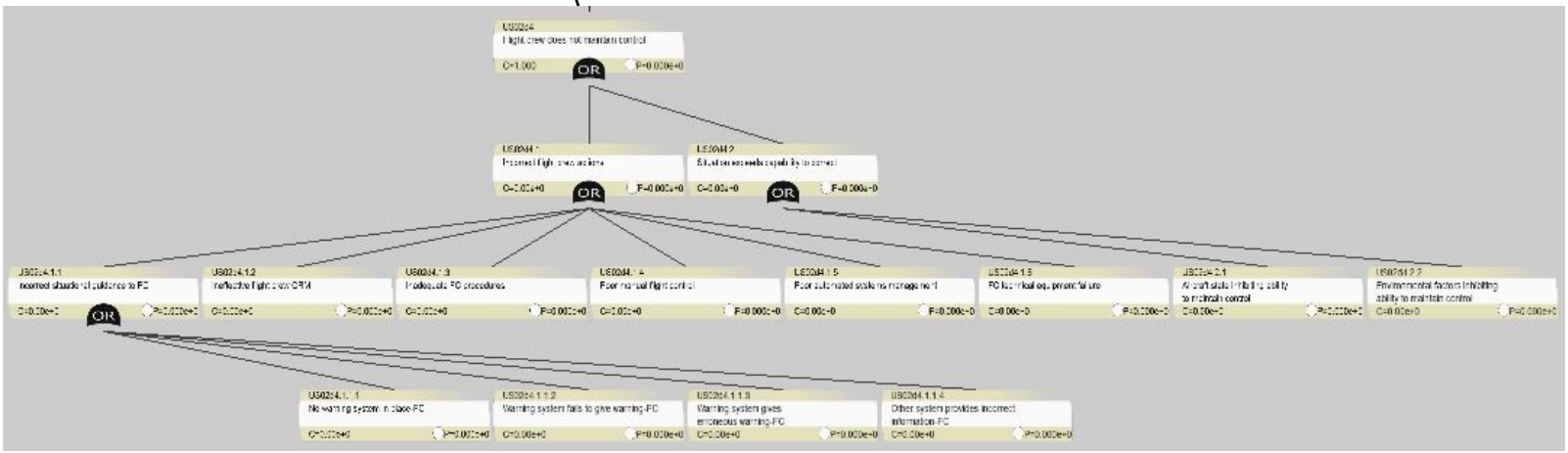
E.g., aircraft system failure during take-off



Pr{end event}

- Over-run
- Veer-off
- Aircraft stops on runway

Fault trees



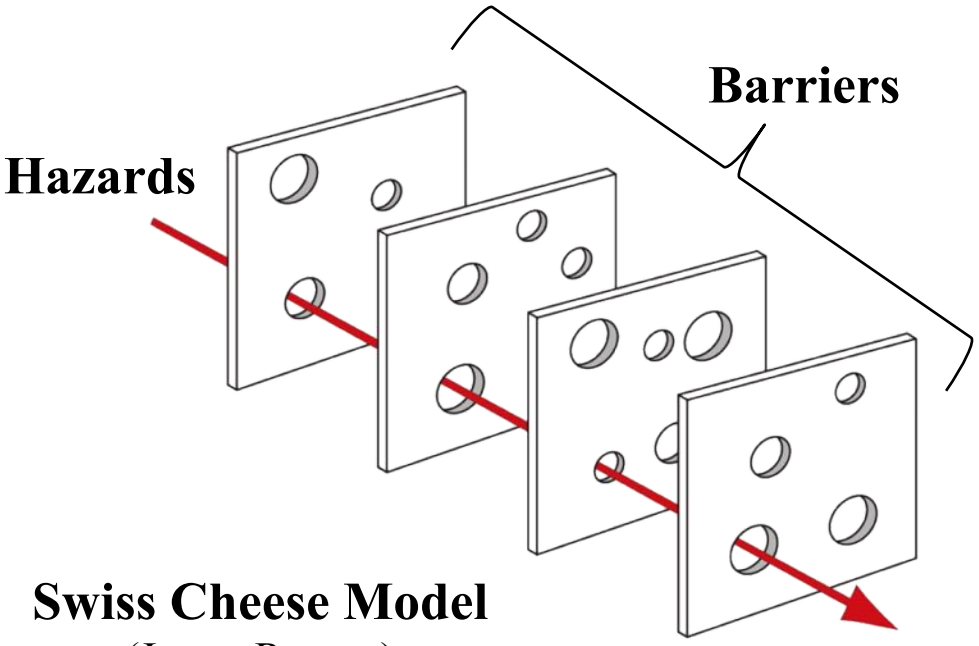
Model Size

- 35 event sequence diagrams (ESDs)
  - Each corresponds to a different initiating event
    - Engine failure on take-off
    - Aircraft on collision course
    - Unstable approach
    - …
- 205 pivoting events
- 3,454 fault tree nodes

Counts are given for ISAM 3.0

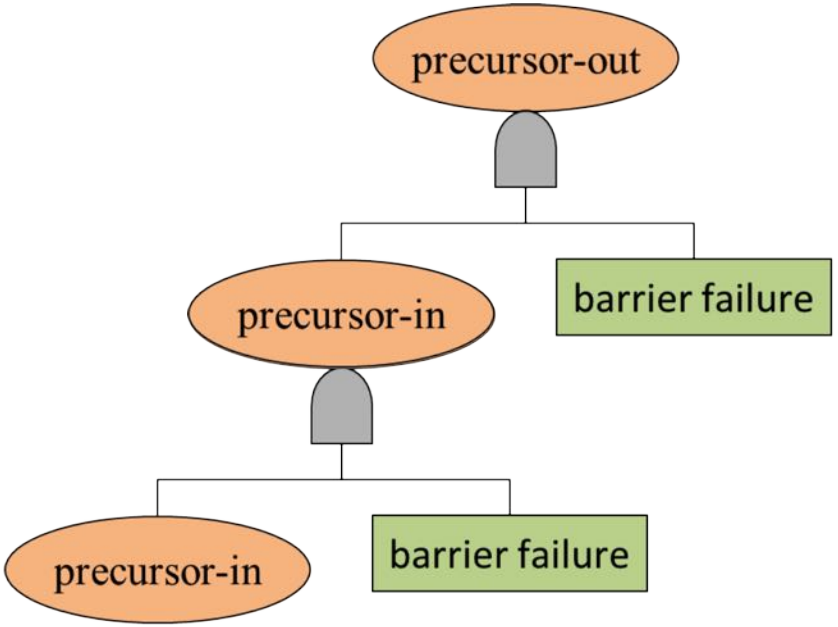
Safety Barriers

- Barriers reduce probability of undesirable event or its consequence
- Highly reliable systems typically designed with multiple barriers



Common Barrier Structure in Fault Tree

- Each barrier has at least one precursor-in (event that activates barrier) and one precursor-out (condition when barrier has failed)
- Precursor-out of one barrier is the precursor-in of the next downstream barrier



Motivation and Objectives

Motivation

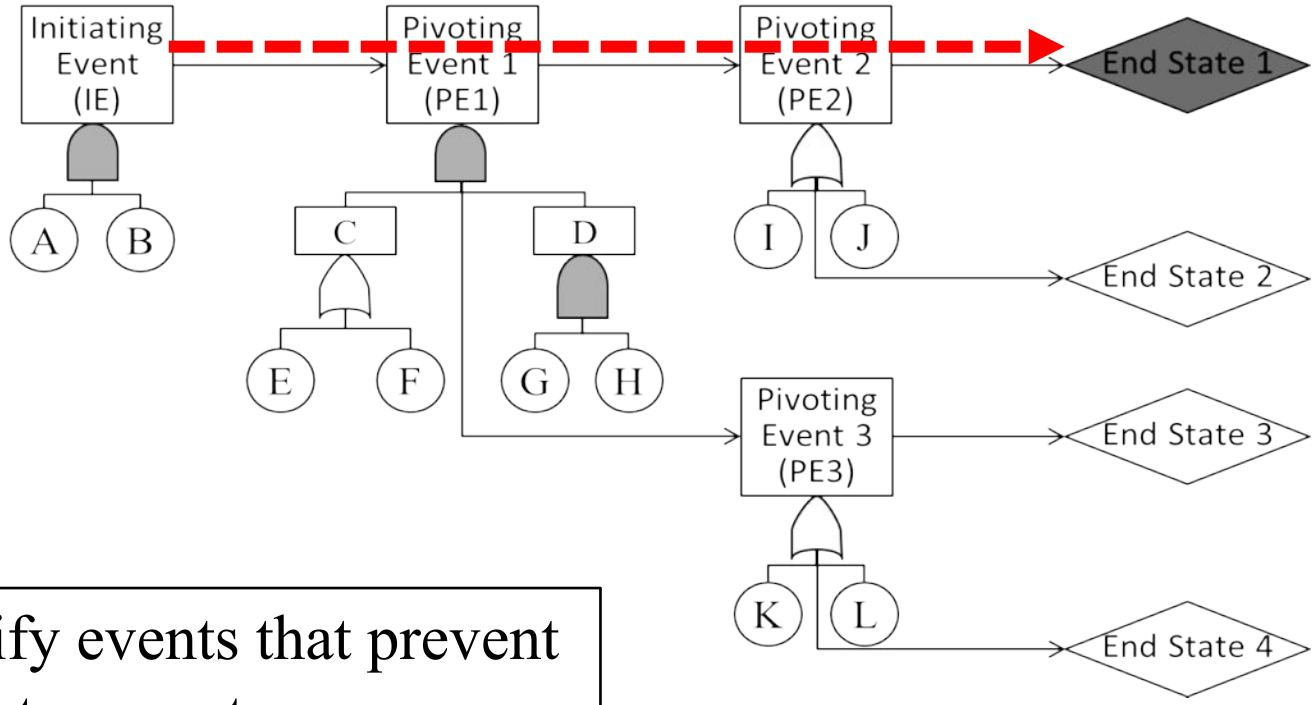
- No formal specification of barriers or precursors in ISAM
  - Model was not designed with precursor-barrier framework in mind
- No system-wide analysis of barrier dependencies

Objectives

- Identification of barriers within ISAM
- Evaluation of overall effectives of barriers
- Identification of common barrier elements for common cause failures

Heuristic for Barrier Identification

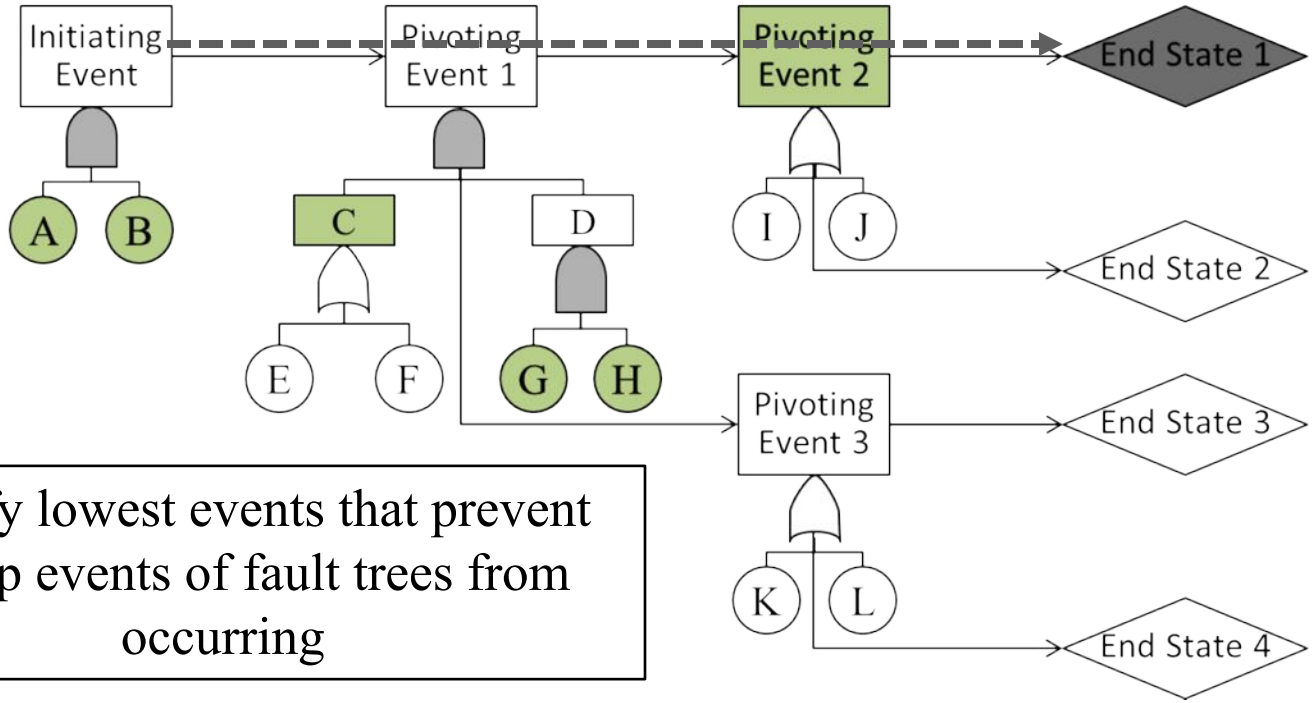
1. Identify all events on the path from the initiating event to the top-most accident scenario (often the most severe)



Identify events that prevent the top-most sequence

Heuristic for Barrier Identification

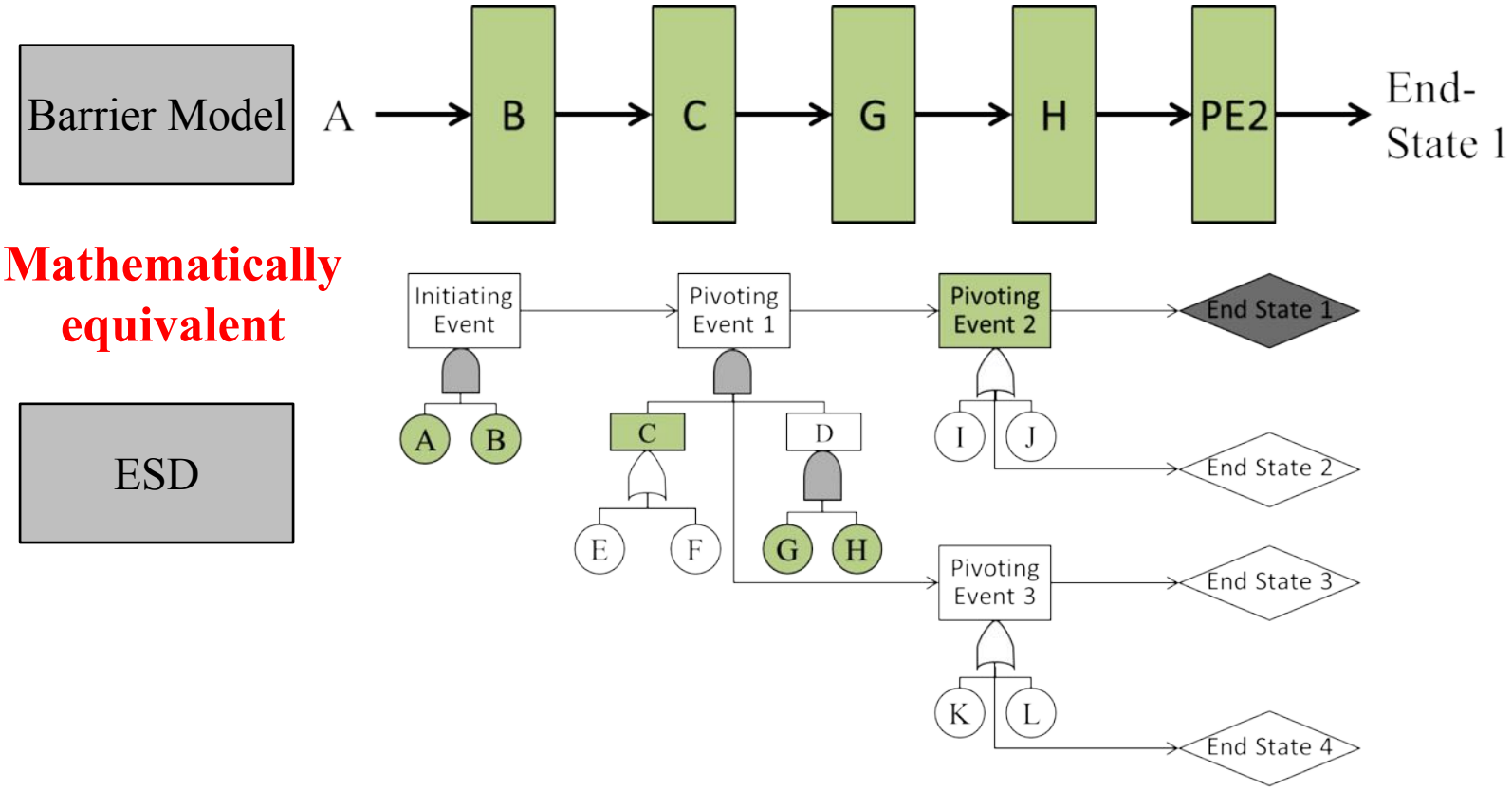
2. Traverse the fault tree underneath each event in a depth-first manner until reaching an OR gate or a basic event
   A. Barriers are the lowest level events identified
   B. The left-most barrier assumed as an initiating precursor



Identify lowest events that prevent the top events of fault trees from occurring

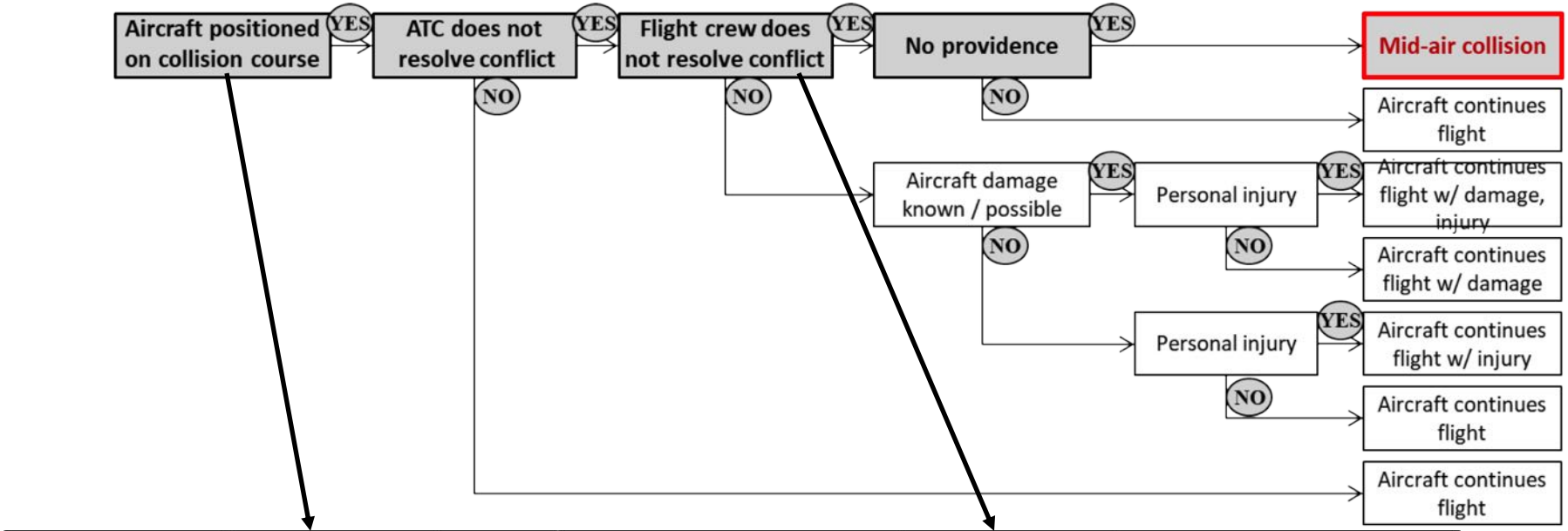
Heuristic for Barrier Identification

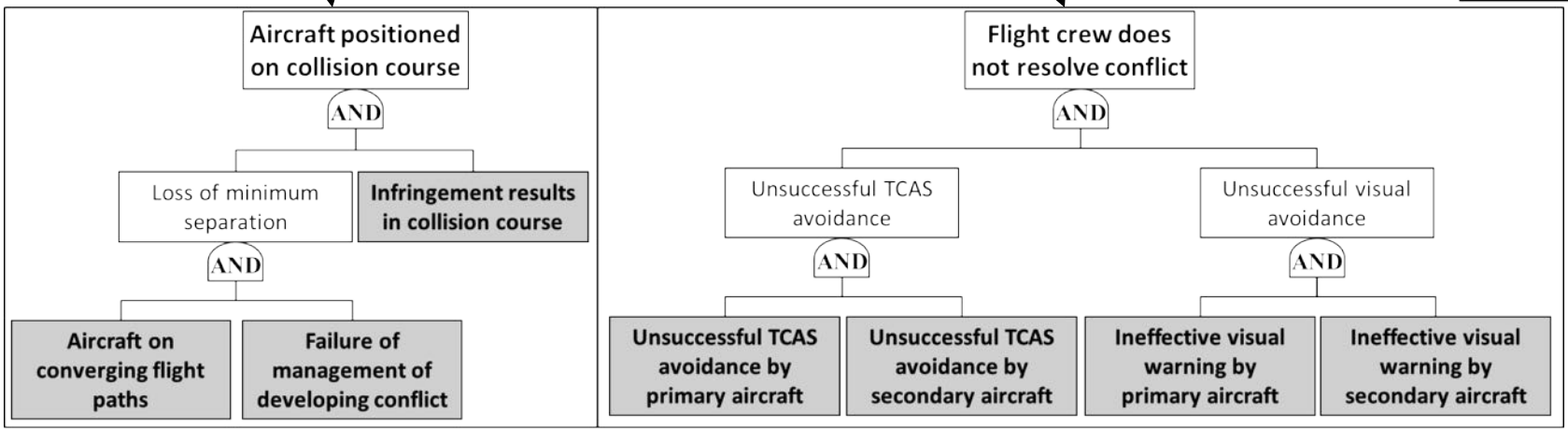
3. Line up identified barriers in the same sequence as events of the accident scenario



Case Study: Mid-air Collision

Barrier Identification



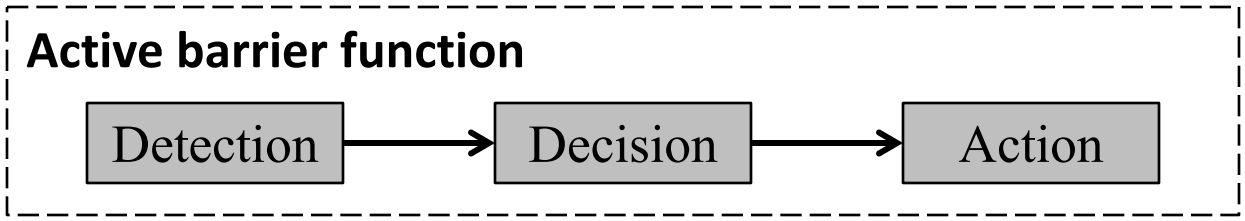


Observation

- By design, heuristic identifies nodes that reduce the probability of a catastrophic accident
- However, not all nodes are *active barriers* (i.e., designed barriers with specific responses to specific conditions)
- We call these elements *circumstantial factors*

Active Safety Barriers

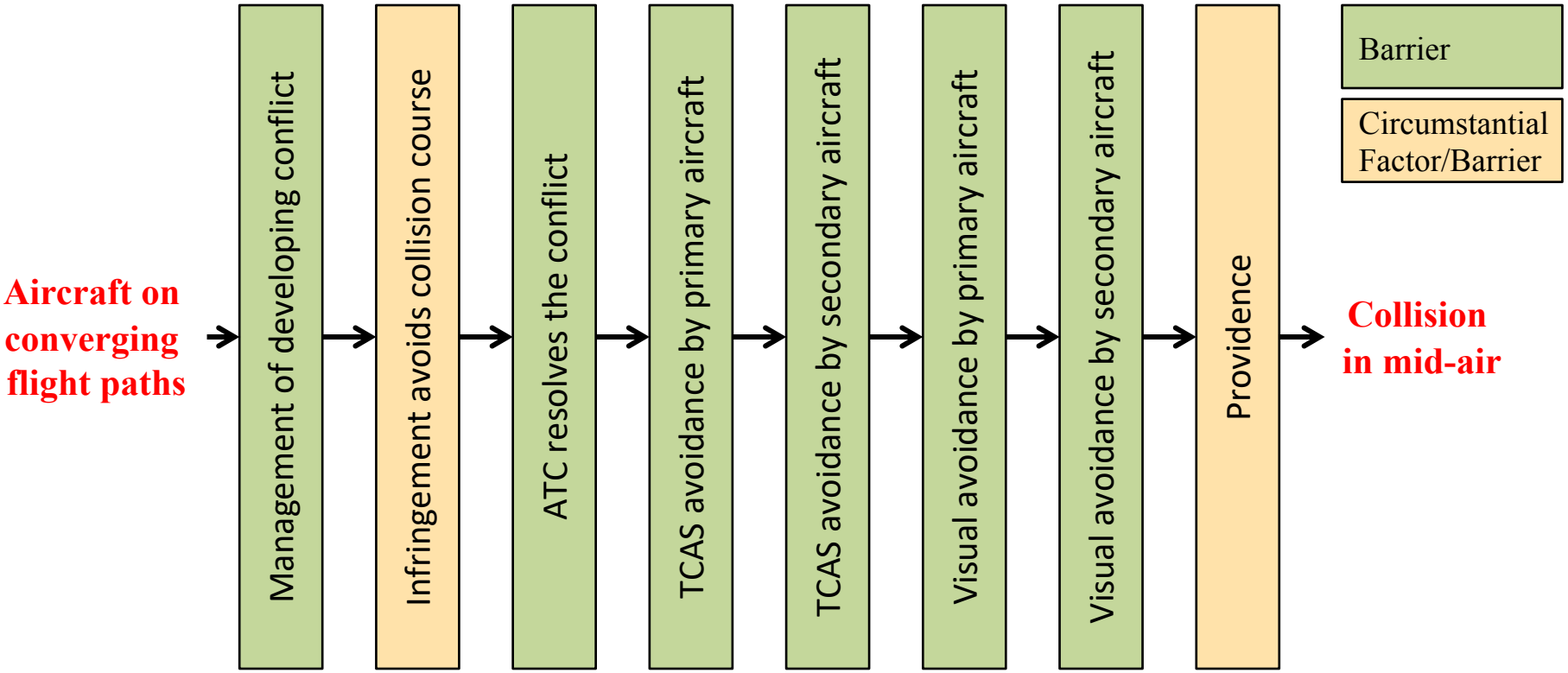
- Barrier function
  - planned to prevent, control, or mitigate the propagation of a condition (event) into an undesired condition (event)
- Barrier system
  - a series of elements that implement a barrier function
- Active barrier elements
  - detection - detect potential hazardous condition
  - decision - made in response to the hazardous condition
  - action - executed based on the decision



Duijm, N. J., 'Safety-barrier diagrams as a safety management tool', 2009.

Case Study: Mid-air Collision

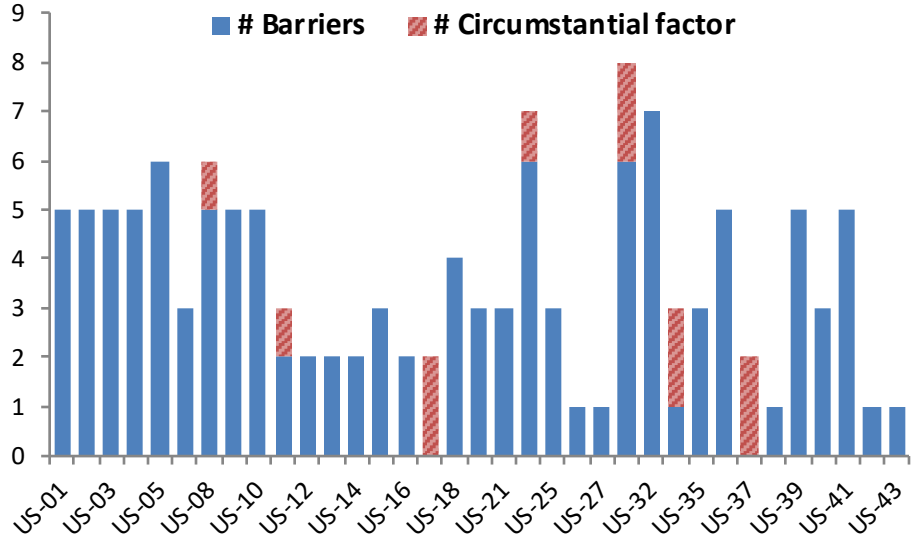
Barrier View



Circumstantial factor/barrier - random circumstances that prevent a worse outcome

ISAM Barrier Analysis

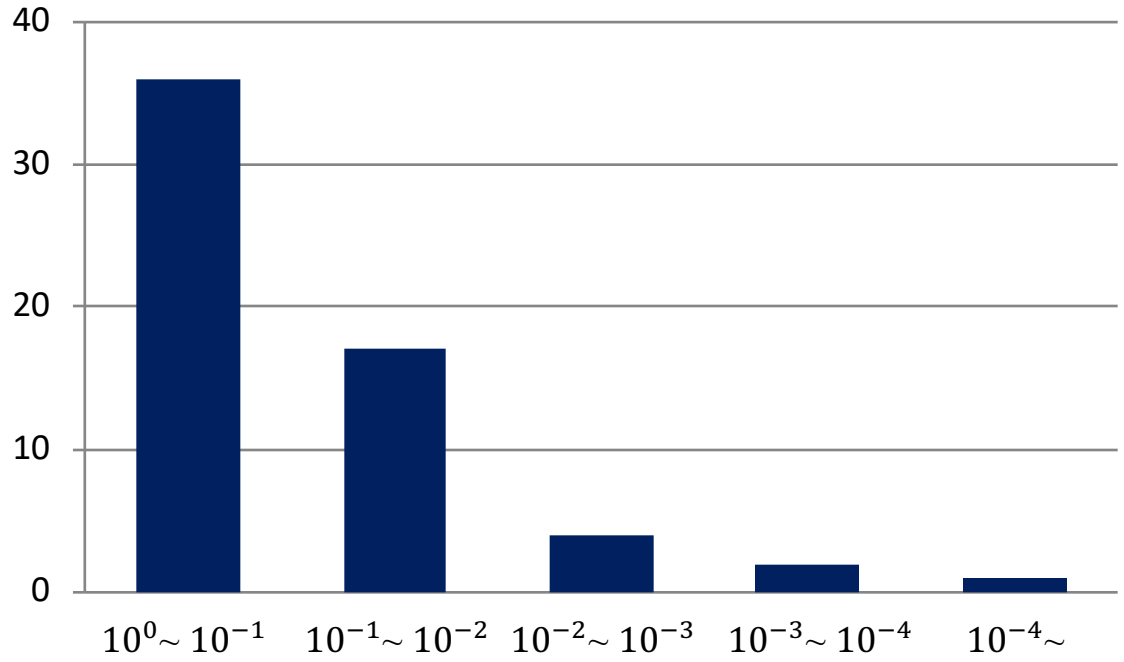
- Barriers per ESD: 1 – 8
  - Includes circumstantial factors
- 16 ESDs have non-zero frequencies in initiating event and end-state



Quantifiable ESDs	US-03, US-09, US-11, US-12, US-13, US-15, US-18, US-19, US-23, US-26, US-27, US-31, US-32, US-35, US-36, US-38
ESDs w/ zero end-state freq.	US-01, US-02, US-04, US-05, US-06, US-08, US-10, US-14, US-16, US-17, US-25, US-37, US-39, US-41, US-42, US-43
ESDs w/ zero init. event freq.	US-21, US-33, US-40

Barrier Effectiveness

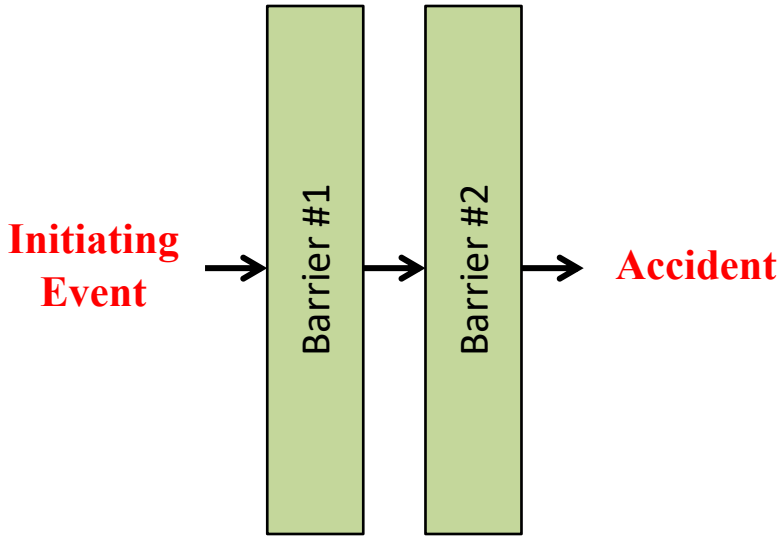
- Effectiveness ≡ Failure probability
- Mean of barrier effectiveness: 0.28 ($\approx 10^{-0.55}$)

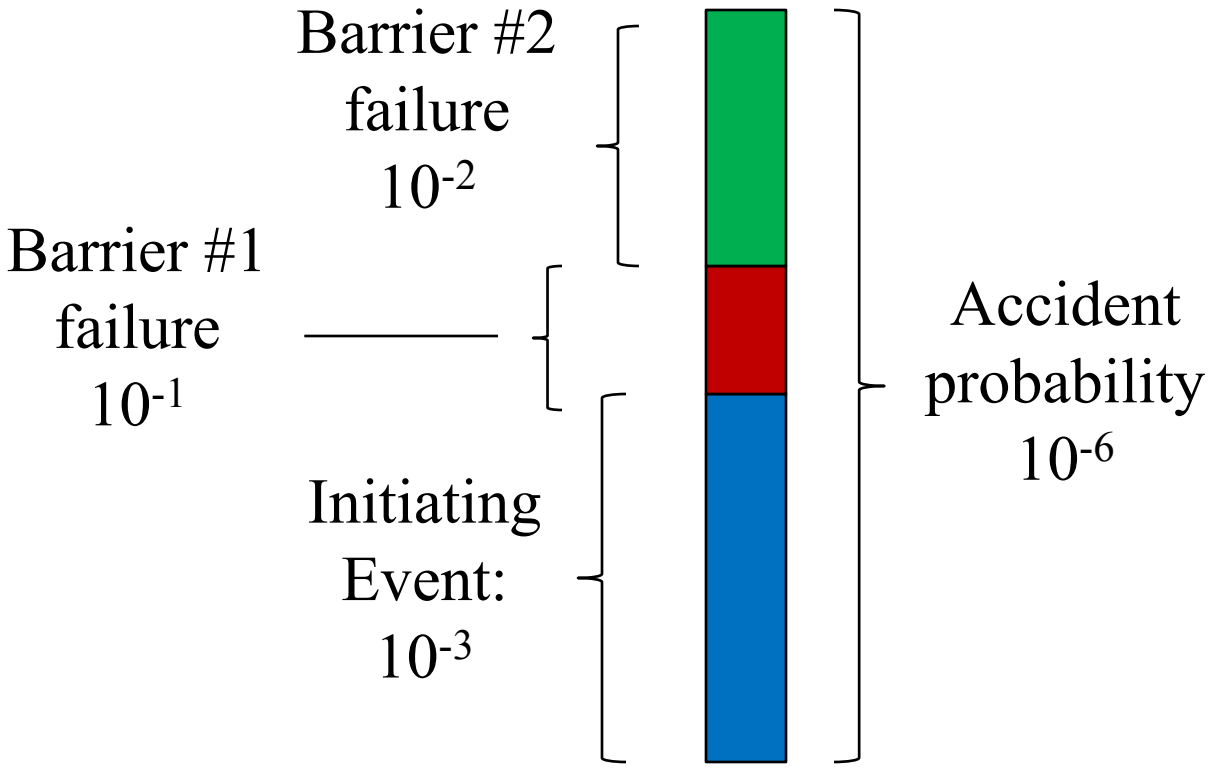


Less effective barrier

More effective barrier

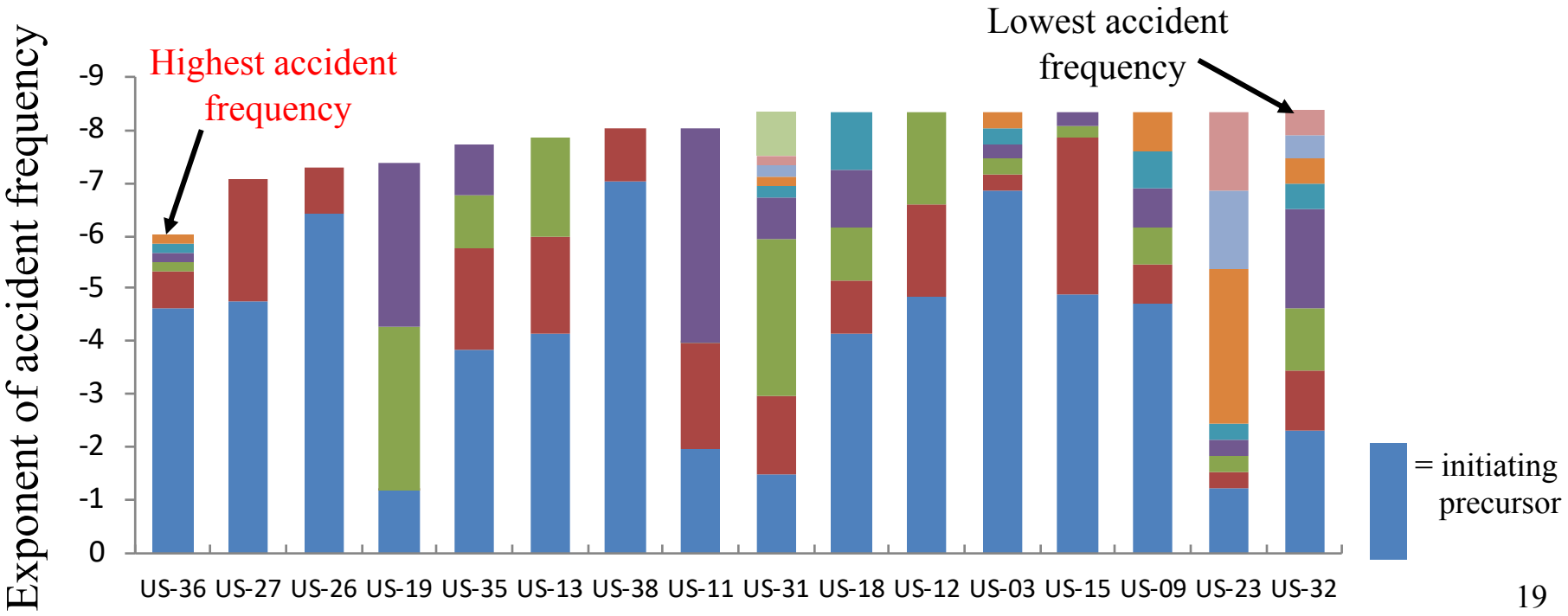
Graphical Representation





Effectiveness by Barriers

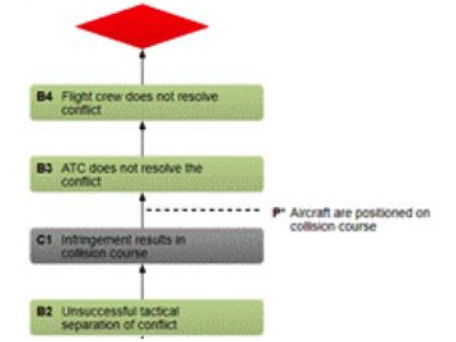
- No obvious trend between accident frequency and # of barriers, initiating precursor frequency
- Risk can be reduced either improving effectiveness of existing barriers or adding more barriers



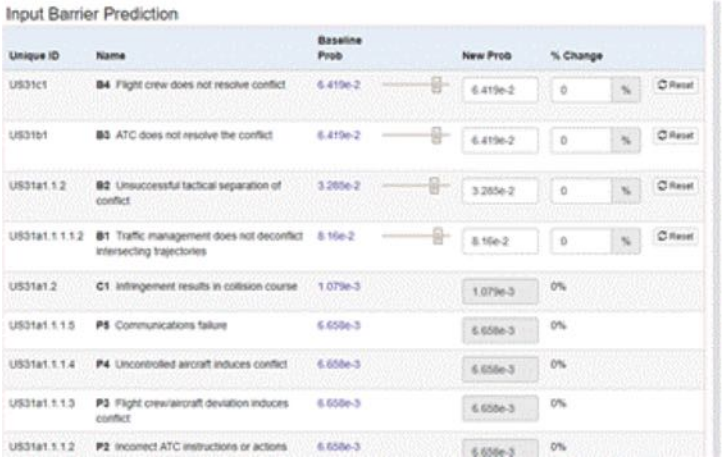
Added ISAM Features

- User can identify barrier nodes in model
- Verification check if selected nodes represent allowable set of barriers
- Generation of "barrier view" of accident
- Barrier "what if" dashboard

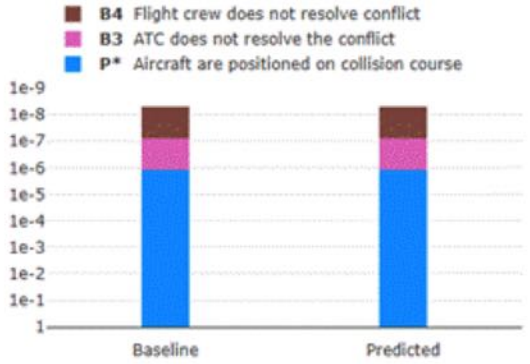
Barrier view



Barrier effectiveness slider



Overall risk (before / after)

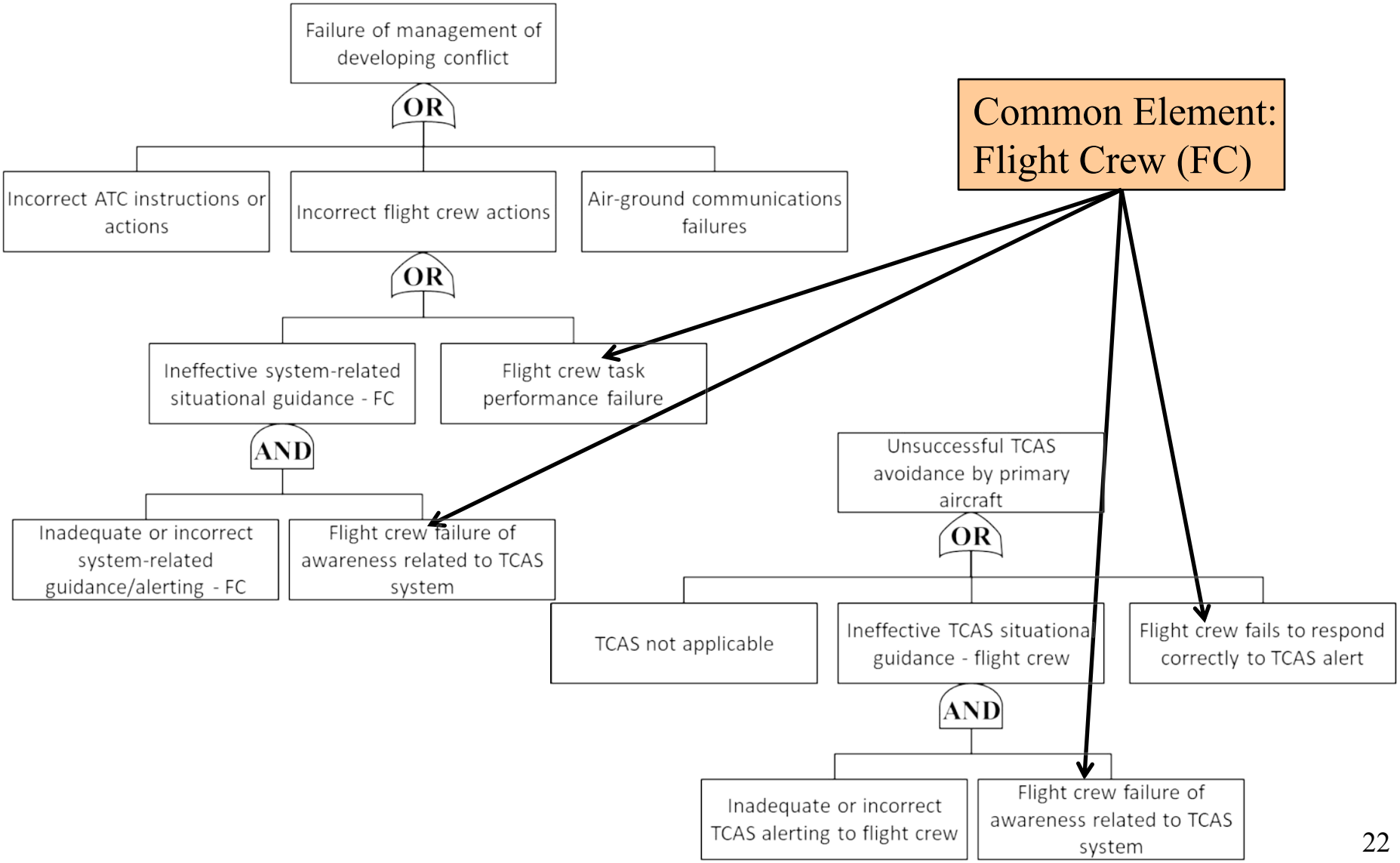


Features implemented by Saab-Sensis

Barrier Element Analysis

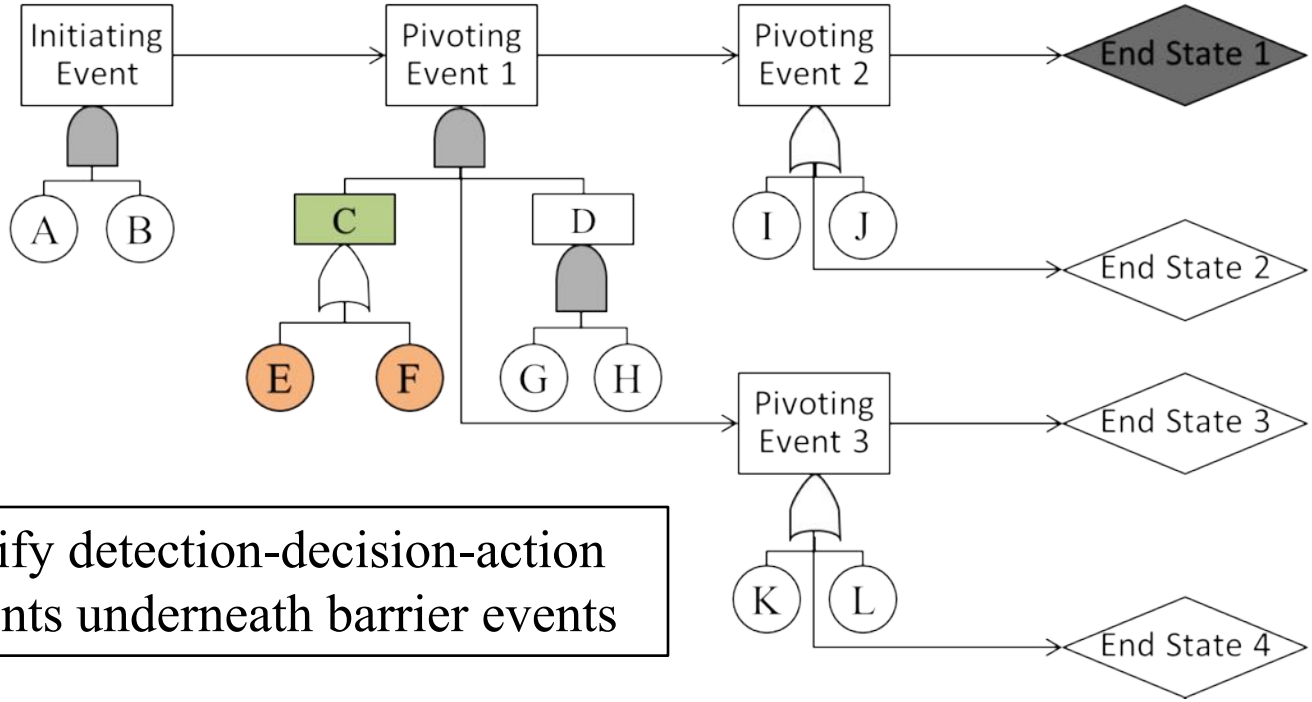
- Barrier functions in different parts of the system may have common elements
  - e.g., data sources, sensors, human agents, etc.
- Barrier failures not independent, since the elements executing the barrier function are shared
- Objective: To show examples of how barriers share elements, and to model dependency between barriers

Example of Common Element



Barrier Elements

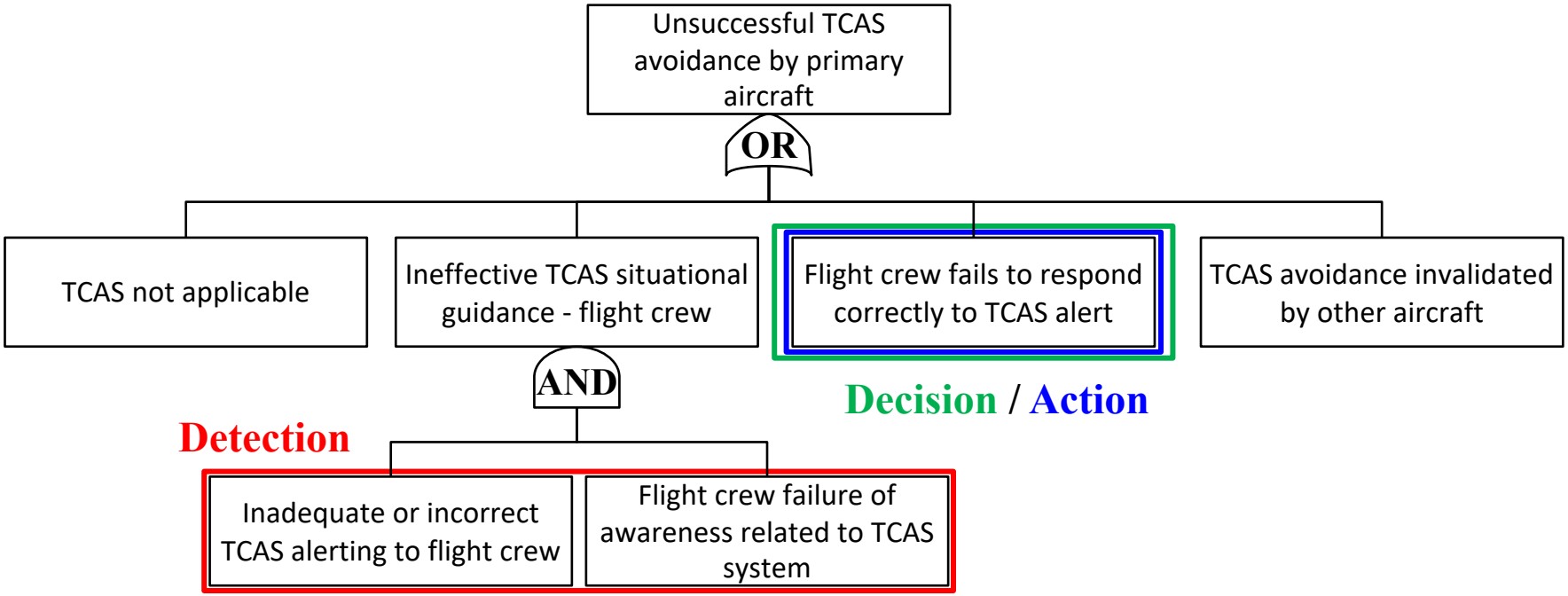
- Further explore fault trees underneath barrier events
- Manually evaluate textual description of nodes to identify detection-decision-action elements



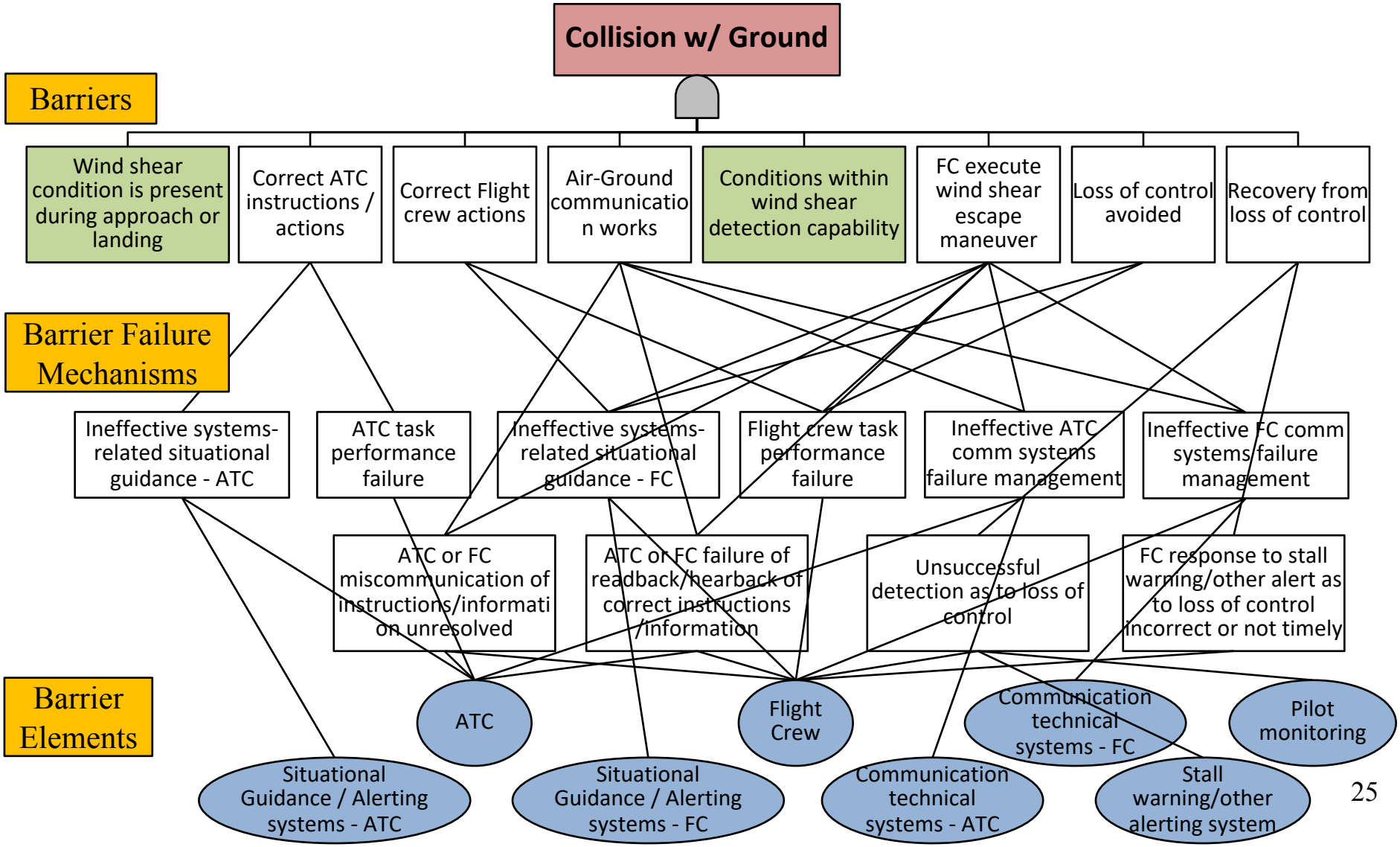
Identify detection-decision-action elements underneath barrier events

Example: Mid-air Collision

Identification of barrier elements



Example: Wind Shear



Barrier Element Matrix

- Create matrix showing which element is shared by which barrier
  1) break-down barriers by failure mechanism through fault trees
  2) find elements involved in barrier failure mechanisms
  3) create matrix barrier by elements

Failure Mechanism	Barrier		
	1	2	3
1	√		
2	√		√
3		√	
4		√	√
5	√		

+

Barrier Element	Failure Mechanism					
	1	2	3	4	5
1		√			√
2	√		√	√	
3			√		√
4		√			

=

Barrier Element	Barrier		
	1	2	3
1	√		√
2	√	√	√
3	√	√	
4	√		√

Example Barrier Element Matrix

Barrier × Barrier Element

* US23 Aircraft encounters wind shear during approach / landing

Barrier / Barrier Element	wind shear condition is present during approach or landing	Correct ATC instructions / actions	Correct Flight crew actions	Air-Ground communication works	Conditions within wind shear detection capability	FC execute wind shear escape maneuver	Loss of control avoided	Recovery from loss of control
ATC	**initiating precursor**	√		√	**Circumstantial factor**	√		
Situational Guidance / Alerting systems - ATC		√						
Flight Crew (FC)			√	√		√	√	√
Situational Guidance / Alerting systems - FC			√			√	√	
Communication technical systems - ATC				√		√		
Communication technical systems - FC				√		√		
Stall warning/other alerting system								√
Pilot monitoring								√

Conclusions

- Identified barriers based on their structural location in model
  - Helped to identify structural errors in the model
  - Can guide more formal structuring of model
- Analysis of overall barrier effectiveness
- Identified barrier elements through detection-decision-action framework
- Ongoing work: Model and analyze dependency between barriers (e.g., beta-factor model)

Questions?

Case Study: Mid-air Collision

barrier	Precursor	detection	decision/action	note
Management of developing conflict	Aircraft on converging flight paths	• Inadequate or incorrect system-related situational guidance/alerting - ATC • ATC failure of awareness related to situational guidance systems	ATC task performance failure	
		• Inadequate or incorrect system-related situational guidance/alerting - FC • FC failure of awareness related to situational guidance systems	Flight crew task performance failure	
		• Air-ground communications failure		Communication
Infringement avoids collision course	Loss of minimum separation			Circumstantial factor

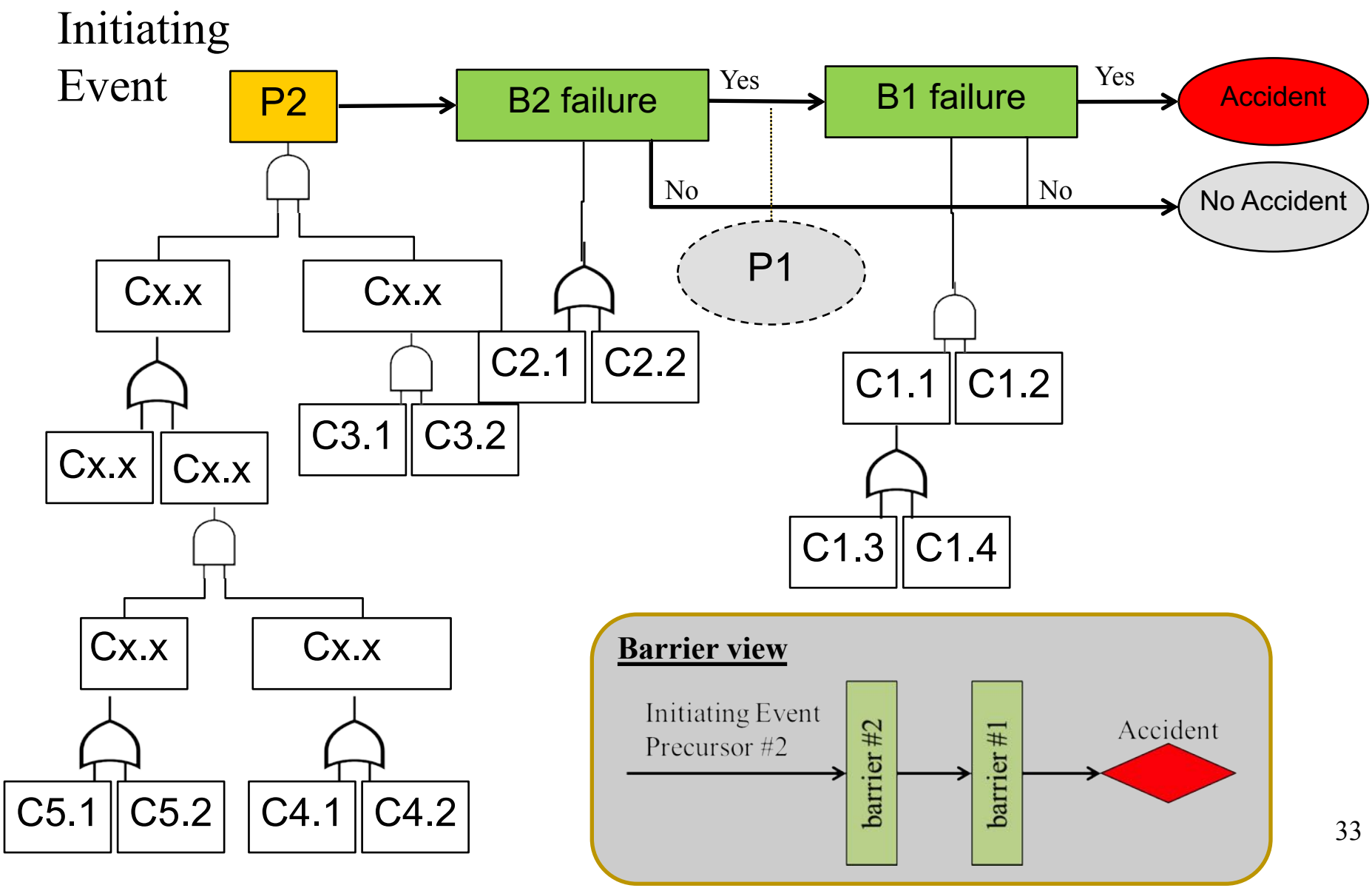
Case Study: Mid-air Collision

barrier	Precursor	detection	decision/action	note
ATC resolves the conflict	Aircraft on collision course	• Inadequate or incorrect Conflict Alert system warning • ATC failure of awareness related to conflict alert system • Ineffective other ATC warning	ATC task performance failure	
			Incorrect FC response to ATC instructions	
		• Air-ground communications failure		Communication
TCAS avoidance by primary a/c	ATC failure to resolve the conflict	• Inadequate or incorrect TCAS alerting to FC • FC failure of awareness related to TCAS system	Flight crew fails to respond correctly to TCAS alert	(Bad luck) TCAS not applicable (Bad luck) TCAS avoidance invalidated by other aircraft
TCAS avoidance by secondary a/c	TCAS failure by primary a/c			

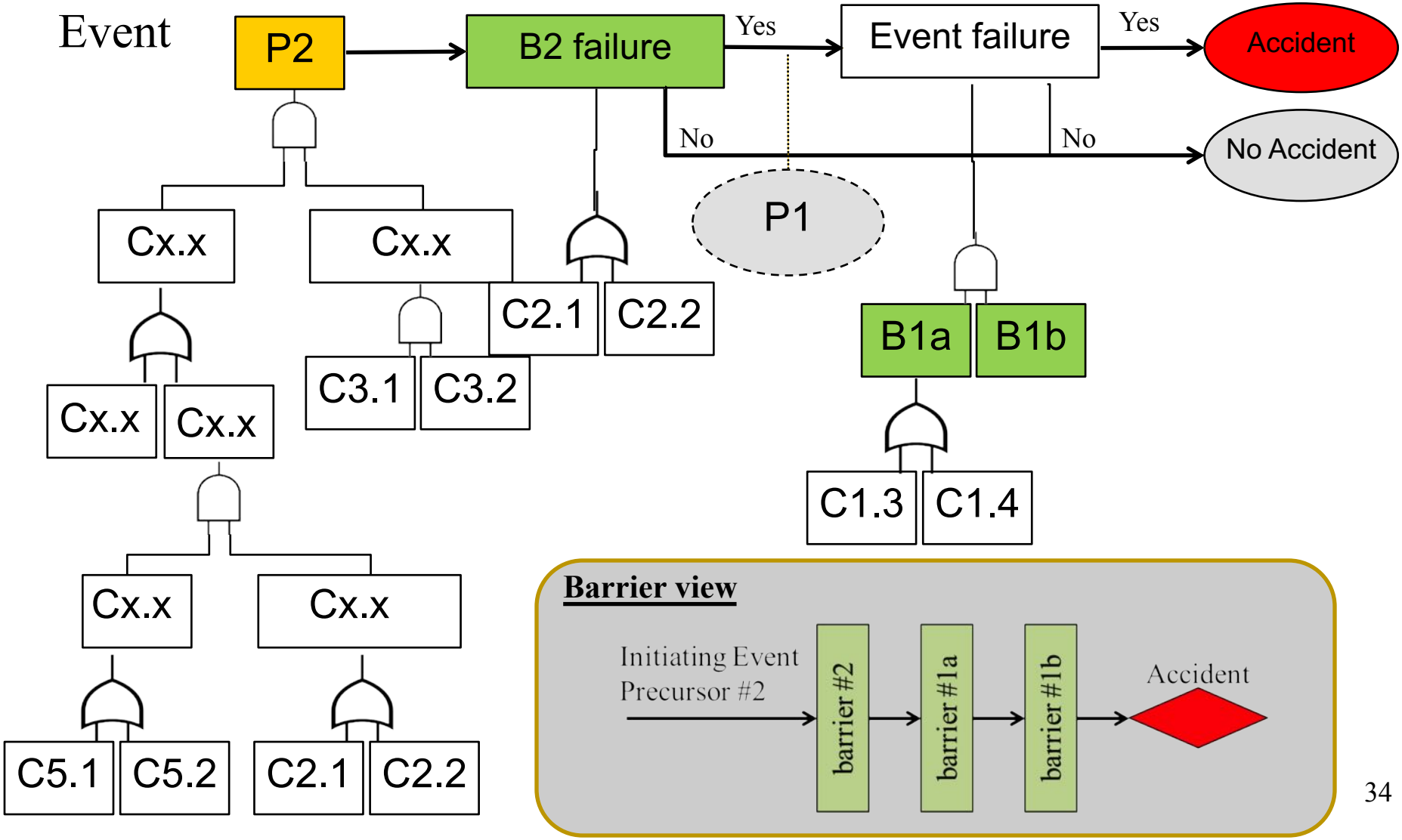
Case Study: Mid-air Collision

barrier	Precursor	detection	decision/action	note
Visual avoidance by primary a/c	TCAS failure by both a/c	• FC fail to correctly observe visible aircraft in time	Flight crew fails to respond correctly	(Bad luck) Other aircraft effectively invisible (Bad luck) Visual avoidance invalidated by other aircraft
Visual avoidance by secondary a/c	Visual avoidance failure by primary a/c			
Providence	Visual avoidance failure by both a/c			Circumstantial factor

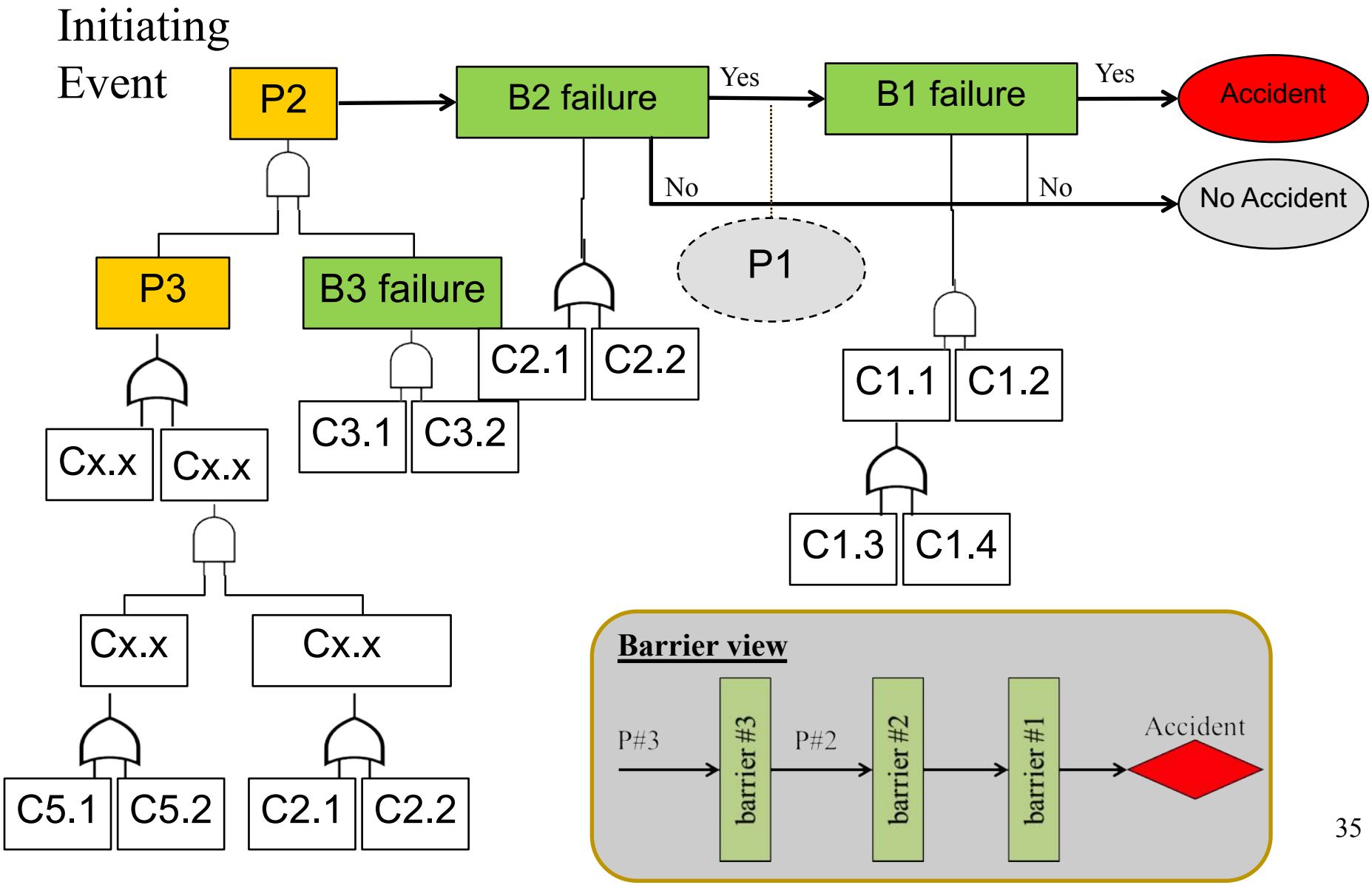
Example


Initiating Event
P2
B2 failure
Yes
B1 failure
Yes
Accident
No
No
No Accident
P1
Cx.x
Cx.x
C2.1
C2.2
C3.1
C3.2
Cx.x
Cx.x
C1.1
C1.2
C1.3
C1.4
Cx.x
Cx.x
C5.1
C5.2
C4.1
C4.2
Barrier view
Initiating Event
Precursor #2
barrier #2
barrier #1
Accident

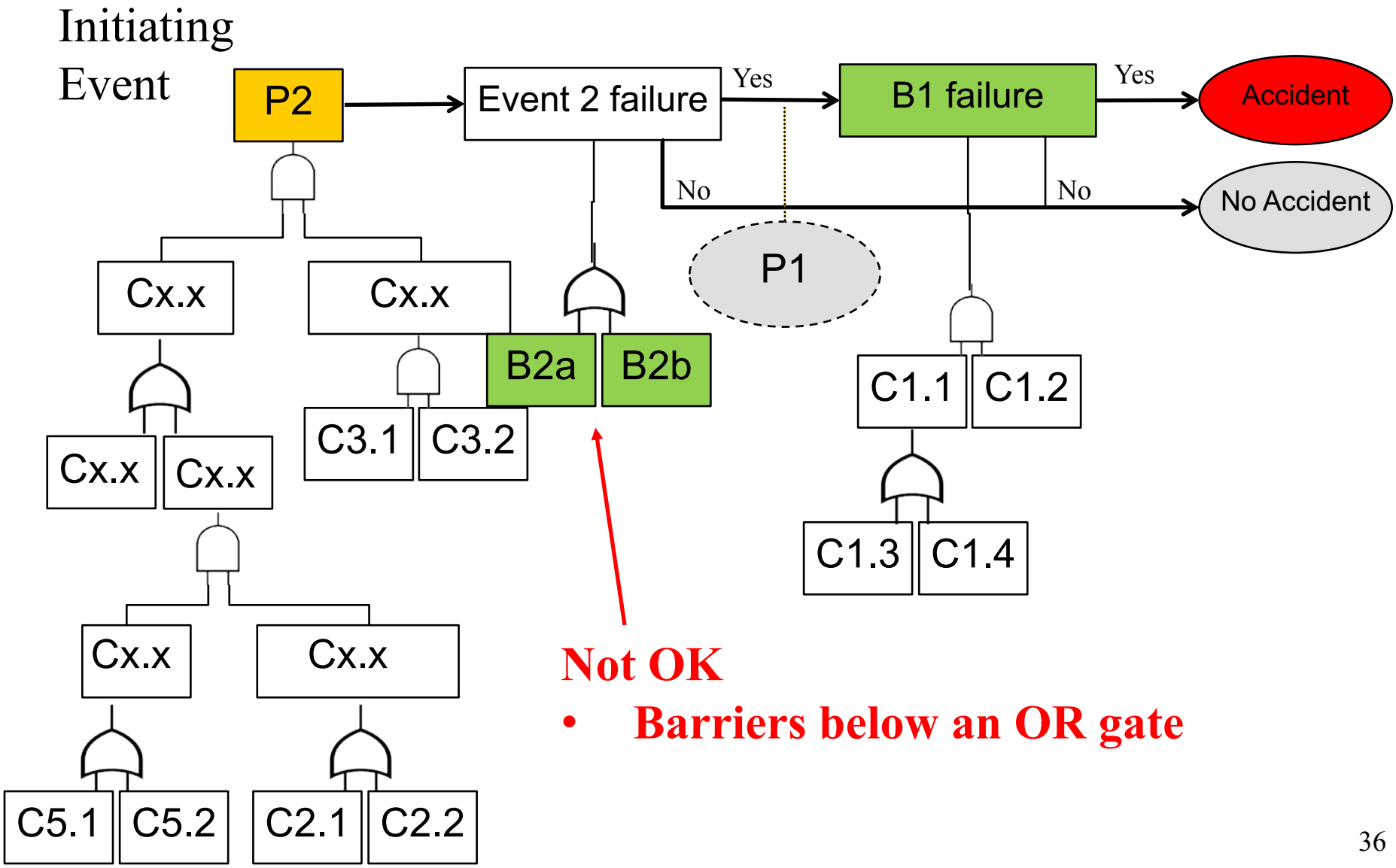
Example


Initiating Event
P2
B2 failure
Yes
Event failure
Yes
Accident
No
No
No Accident
P1
Cx.x
Cx.x
C2.1
C2.2
C3.1
C3.2
Cx.x
Cx.x
B1a
B1b
C1.3
C1.4
Cx.x
Cx.x
C5.1
C5.2
C2.1
C2.2
Barrier view
Initiating Event
Precursor #2
barrier #2
barrier #1a
barrier #1b
Accident

Example


Initiating Event
P2
B2 failure
Yes
B1 failure
Yes
Accident
No
No
No Accident
P1
P3
B3 failure
C2.1
C2.2
C3.1
C3.2
C1.1
C1.2
Cx.x
Cx.x
C1.3
C1.4
Cx.x
Cx.x
C5.1
C5.2
C2.1
C2.2
Barrier view
P#3
barrier #3
P#2
barrier #2
barrier #1
Accident

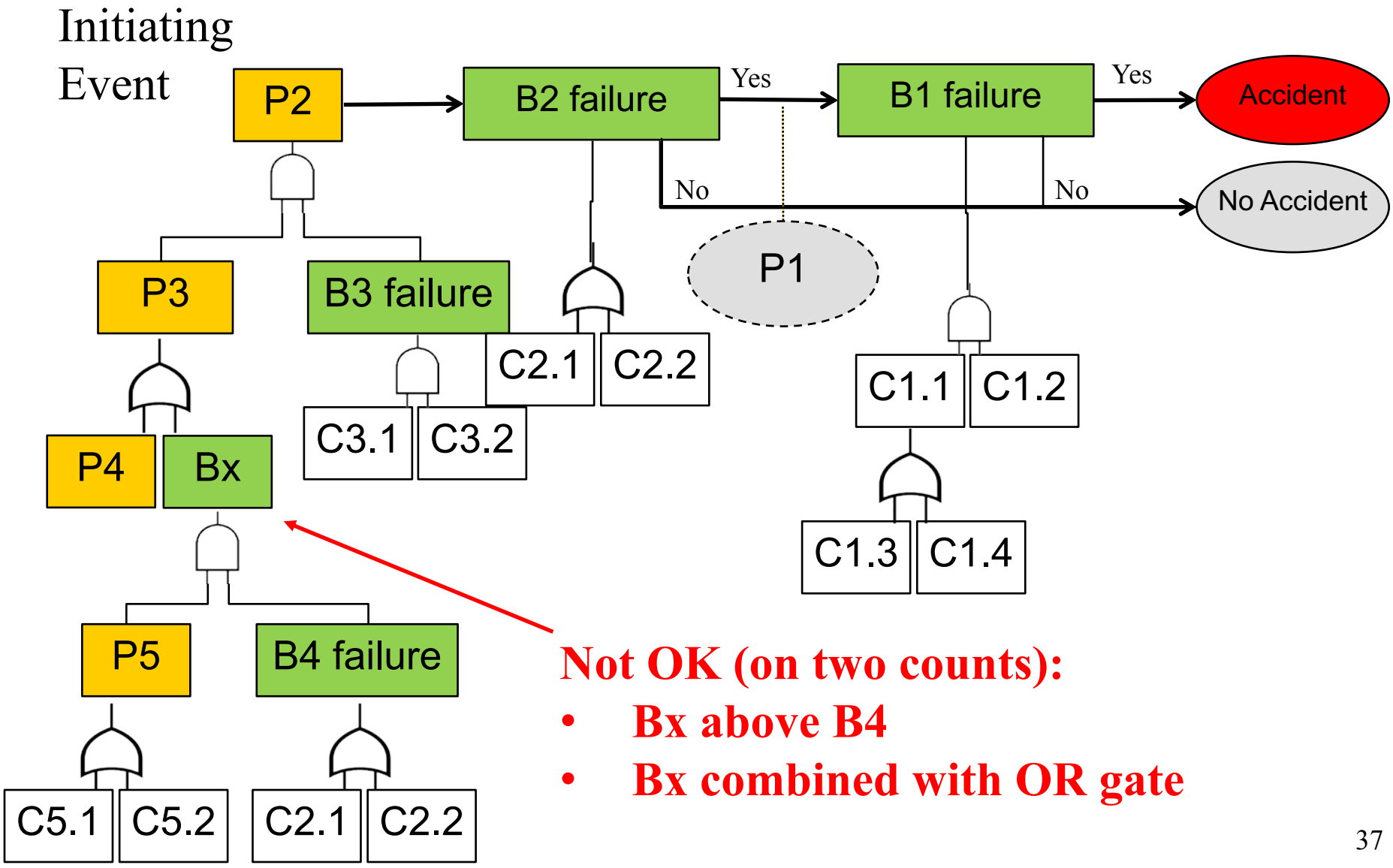
Counter-Example



Not OK

- **Barriers below an OR gate**

Counter-Example



Not OK (on two counts):

- **Bx above B4**
- **Bx combined with OR gate**

The Rules: 1 - 4

Rule 1 - Barriers Have No Ancestor Barriers

Description: No barrier in any fault tree shall have a barrier as an ancestor.

Scope: All fault trees

Rule 2 - Barriers are Children of AND Gates

Description: Fault tree nodes designated as a barrier shall always be children of AND-gate nodes

Scope: All fault trees

Rule 3 - Barriers in Initiating Event Fault Tree Paired with One Precursor

Description: If a barrier exists in the initiating event fault tree, the barrier shall be paired with one and only one precursor, and the precursor shall be a sibling of the barrier.

Scope: Initiating event fault tree

Rule 4 - Precursors Combined with (X)OR Gates

Description: Precursor fault tree nodes shall be combined using OR or XOR gates only. In other words, if two precursors are siblings then their parent node shall have an OR or an XOR gate.

Scope: Initiating event tree

The Rules: 5 - 7

Rule 5 - Fault Tree Top Event Node Class Matches Containing Event Node Class

Description: The top event in a fault tree shall have the same node class as the event that contains the fault tree. Note: this rule is needed because fault trees and event sequences have different representations in the ISAM model, and thus we need a mechanism to synchronize the data in the fault tree root node and its paired event.

Scope: All fault trees

Rule 6 - Precursors Exist In Initiating Event Fault Tree Only

Description: Nodes in the initiating event fault tree are the only ones that can be designated as precursors. All other fault trees cannot contain precursor nodes.

Scope: All fault trees

Rule 7 - Pivotal Event Fault Tree Base Events Have Exactly One Barrier Ancestor

Description: Each base event in each pivotal event fault tree must have one barrier as an ancestor.

Scope: Pivotal event fault trees

The Rules: 8 – 10

Rule 8 - Barrier Nodes in Pivotal Event Fault Trees Are Descendants of AND Nodes Only

Description: If a barrier node exists in a pivotal event fault tree, then all of the ancestors of the barrier node must contain AND gates.

Scope: Pivotal event fault trees

Rule 9 - Base Events Contained in Initiating Event Fault Tree Have One or Zero Barrier Ancestors

Description: Base events in the initiating event fault tree can have at most one barrier ancestor node. (They can have no barrier ancestor node.)

Scope: Initiating event fault tree

Rule 10 - Initiating Event Fault Tree Top Event Is Precursor If Tree Contains No Barriers

Description: If the initiating event fault tree contains no barrier nodes, then the top event of the fault tree must be designated a precursor.

Scope: Initiating event fault tree

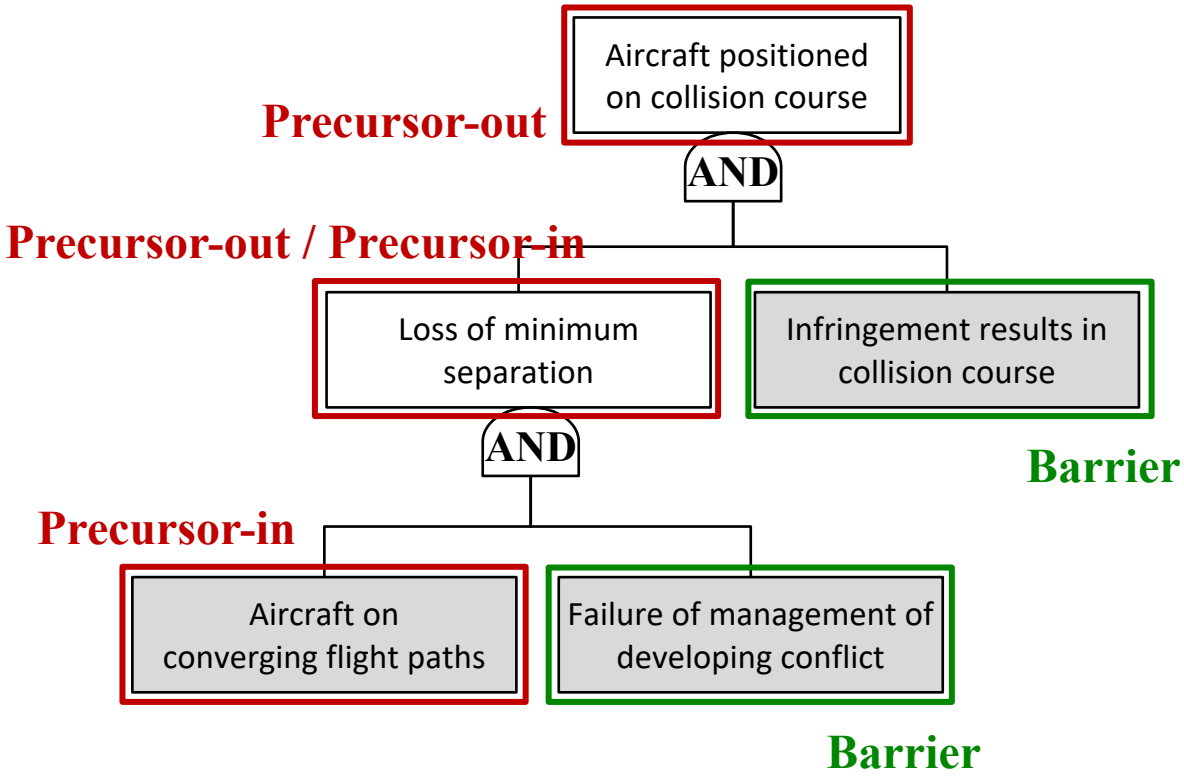
The Rules: 11

Rule 11 - Ancestors of Barriers in Initiating Event Fault Tree Are Precursors

Description: All ancestors of a barrier node in the initiating event fault tree must be precursors. This is a simplification of the rule you stated on p.19 of the attached slides. I think if all of the rules are satisfied then the restriction on sibling fault tree nodes being precursors is also satisfied.

Scope: Initiating event fault tree

Case Study: Mid-air Collision



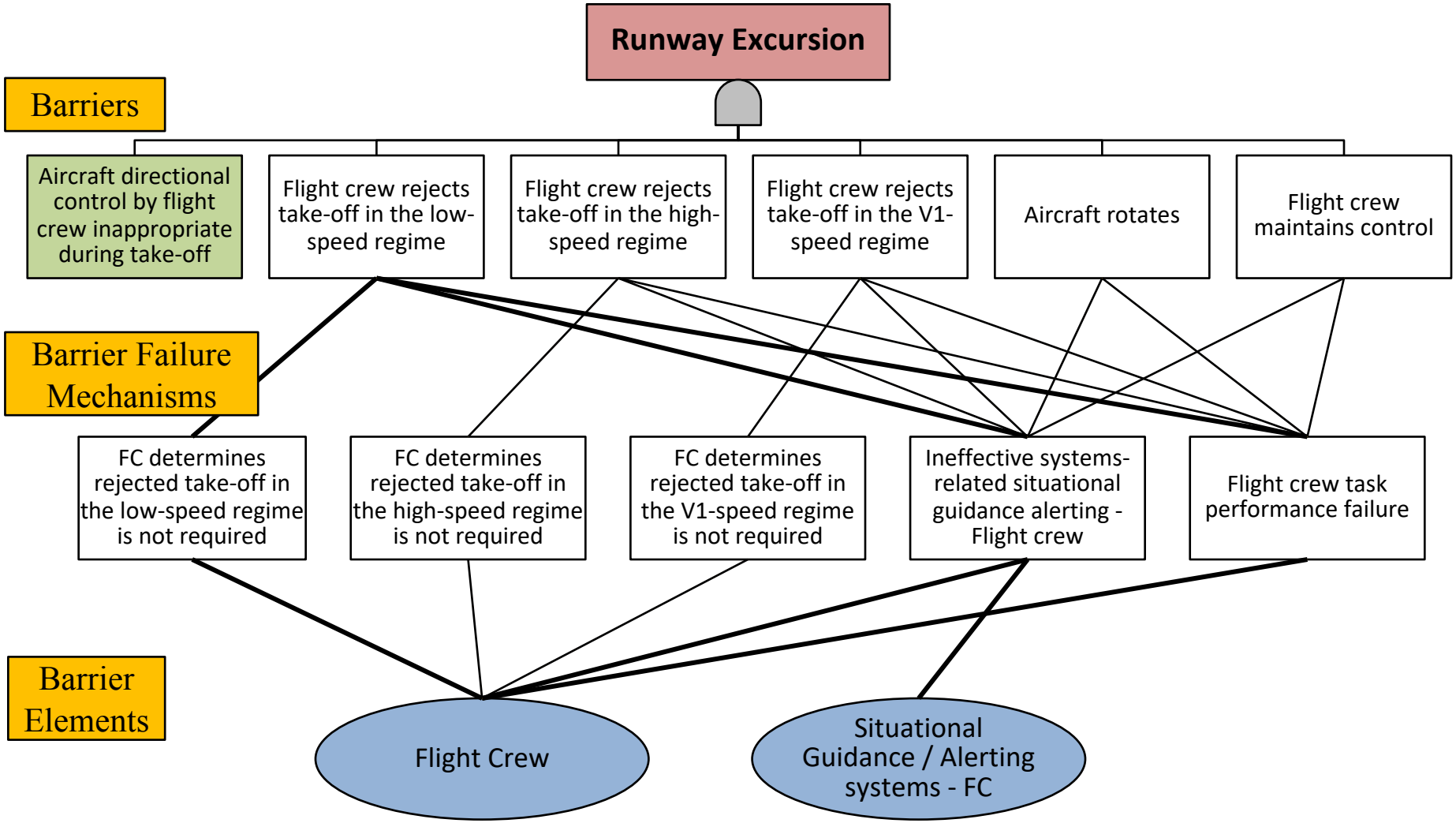
Example Barrier Break-Down Matrix

* US03 Aircraft directional control by flight crew inappropriate during take-off						
Barrier Failure Mechanism	Aircraft directional control by flight crew inappropriate during take-off	Flight crew rejects take-off in the low-speed regime	Flight crew rejects take-off in the high-speed regime	Flight crew rejects take-off in the V1-speed regime	Aircraft rotates	Flight crew maintains control
Ineffective systems-related situational guidance alerting - Flight crew	**initiating precursor**	√	√	√	√	√
Flight crew task performance failure		√	√	√	√	√
Flight crew determines rejected take-off in the low-speed regime is not required		√				
Flight crew determines rejected take-off in the high-speed regime is not required			√			
Flight crew determines rejected take-off in the V1-speed regime is not required				√		

Failure Mechanism Barrier Element	Ineffective systems-related situational guidance alerting - Flight crew	Flight crew task performance failure	Flight crew determines rejected take-off in the low-speed regime is not required	Flight crew determines rejected take-off in the high-speed regime is not required	Flight crew determines rejected take-off in the V1-speed regime is not required	
Flight Crew (FC)	√	√	√	√	√	
Situational Guidance / Alerting systems - FC	√					

Barrier Barrier Element	Aircraft directional control by flight crew inappropriate during take-off	Flight crew rejects take-off in the low-speed regime	Flight crew rejects take-off in the high-speed regime	Flight crew rejects take-off in the V1-speed regime	Aircraft rotates	Flight crew maintains control
Flight Crew (FC)	**initiating precursor**	√	√	√	√	√
Situational Guidance / Alerting systems - FC		√	√	√	√	√

Diagram view (US03)



Example Barrier Break-Down Matrix

Barrier × Failure Mechanism

g approach / landing

Barrier / FT Node	present during approach or landing	Correct ATC instructions / actions	Correct Flight crew actions	Air-Ground communication works	Conditions within wind shear detection capability	FC execute wind shear escape maneuver	Loss of control avoided	Recovery from loss of control		
Ineffective systems-related situational guidance - ATC	initiating precursor	√			Circumstantial factor					
ATC task performance failure		√								
Ineffective systems-related situational guidance - Flight Crew			√			√	√			
Flight crew task performance failure			√			√	√			
Ineffective ATC comm systems failure management				√		√				
Ineffective Flight crew comm systems failure management				√		√				
ATC or flight crew miscommunication of instructions/information unresolved				√		√				
ATC or flight crew failure of readback/hearback of correct instructions/information				√		√				
Unsuccessful detection as to loss of control								√		
Flight crew response to stall warning/other alert as to loss of control incorrect or not timely								√		

Failure Mechanism × Barrier Element

	performance	Ineffective ATC comm systems failure management	Ineffective Flight crew comm systems failure management	ATC or flight crew miscommunication of instructions/information unresolved	ATC or flight crew failure of readback/hearback of correct instructions/information	Unsuccessful detection as to loss of control	Flight crew response to stall warning/other alert as to loss of control incorrect or not timely
		√		√	√		
Situational Guidance / Alerting systems - ATC	√						
Flight Crew (FC)			√	√	√	√	√
Situational Guidance / Alerting systems - FC							
Communication technical systems - ATC		√					
Communication technical systems - FC			√				
Stall warning/other alerting system						√	
Pilot monitoring						√	

Barrier × Barrier Elements

	Flight crew actions	Air-Ground communication works	Conditions within wind shear detection capability	FC execute wind shear escape maneuver	Loss of control avoided	Recovery from loss of control		
		√	Circumstantial factor	√				
Situational Guidance / Alerting systems - ATC	√							
Flight Crew (FC)	√	√		√	√	√		
Situational Guidance / Alerting systems - FC	√			√	√			
Communication technical systems - ATC		√		√				
Communication technical systems - FC		√		√				
Stall warning/other alerting system						√		
Pilot monitoring						√		

Modeling Dependency

- Beta (β) factor Model can be applied to model common cause failure (ccf)
  - Assume identical components w/ constant failure rate, λ
  - Components fail independently w/ rate $(1-\beta)\lambda$, simultaneously w/ rate $\beta\lambda$ due to common cause