MBSE and Safety Analysis

Bruce Powel Douglass, Ph.D.
Senior Principal Agile Systems Engineer, MITRE Corporation
www.bruce-douglass.com
Twitter: @IronmanBruce

MBSE and Safety

- When / where is safety considered in MBSE
  - Ans: YES

- Initial safety
  - In the context of use case / user story analysis, coherent sets of requirements are considered. This consideration is *black box* and is done on a *per use case basis* and includes:
    - Functionality
    - Qualities of service (e.g. performance)
    - Logical data schema
    - Logical interfaces
    - Identification of system functions
    - Cyber-physical security
    - Reliability
    - **Safety**
- Then these elements are combined into an architectural model and safety must be reconsidered as technological decisions are made

What is Safety?

- **Safety** is freedom from accidents or losses.
  - Normally concerned with human or animal death or injury
  - May be applied to any system in which you desire to avoid certain outcomes
- **Safety** is **not reliability**!
  - Reliability is the probability that a system will perform its intended function satisfactorily.
  - Reliability is a stochastic measure system function delivery
- **Safety** is **not security**!
  - Security is protection or defense against attack, interference, or espionage.
  - Note: the German word *sicherheit* relates to both security and safety, but we draw a distinction in English
- **Dependability** is the term used for the integration of Safety, Reliability, and Security
- **Resilience** is the term for the ability of a system to provide service under different, often unexpected, circumstances. It includes Dependability and Adaptability.

Safety-Related Concepts

- **Accident** is a loss of some kind, such as injury, death, or equipment damage
  - AKA mishap
- **Risk** is a combination of the likelihood of an accident and its severity:

  risk = p(a) * s(a)
- A **Hazard** is a set of conditions and/or events that leads to an accident. That is, hazards result in accidents
  - Hazards are predictable and therefore controllable
  - A safety-relevant system contains two kinds of hazards
    - Intrinsic hazards
      - Hazards due to the inherent job of the system
    - Extrinsic hazards
      - Hazards due to the operational environment
    - Technology hazards
      - Hazards due to the addition of specific technological solutions
- A **safety control measure** is an action or mechanism to improve the safety of the system by either
  - Reducing the severity
  - Reducing the likelihood

A note about safety control measures

- Safety control measures always do at least one of the following
  - Make the hazard less likely to manifest
  - Make the occurrence of the hazard less severe

- Example: Automotive braking system
  - Hazard: Inability to brake
    - Control measure 1 – decrease likelihood
      - Fault: brake pedal position sensor fails
      - Control measure: have 3 brake pedal position sensors and have them vote
      - Outcome: For this fault to manifest the hazard, multiple sensors must fail. Assuming independence of failure mode, this makes the hazard less likely
    - Control measure 2 – decrease severity
      - Fault: brake pedal position sensor fails
      - Control measure: air bag inflates in 20ms of crash detection
      - Outcome: Damage to vehicle occupants in minimized via active shock absorption with the air bag, lessening the forces applied to occupants

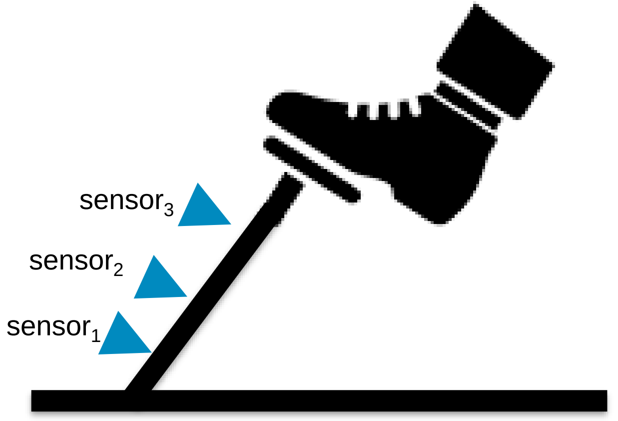
A note about safety control measures

- During safety analysis, safety control measures turn into safety requirements for a design means to achieve a safety goal

- A SE control measures should specify **what** and **how well** some aspect is to be controlled but **not how** it should be controlled: For example:
  - *The braking systems shall be able to receive user braking inputs in the presence of a single point failure of the pedal assembly sensor with a failure rate of less than 10^{-9}* per year,
  - **NOT:** *There shall be three redundant brake pedal position sensors.*

Safety Measure Requirement

The braking systems shall be able to receive user braking inputs in the presence of a single point failure of the pedal assembly sensor with a failure rate of less than 10^{-9}



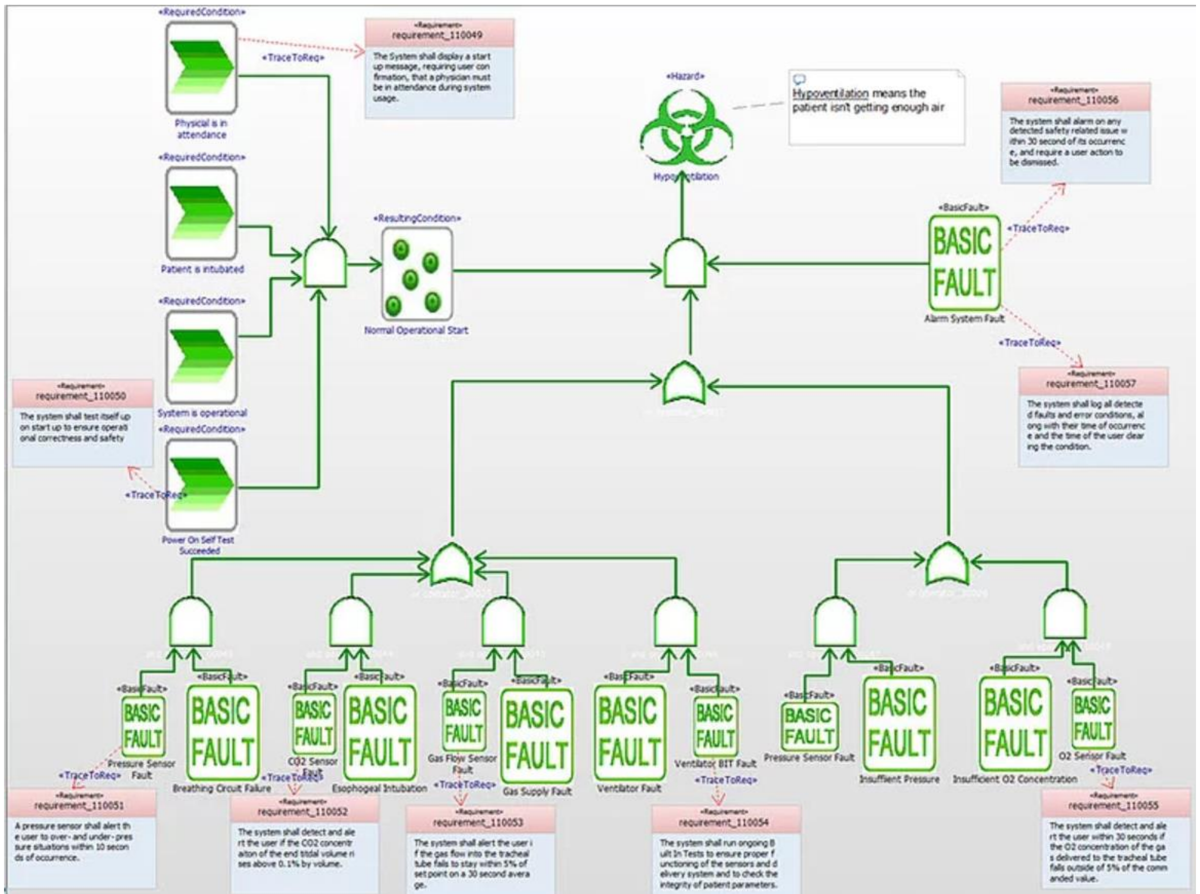
Safety Measure Design

FMEA and FMECA

- FMEA is a reliability analysis, FMECA can be used for safety analysis
  - FMEA/FMECA is a bottom-up approach and should be rarely used in systems engineering but can be used to assess an existing design
  - FMEA/FMECA cannot be performed until design is complete or is at least underway
- FMEA looks at the faults and failure modes of specific design parts and their impact on system reliability
  - FMEA cannot be used for safety analysis
- FMECA adds a measure of the criticality of the fault or failure mode
  - This is often what people mean when they use the term FMEA
- FMEA includes the probability (likelihood) of the fault. This is the same value used in the FTA to ultimately determine hazard likelihood and system risk. Likelihood can be specified as
  - an enumerated range , such as 0 – 10, where 0 is impossible and 10 is certain
  - a probability of occurrence (typically per hour) as in 2.3×10^{-5}
- FMEA/FMECA is most often represented within a spreadsheet

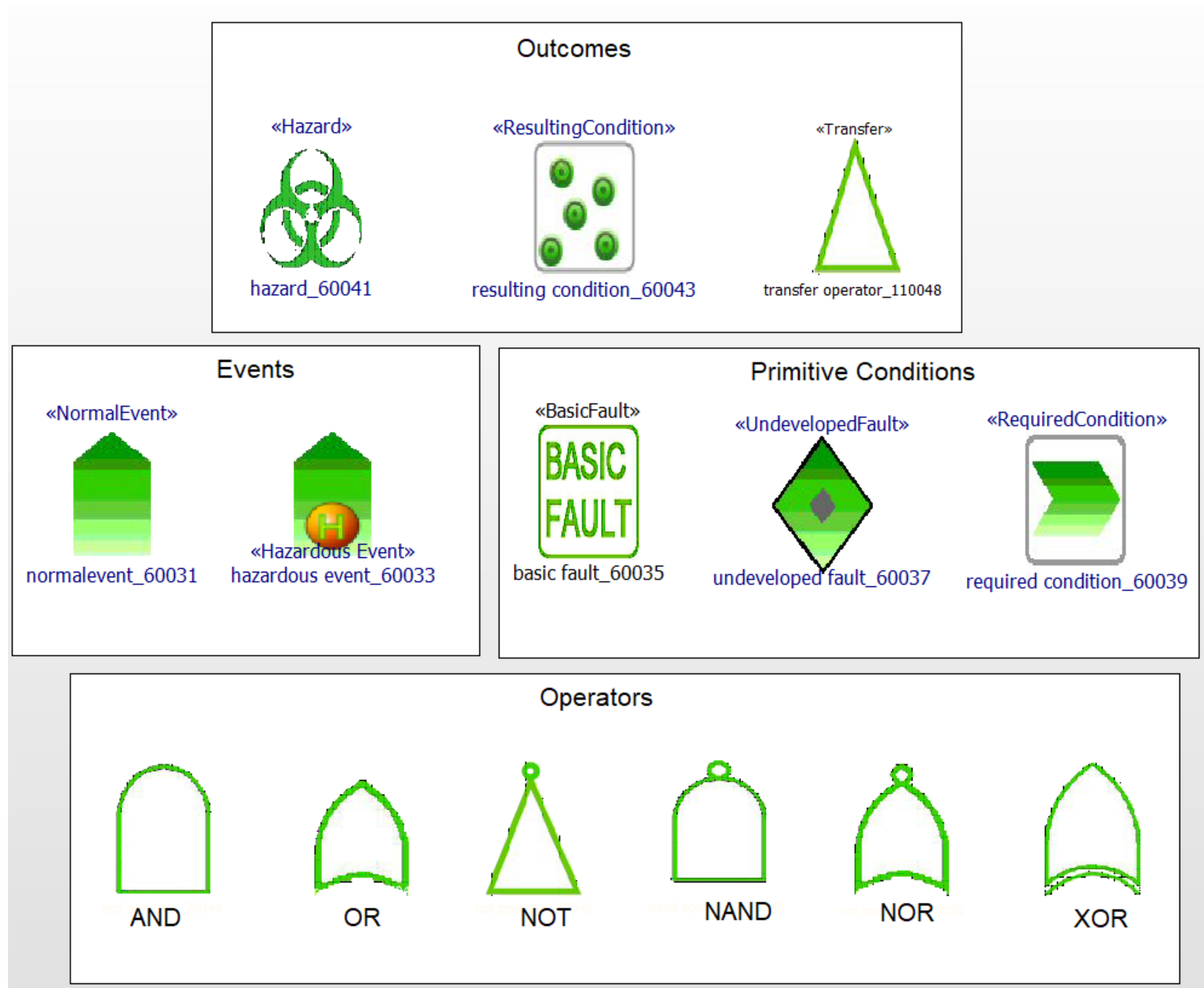
Dependability Profile includes Safety Analysis

- The Dependability Profile for UML (and SysML) that allows engineers to create FTA diagrams, hazard analyses, FMEAs, and model-based cyber-physical threat analyses.
- The Dependability profile is available for Rhapsody and may be downloaded from my web site https://www.bruce-douglass.com/safety-analysis-and-design
- There are, of course, other tools for safety analysis but none at the current time for UML and SysML tools (of which I am aware). Some do connect to UML/SysML tools, such as Medini Analyze.



Fault Tree Analysis (FTA)

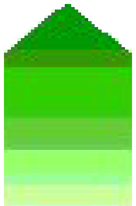
Fault Tree Analysis is discussed in ARP4761 "Guidelines for Conducting the Safety Assessment Process on Civil Airborne Systems and Equipment"



Fault Tree Analysis is a kind of causality chain that determines what combinations of conditions or events are necessary for a hazard condition to occur

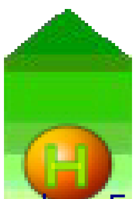
Events

«NormalEvent»



normalevent_60031

An event that could be expected during the normal lifecycle of the system. May or may not be explicitly associated with safety concerns. One or more outputs.



«Hazardous Event»
hazardous event_60033

An event that could be expected during the normal lifecycle of the system but is explicitly considered to raise safety concerns. One or more outputs.

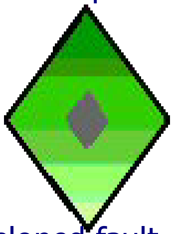
Primitive Conditions

«BasicFault»

basic fault_60035

An condition in which the system or some aspect of the system is not operating as according to its specification. Is not decomposable in this analysis. One or more outputs. Generally a fault of a design element.

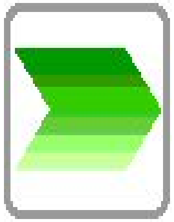
«UndevelopedFault»



undeveloped fault_60037

A fault which could be decomposed but, for the purpose of this analysis, is not. One or more outputs.

«RequiredCondition»

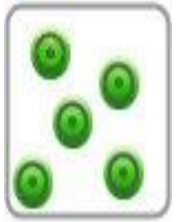


required condition_60039

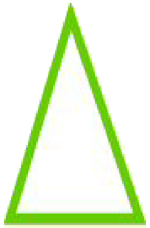
A normal condition which is identified as a pre-condition of this specific analysis. One or more outputs.

Outcomes

An condition which will lead to an accident or loss. Normally the final output condition of the FTA. There is normally one FTA per hazard. One input only.

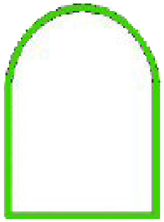


An intermediate condition resulting from the logical relations of predecessor outputs of logic operators combining more primitive inputs. One input and one output.



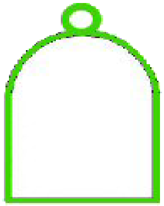
A kind of resulting condition which also serves to connect across diagrams; this is a kind of diagram connector allowing the decomposition of complex FTAs into multiple FTA diagrams. One input or one output.

Logic Operators



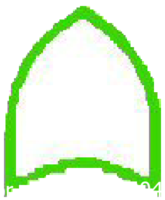
AND

Output is the logical AND of its input. 2 inputs, one or more output.



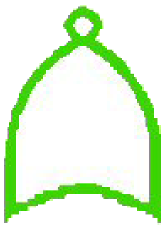
NAND

Output is the logical NAND (NOT AND) of its input. 2 inputs, one output.



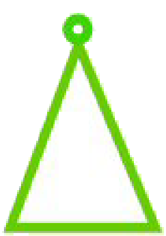
OR

Output is the logical OR of its input. 2 inputs, one output.



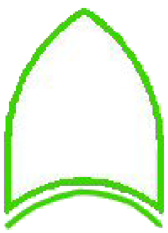
NOR

Output is the logical NOR (NOT OR) of its input. 2 inputs, one output.



NOT

Output is the logical NOT of its input. 1 input, one output.



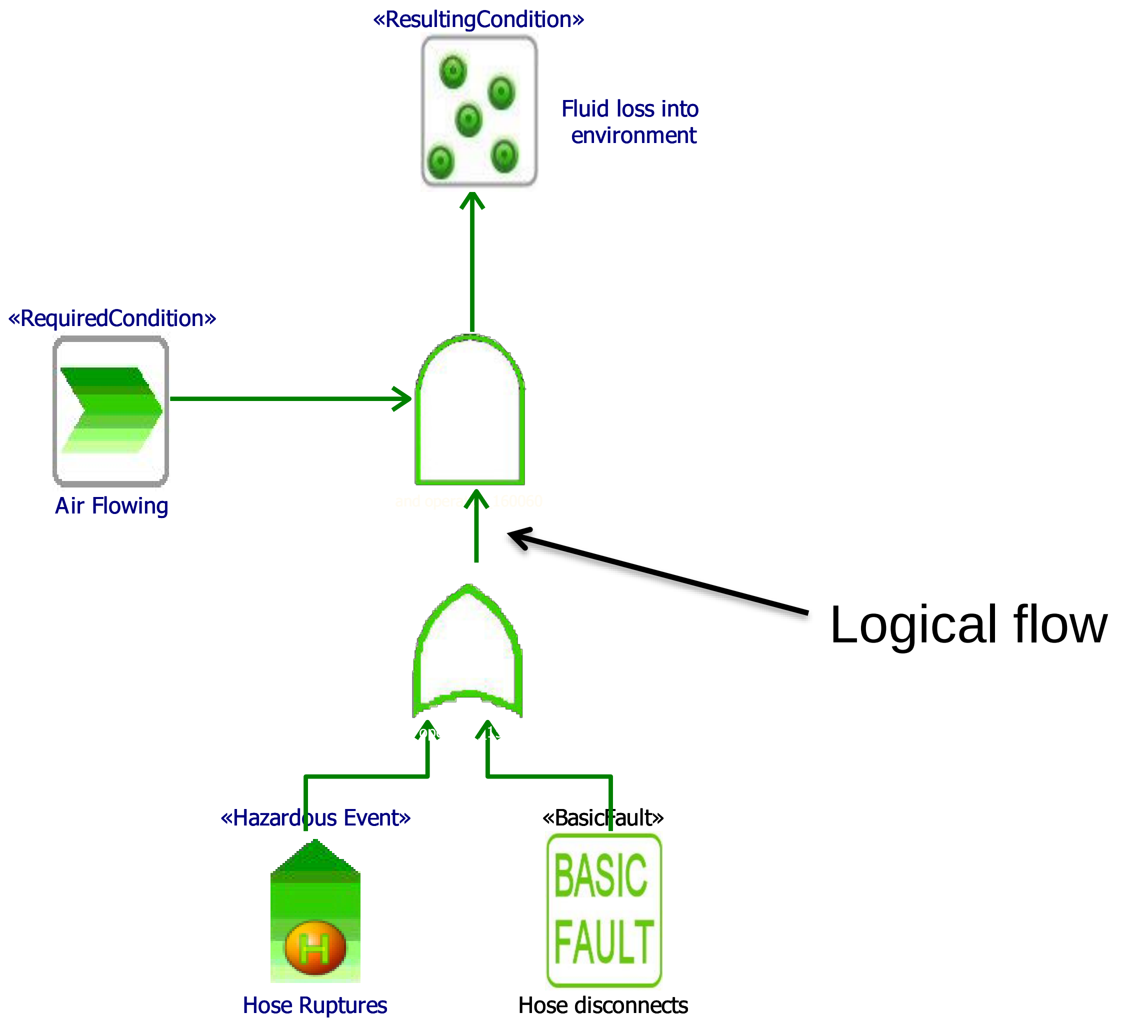
XOR

Output is the logical XOR (EXCLUSIVE OR) of its input. 2 inputs, one output.

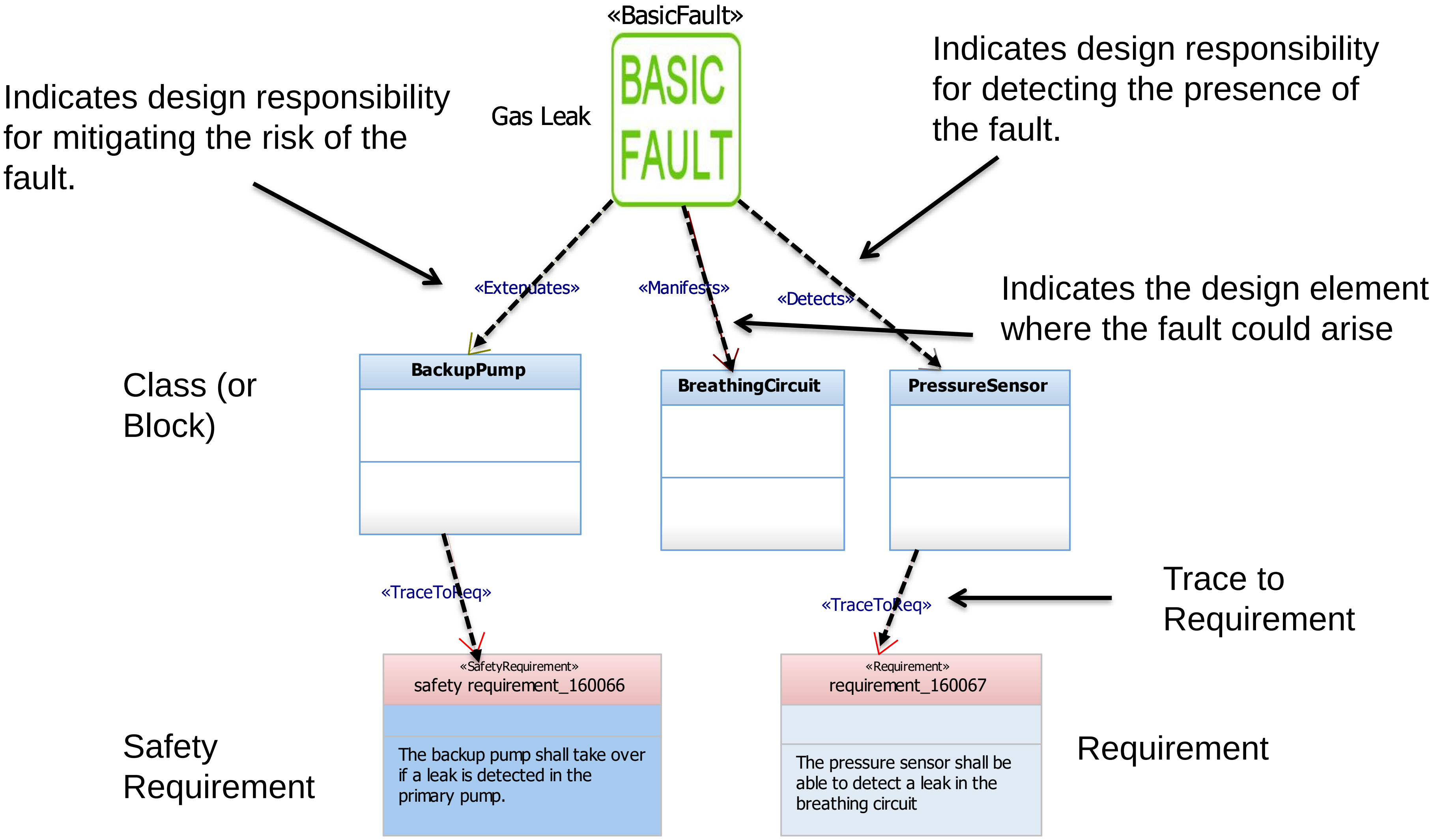
P_{XOR} = (P_{input1} AND (NOT P_{input2})) OR ((NOT P_{input1}) AND P_{input2})

Logic Flow

Conditions, events and outcomes are connecting into causality statements with logic flows, shown as a directed line.

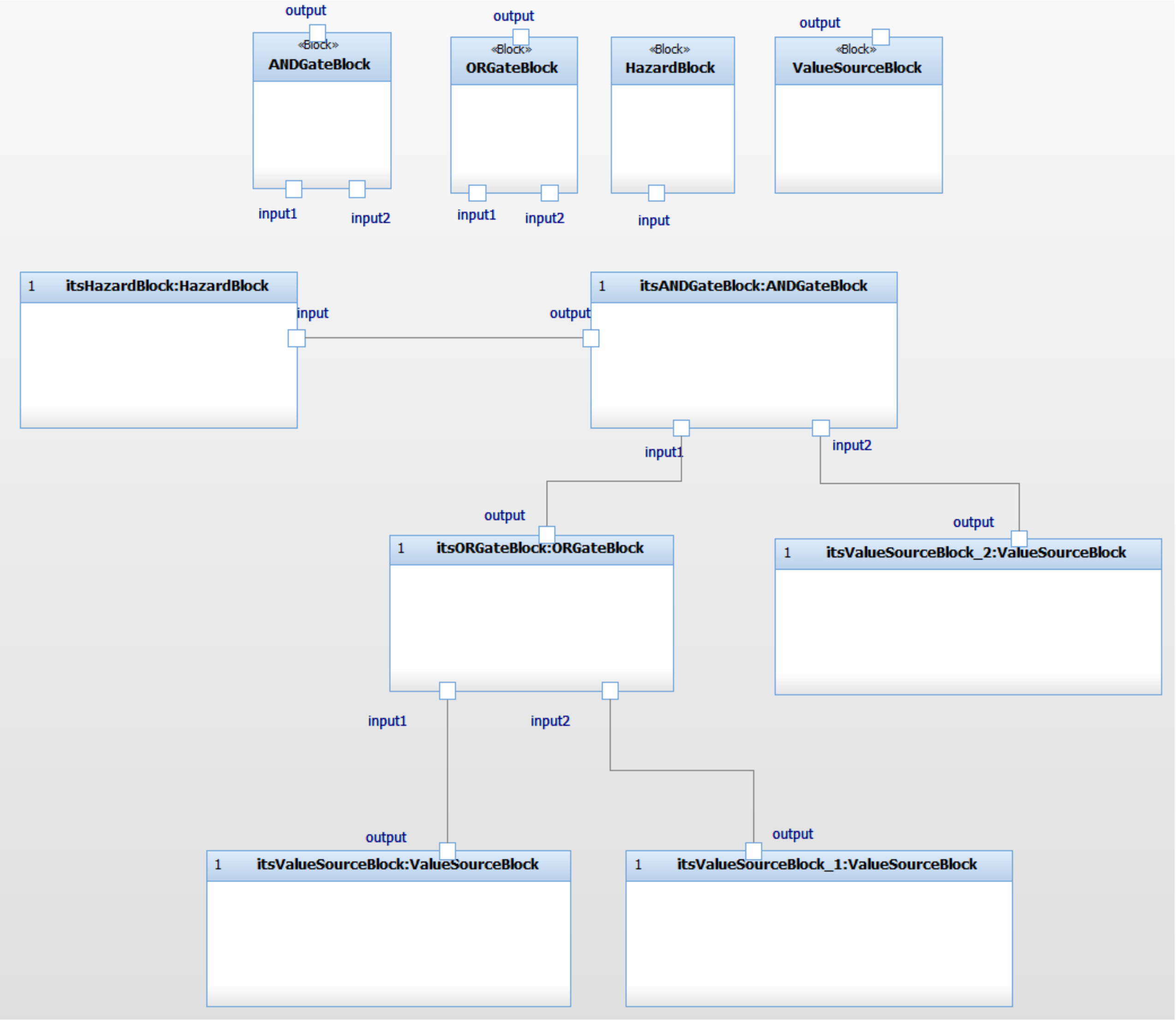


Other things on FTA Diagrams using the Dependability Profile



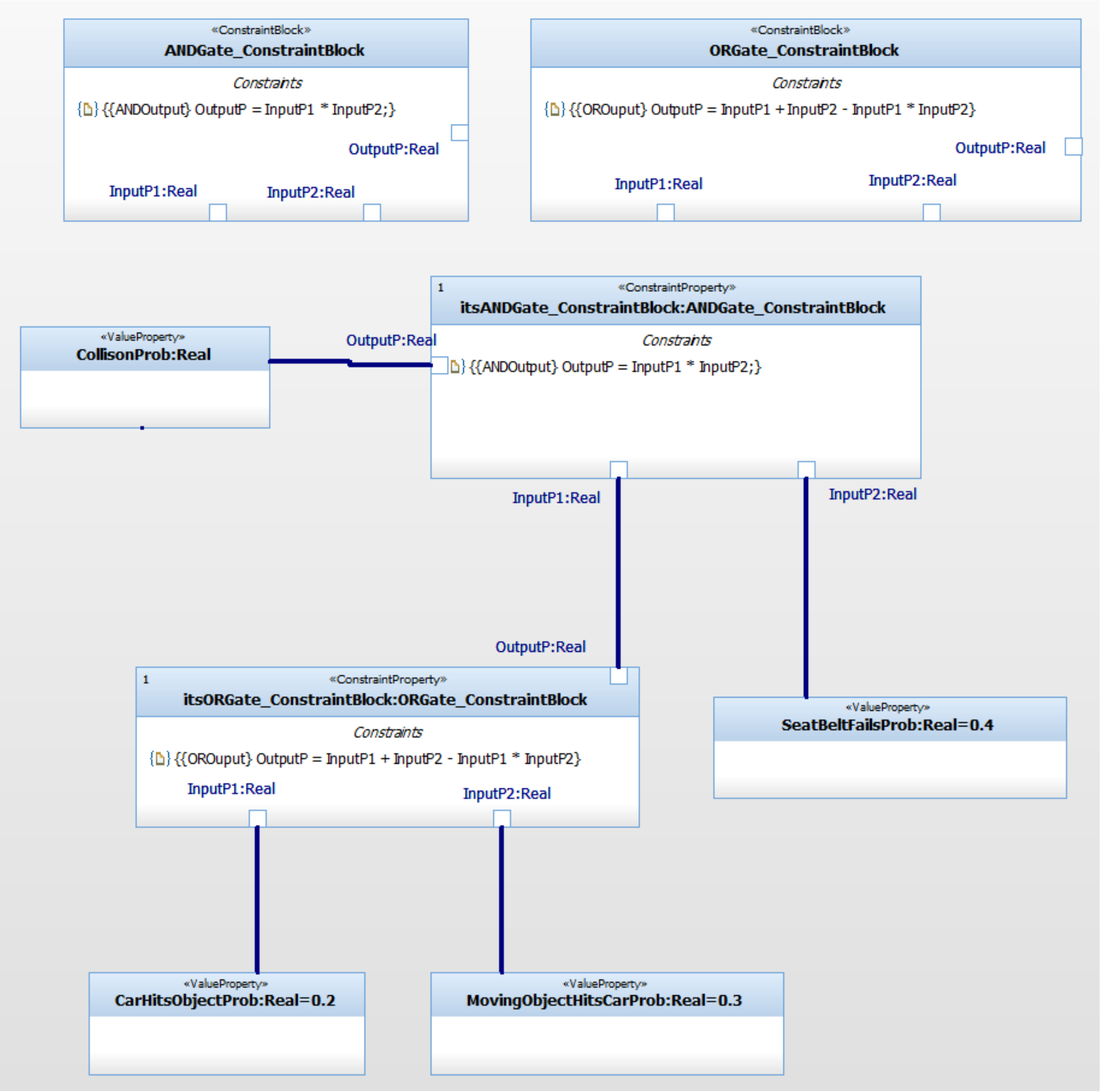
What if I just have a SysML Tool? Option 1 – Block Diagram

- Option 1: Block Diagram
  - Create blocks with ports
    - Operators have x input ports and y output puts (ex. 2 input ports and 1 output port for AND operator)
  - Add blocks for Faults (1 output port), Resulting Conditions (1 input, 1 output) and hazards (1 input)
  - Create an instance diagram and connect the instances with connectors between the ports of the instances



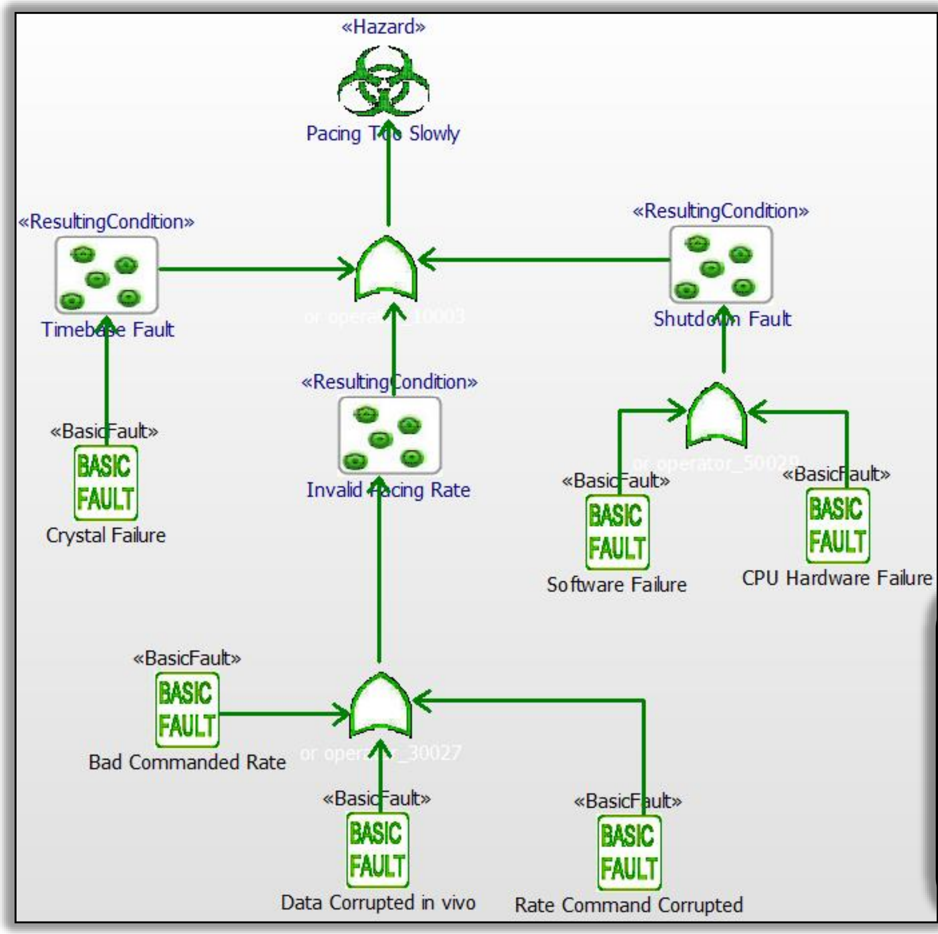
What if I just have a SysML Tool? Option 2 – Parametric Diagram

- Option 2: Parametric Diagram
  - Create operators as Constraint Blocks
  - Add Constraint Parameters for inputs and outputs (as above)
  - Use Value Properties for scalar inputs and outputs
  - Create a diagram with Constraint Properties (instances of Constraint Blocks) linking constraint parameters with Binding Connectors

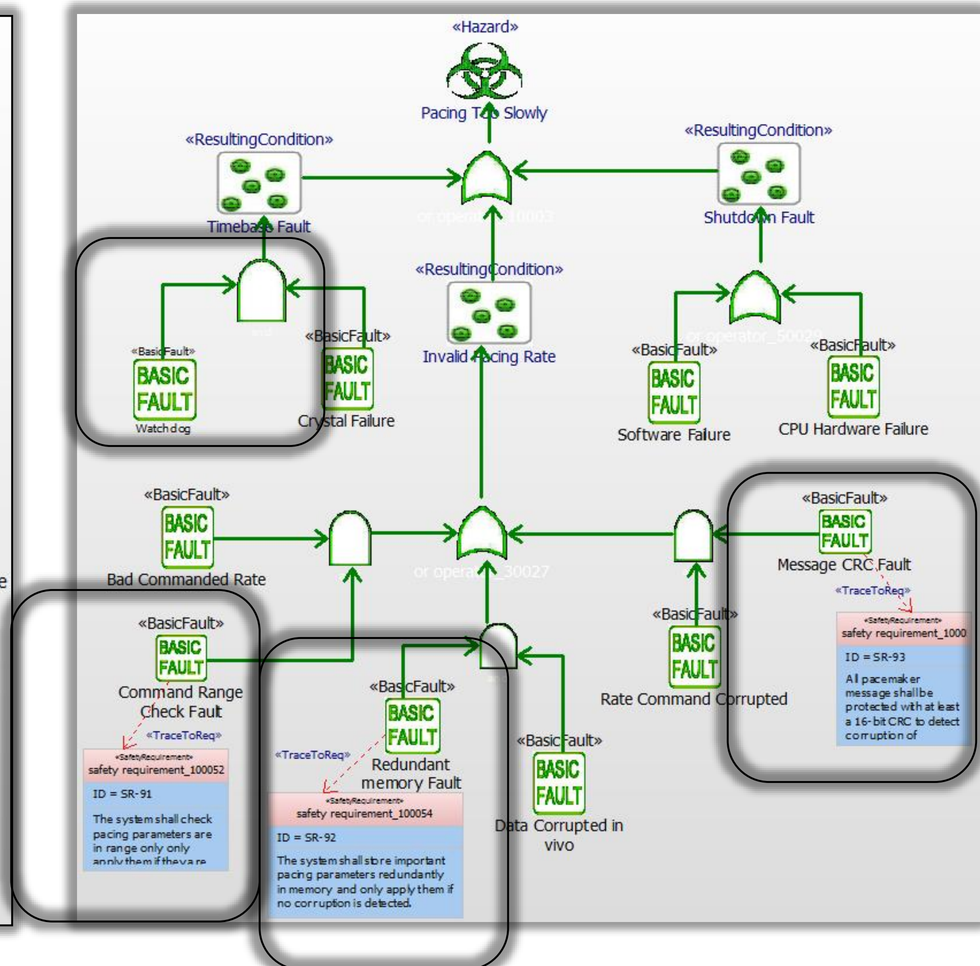


Addition of Safety Measures is Analysis → Design FTA

Analysis FTA



Design FTA



Safety Analysis Diagram

- A Fault Tree Analysis diagram is a causality diagram used to specifically show the caual relations between faults, events and conditions that manifest as hazards
  - Its purpose is to clearly understand how elements combine to cause hazards and to find the best places to add safety measures
- A Safety Analysis diagram is shows the relation between safety goals, safety requirements, control measures and design elements.
  - Its purpose is to show how the safety goals are met by the safety requirements, how they relate to safety control measures, and how control measures are realized by design elements

Safety Analysis Diagram Elements

Abstract Elements

Safety Goal

An abstract requirement

«SafetyGoal»
safetygoal_160073

A safety goal is a high-level abstract requirement that is generally not directly testable. It uses the contain relation to trace to associated, testable safety requirements. It is realized by safety measures.

Safety Requirement

A concrete requirement

«SafetyRequirement»
safety requirement_160075

A safety requirement is a normal, testable requirement whose compliance impacts the safety of the system. Contributes to a safety goal.

Safety Measure

A safety design pattern

«SafetyMeasure»
safety measure_160077

A safety measure is an abstraction of a set of related design element structures and behaviors that collectively realize one or more safety requirements. It connects to design elements via the implements relation.

FTA Elements

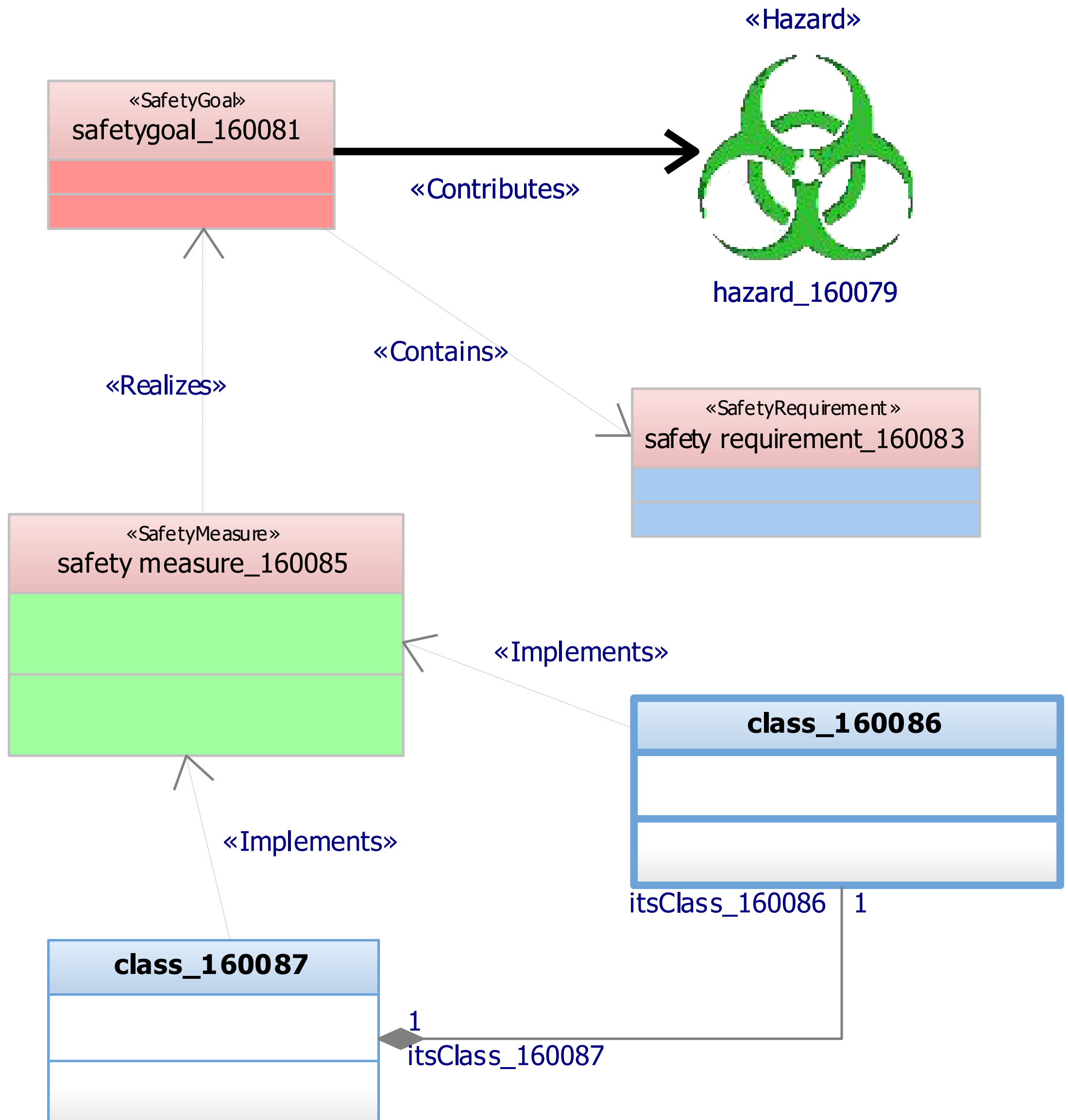
Any FTA element may be added to this diagram

UML/SysML Elements

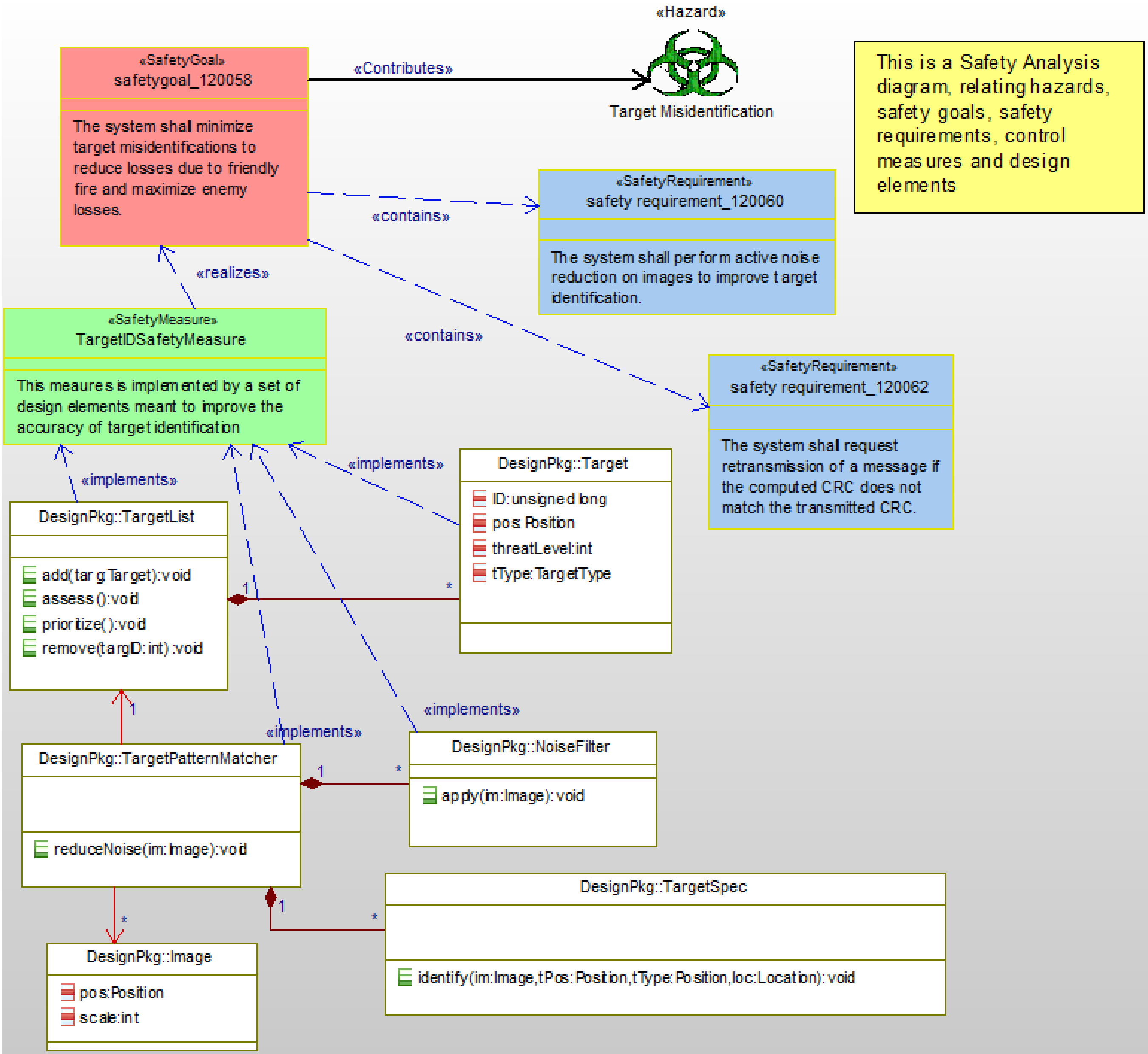
Classes, blocks, and relations among them maybe added to this diagram

Safety Analysis Diagram Relations

- Contributes
  – Points to an element to which the current one contributes, primarily used to show which safety goals address which hazards
- Contains
  – Points to an element logically contained within the abstraction, primarily used to trace from safety goals to specific safety requirements
- Realizes
  – Points to an abstraction realized by the current element; often used for safety measures realizing a goal or requirement.
- Implements
  – Points to the goal, measure, or requirement realized by a design or implementation element.

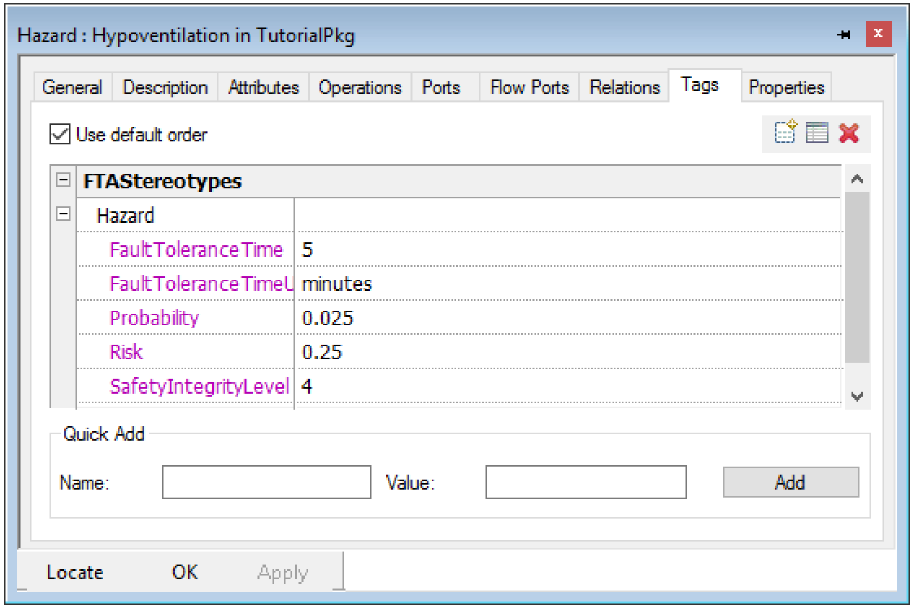


Safety Analysis Diagram



Safety Relevant Metadata: Hazards

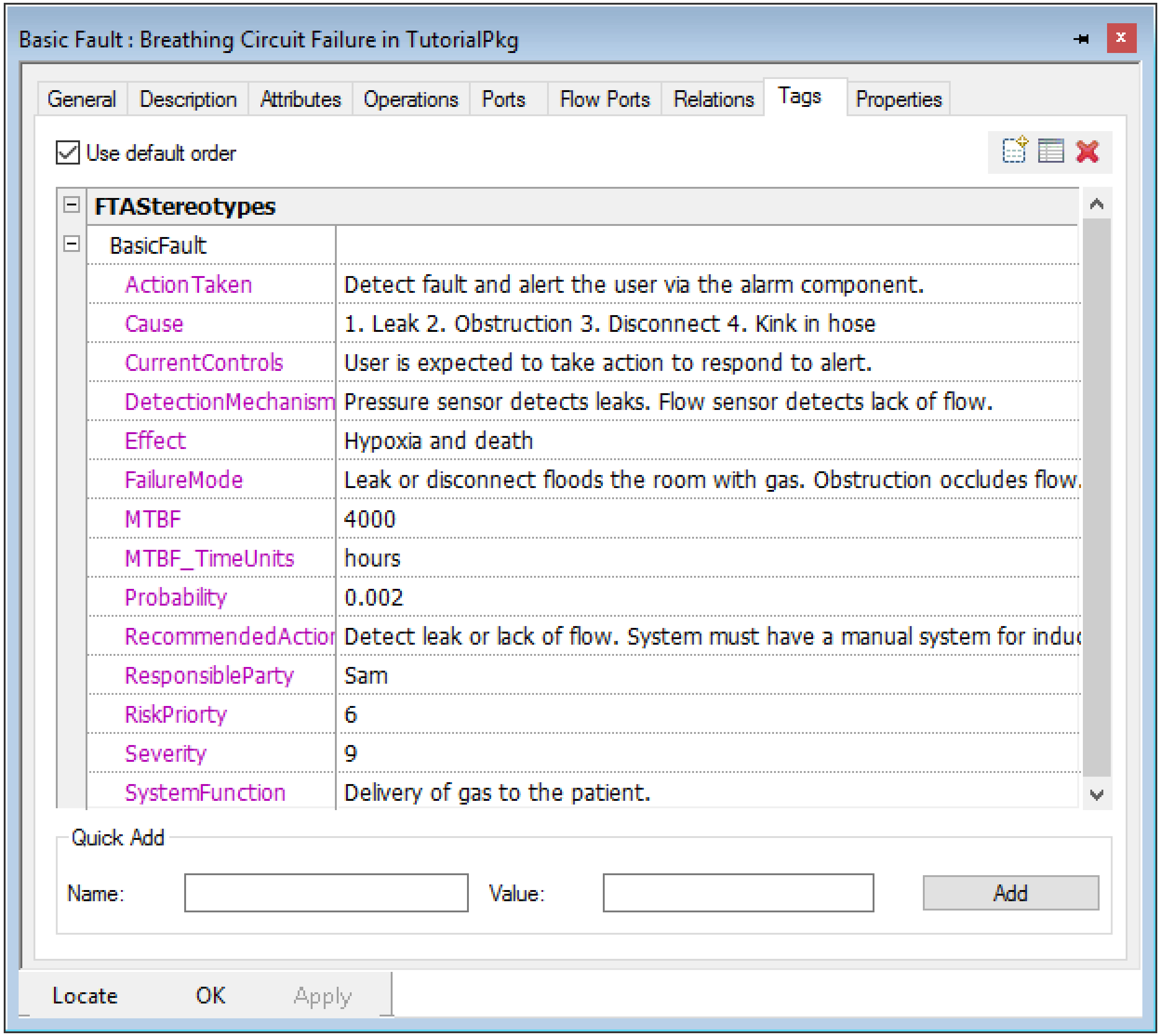
Hazards are a stereotype and as such, contain tags to hold relevant metadata



Hazards can be summarized in a Hazard Table

Name	Description	Probability	Severity	Risk	SafetyIntegrityLevel	FaultToleranceTime	FaultToleranceTimeUnits
Anesthesia leak into ER	Anesthesia leak can lead to short or, in smaller doses, to long-term poisoning of medical staff.	1e-5	5	4e-5	5	10	minutes
Hyperoxia	Hyperoxia problems are usually limited to neonates, where it can cause blindness.	1e-5	4	4e-5	4	10	minutes
Hypoxia	The hypoxia hazard occurs when the brain and other organs receive insufficient oxygen. In a normal 21% O2 environment, death or irreversible injury occurs after 5 minutes of no oxygen. If the patient is breathing 100% for a singificant period of time, this time is about 10 minutes.	1e-2	8	8e-2	3	5	minutes
Inadequate Anesthesia	In adequate anesthesia leads to patient discomfort and memory retention of the surgical procedures. This is normally not life threatening but can be severely	1e-4	2	2e-4	2	5	minutes
Over anesthesia	Over anesthesia can lead to death.	1e-3	4	4e-3	4	3	minutes
Overpressre	Overpressure can damage the lungs. This is an especially severe trauma, possibly fatal, to neonates.	1e-4	4	3e-4	3	200	miliseconds

Safety Relevant Metadata: Basic Faults



Safety Relevant Metadata: FMEA

Found 25 elements

Name	Description	SystemFunction	Cause	Effect	Current Controls	Severity	MTBF	MT
Backup Power Fails	The battery backup exists as a safety means to enable the system to continue to provide therapy and monitoring when mains fail. This fault means that the backup system is unable to provide that backup.	Provide backup power		If mains are on, system remains on; if mains are off, system fails	none	7	1e4	
Breathing Circuit Leak	This fault occurs when a significant amount of gas leaks from the breathing circuit into the surrounding environment. This can lead to a poisoning hazard when the gas contains anesthetic drugs.	deliver breathing gas to patient	Leak or disconnect	Hypoxia and death	None	9	1e3	
Breathing Circuit O2 Sensor Fault	The breathing circuit O2 sensor is provided to ensure that the O2 delivered from the system matches expectations. This fault means that it is unable to either determine the O2 concentration or unable to communicate that information.	Detect low O2 in breathing circuit	Electrical fault, configuration fault	Loss of ability to ensure adequacy of O2 delivery	This is a safety mechanism.	7	1e7	
Breathing Circuit Problem								
Connection problem								
Esophageal Intubation	This is a user-fault, but is common. This is mitigated by a CO2 sensor on the expiratory limb of the breathing circuit.	deliver breathing gas to patient	Physician intubates the esophagus rather than the trachea	Hypoxia and death	None	9	1e5	
Expiratory Limb CO2 sensor fault	The expiratory limb CO2 sensor exists to ensure that the breathing circuit is properly connected to the patient - if there is inadequate CO2 in the expiratory limb than either the patient isn't generating CO2 or the expiratory limb is disconnected from the patient. This fault means that the sensor is either unable to accurately determine the CO2 concentration or is unable to communicate those values to the system.	Detect esophageal intubation	Lack of connection to sensor; electrical fault; sensor configuration fault	Unable to detect esophageal intubation, leading to hypoxia and death	None	8	1e7	
Failure to Alarm	The alarm system is a system that exists solely for safety reasons. Therefore, it need not be extenutated by another system since it exists solely to address safety issues of the primary systems. It must, however, be tested as a part of system start up.	Alert the user to patient and system problems	System electrical fault; screen and audio fault; power fault; message loss; message	Missed alerts can lead to death	None	9	1e5	
Gas Flow Sensor Fault	This fault occurs if the gas flow sensor fails to correctly measure the gas flow in the breathing circuit limb to which it is attached, or if it fails to send that information to the system.	Ensure proper gas flow	Electrical fault; bus fault; configuration corruption;	Inability to detect incorrect gas flow	None	9	1e-7	
Gas Supply Fault	This fault occurs when gas from a required source (e.g. O2 air N2 or He). This may be to any number of root causes such as a stuck or closed valve, running out of gas, a leak_ etc.	Ensure proper gas flow					1e6	
Inspiratory Pressure Sensor Fault	The inspiratory pressure sensor is used to determine that the pressures delivered to the patient lungs are within min and max limits and that they match the expectations of the system based on the delivery of the shaped breath. This fault means that the sensor is either unable to determine pressure accurately or that it cannot communicate these values to the system.	Detect leak or obstruction					1e7	
O2 Concentration Problem								
O2 Supply Fault	The O2 supply fault can occur because of a exhaustion of the supply itself, stuck or incorrectly commanded valves, or a problem in the supply line to the ventilator.	Deliver breathing gas to patient					1e4	
Patient disconnect from Breathing Circuit	This fault can occur as a result of jostling the breathing circuit during a surgical procedure.	Deliver breathing has to patient					1e4	
Physician unable to manually ventilate	The anesthesiologist is required to have a manual ventilation system available in the case of an unrecoverable system failure. This fault may occur because that manual system is missing or nonfunctional or if the system has alarmed but the physician is unaware of the alarm or of the need for immediate action.	P:rovide backup ventilation					1e10	
Power Supply Fault	The mains can fail because of a source power supply fault or if the power cord becomes unplugged.	Provide power to run system					1e5	
Power Supply Problem								
Redundant computational Channel fails	The redundant computational channel uses a heterogeneous algorithm to compute the output values as a check on the primary. Since there are only two computational channels, if one is in error, the system cannot determine which channel is in error, only that an error has	Deliver breathing gas to patient					1e5	
SpO2 Sensor Fault	The SpO2 sensor is a fingercuff O2 sensor. This fault occurs if the sensor does not accurate;y determine the blood concentration of O2 or if the sensor is unable to communicate its readings to the system.	Ensure adequate blood oxygenation					1e7	
Ventilator Computation Incorrect	This fault occurs when an error in the software or a fault in a necessary resource (e.g. memory) results in an incorrect computation that in turn results in incorrect delivery of	Deliver breathing gas to patient					1e5	
Ventilator Parameter CRC check fails	Ventilator parameters are protected with a 32-bit CRC algorithm. This is specifically designed to identify situations in which the value has been changed through inappropriate means (e.g. memory cell fault). A fault here means that the CRC fails to identify the corruption of the	Validate command parametrs					1e5	
Ventilator Parameter Limiting Fails	This fault occurs if the limit checks on the setting of ventilator parameters fail, i.e. allow a value to be entered that is out of the allowed range, given the mode (neonate or adult) of the system.						1e6	
Ventilator Parameter Setting wrong	This fault occurs when a ventilator parameter is out of range. This includes: I:E ratio Tidal Volume Respiration Rate Inspiratory Pause Maximum inspiratory pressure Inspiration time						1e4	
Ventilator Problem								
Ventilator Pump Fault	This fault occurs when the pump internal to the ventilator no longer functions to shape the breath and push gas into the breathing circuit.						1e6	

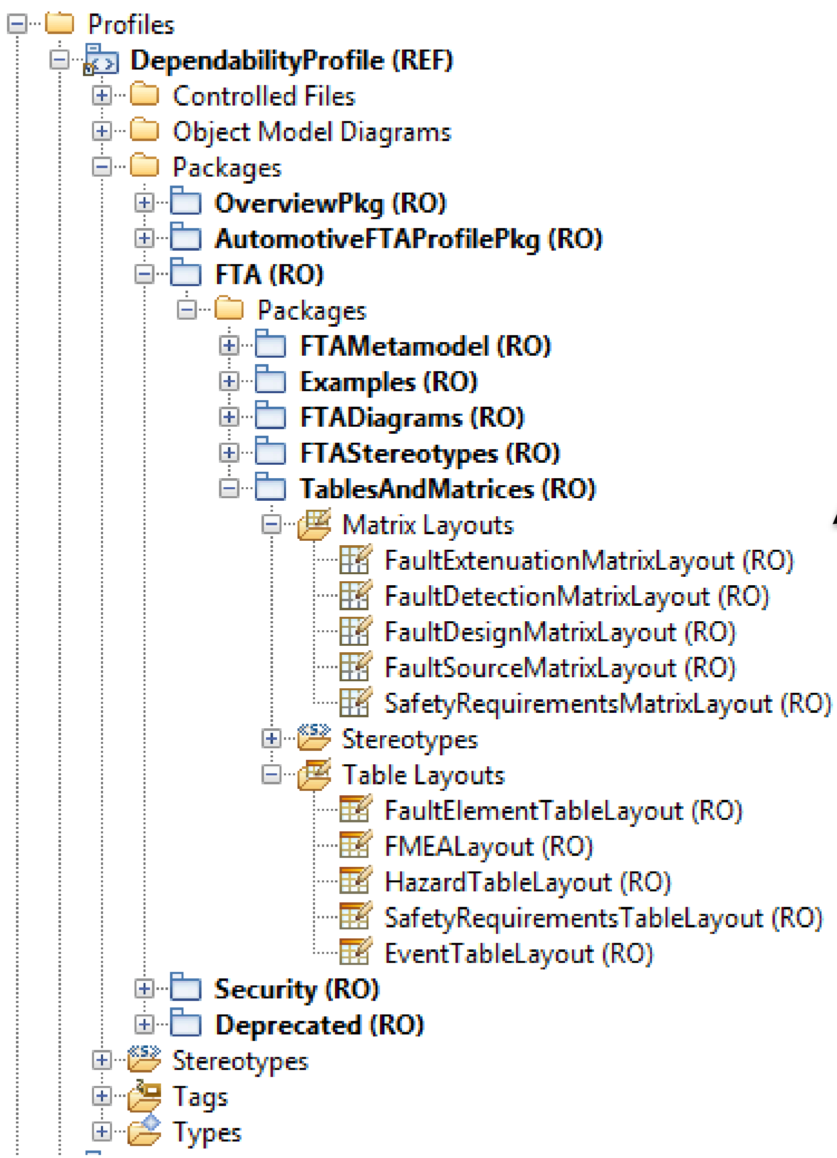
Table/Matrix
- Refresh
- Add model elemer
- Fill Defaults
- Export to file...

export

Safety Relevant Metadata: FMEA (shown in Excel)

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
1	**Name**	**Description**	**SystemFunction**	**Cause**	**Effect**	**Current Controls**	**Severity**	**MTBF**	**MTBF_TimeUnits**	**Probability**	**Action Taken**	**Detection Mechanism**	**FailureMode**	**Recommended Action**	**Responsible Party**	**Risk Priorty**		
2	Backup Power Fails	The battery backup exists as a safety means to enable the system to continue to provide therapy and monitoring when mains fail. This fault means that the backup system is unable to provide that backup.	Provide backup power		If mains are on, system remains on; if mains are off, system fails	none	7	1.00E+04	minutes	1.00E-04	Provide a 1 hr, 20 min, and 5 minute low power warning.	voltage sensor on backup supply	Battery runs out of power	None - the system need only be single point failure safe.	Susan	17		
3	Breathing Circuit Leak	This fault occurs when a significant amount of gas leaks from the breathing circuit into the surrounding environment. This can lead to a poisoning hazard when the gas contains anesthetic drugs.	deliver breathing gas to patient	Leak or disconnect	Hypoxia and death	None	9	1.00E+03	minutes	1.00E-03	Alert the user via the alarm system	Loss of pressure	System leaks into the operating room	Use pressure sensor to detect leak and alert the user	Susan	5		
4	Breathing Circuit O2 Sensor Fault	The breathing circuit O2 sensor is provided to ensure that the O2 delivered from the system matches expectations. This fault means that it is unable to either determine the O2 concentration or unable to communicate that information.	Detect low O2 in breathing circuit	Electrical fault, configuration fault	Loss of ability to ensure adequacy of O2 delivery	This is a safety mechanism.	7	1.00E+07	seconds	1.00E-07	None	O2 sensor at the point of intubation.	Loss of data, spurious data	Alerrt the user via the alarm system	Susan	5		
5	Breathing Circuit Problem																	
6	Connection problem																	
7	Esophageal Intubation	This is a user-fault, but is common. This is mitigated by a CO2 sensor on the expiratory limb of the breathing circuit.	deliver breathing gas to patient	Physician intubates the esophagus rather than the trachea	Hypoxia and death	None	9	1.00E+05	minutes	1.00E-04	None	CO2 sensor on end tidal flow detects a lack of CO2 production from the lungs	Physican error during patient preparation	Add CO2 sensor on end tidal limb of the breathing circuit	Joyce	8		

Other Predefined Tables and Matrices in the Dependability Profile

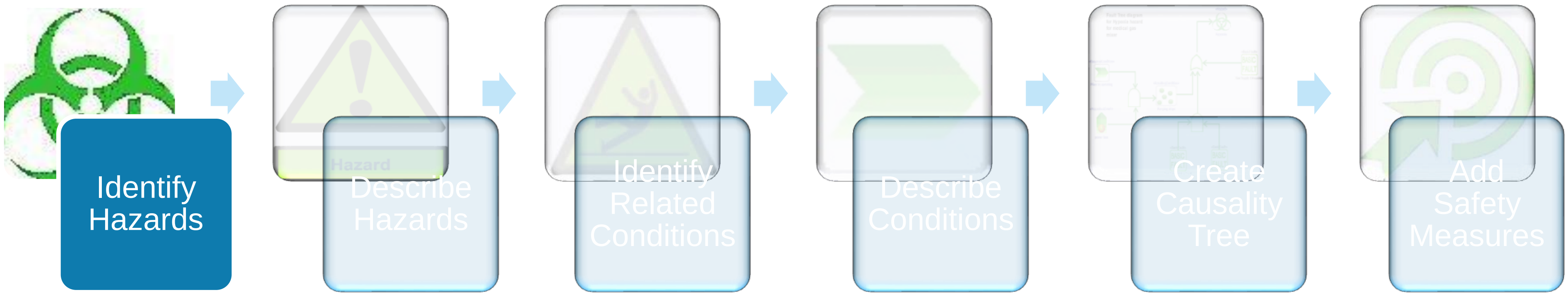


Trace from all fault element types with specific relations

Trace from all fault element types to requirements

Metadata of relevant elements

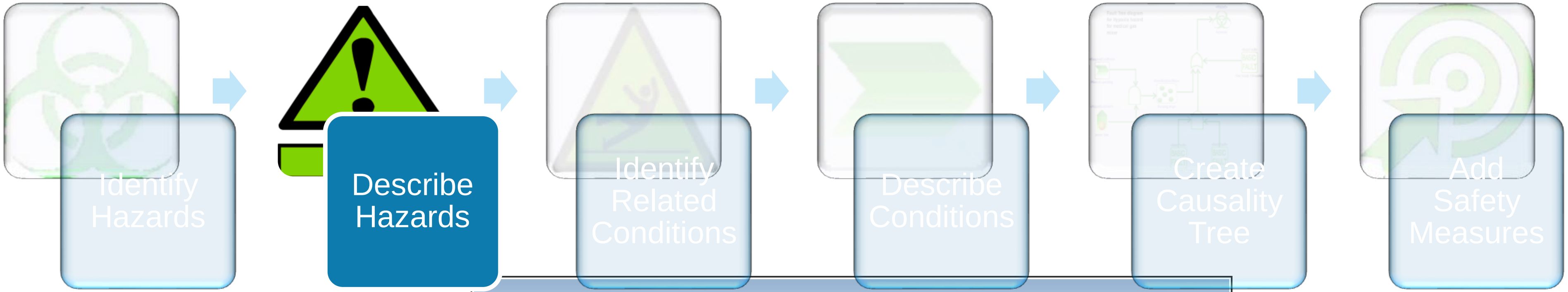
How to build a Safety Analysis

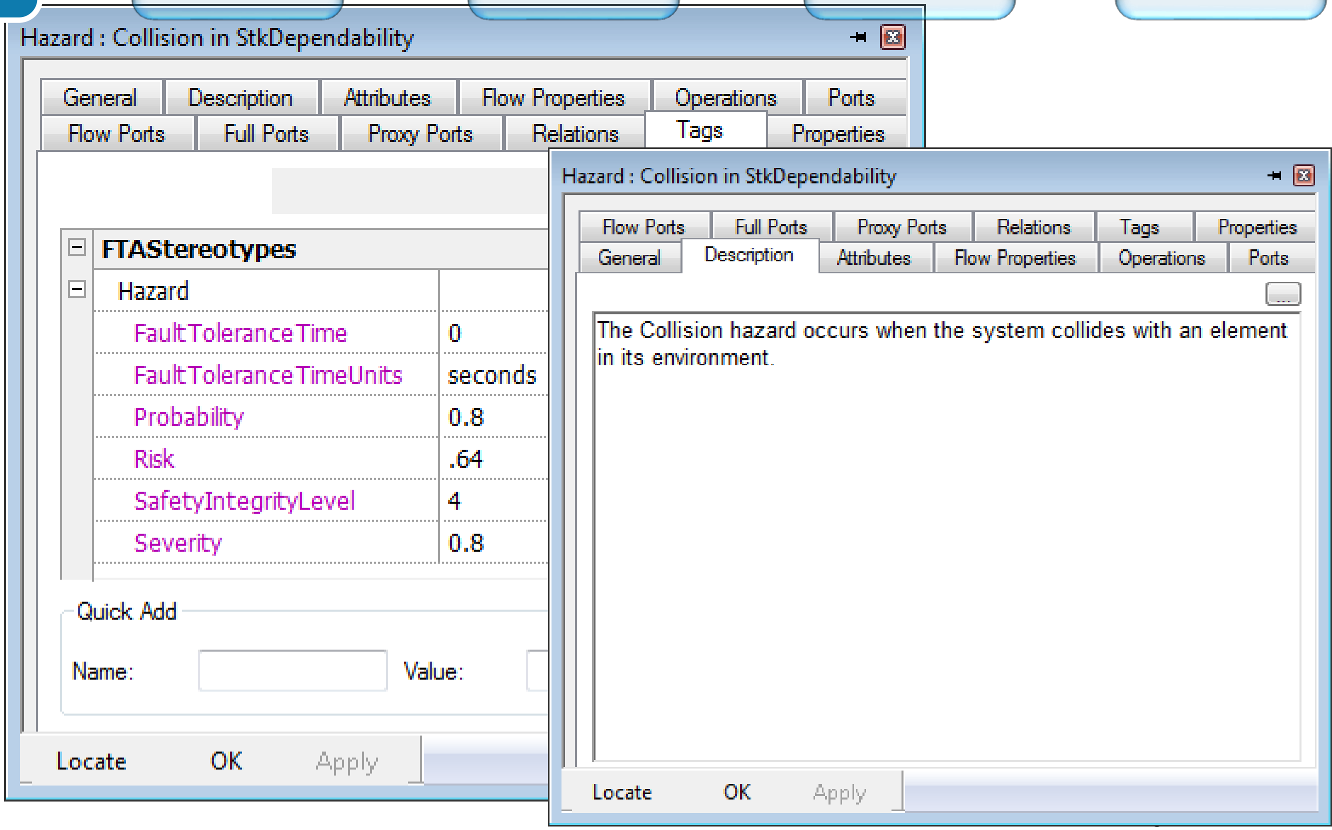


Name	Description	Probabil...	Se...	R..	SafetyIntegrityLevel	FaultToleranceTime	FaultToleranceTimeUnits
Failure to Capture Heart	This hazard means that the pulse amplitude or duration is inadequate to reliable induce a cardiac contraction.	0.06	10	0.6	C	5	minutes
Pacing Too Quickly	Pacing too quickly can result in pacing in the super vulnerable period, potentially leading to fibrillation.	0.001	10	0.01	C	100	miliseconds
Pacing Too Slowly	Pacing too slowly can lead to inadquate blood flow leading to unconsciousness or death.	0.01	10	.1	C	5	minutes
Too much Energy Delivered	Too much energy delivered can result in early battery depletion or, in very rare circumstances, cardiac tissue damage.	0.05	3	.15	C	1	years

- A *hazard* is a condition that leads to an accident or loss
- A hazard is characterized by
  - Likelihood (L)
  - Severity (S)
  - Risk = L * S

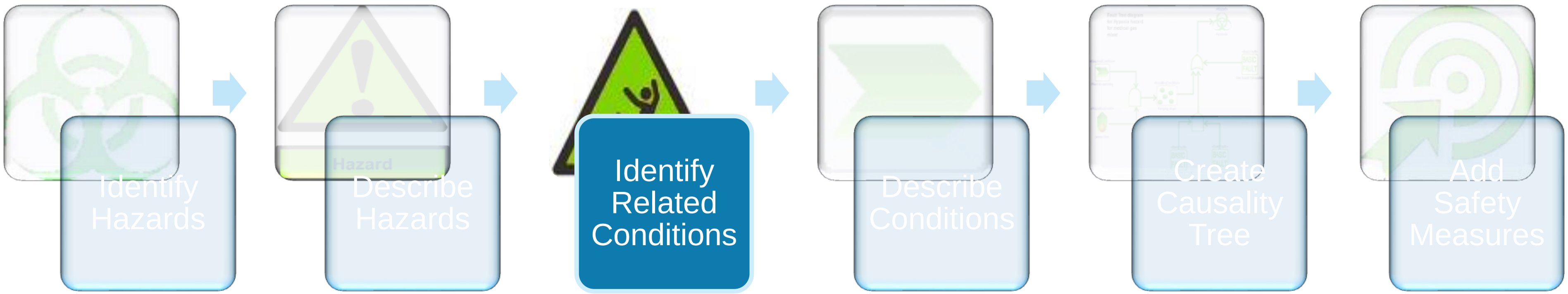
How to build a Safety Analysis





Define the *hazard metadata* to define and understand the hazard, its severity, and its likelihood

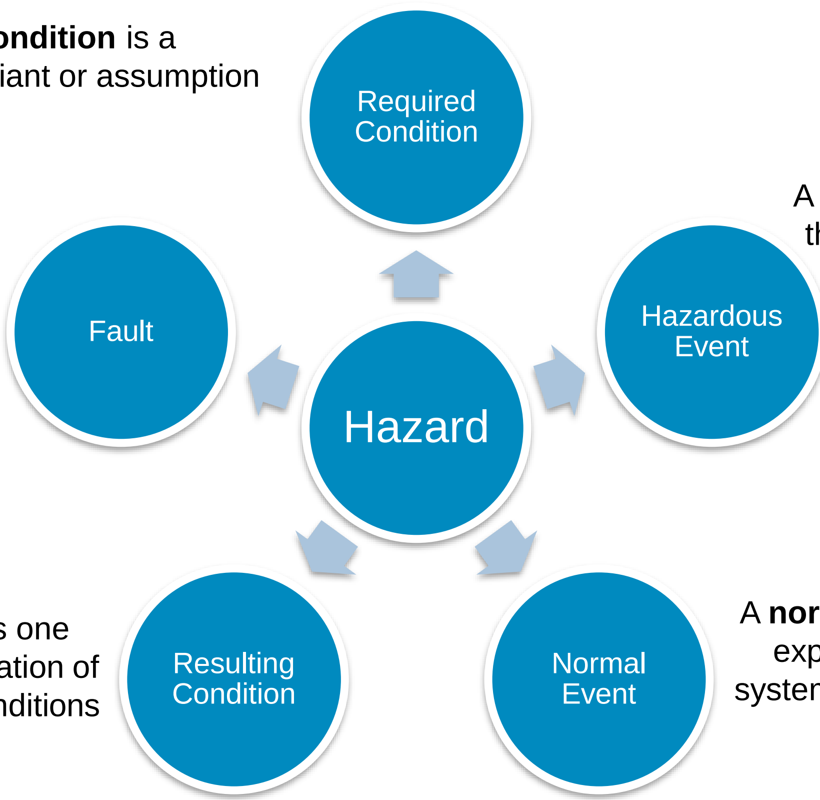
How to build a Safety Analysis



A **required condition** is a preconditional invariant or assumption

A **hazardous event** is an event that is known to pose a safety concern

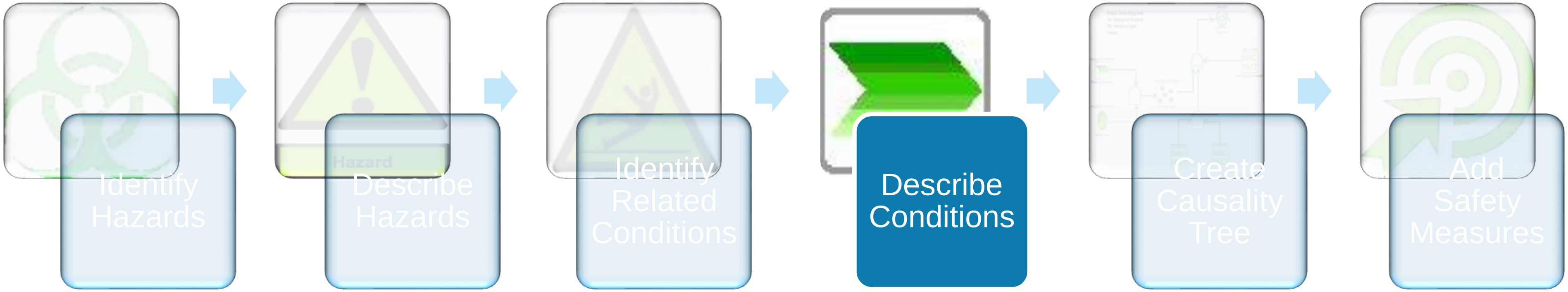
A **fault** is a system non-conformance. It may be systematic (error) or random (failure)



A **resulting condition** is one that results from a combination of more basic events and conditions

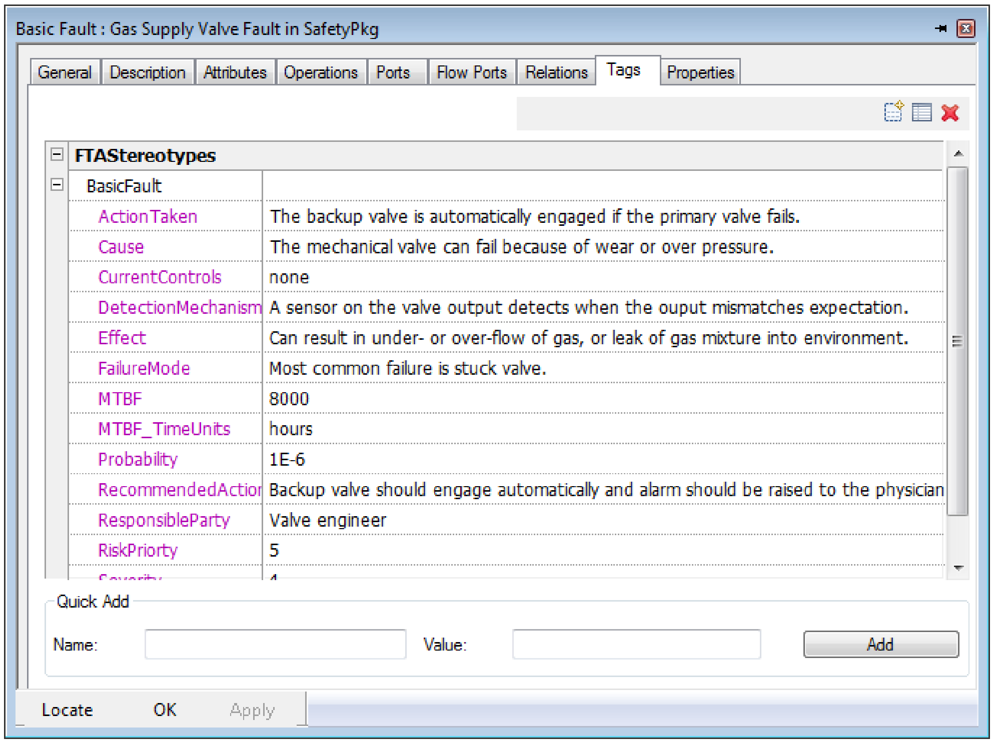
A **normal event** is an occurrence expected by or normal to the system and its operational context

How to build a Safety Analysis



Characterize conditions, especially faults.

This information can be used to generate a Fault Mode and Effect Analysis (FMEA)


Basic Fault : Gas Supply Valve Fault in SafetyPkg

General | Description | Attributes | Operations | Ports | Flow Ports | Relations | Tags | Properties

FTAStereotypes

BasicFault

ActionTaken	The backup valve is automatically engaged if the primary valve fails.
Cause	The mechanical valve can fail because of wear or over pressure.
CurrentControls	none
DetectionMechanism	A sensor on the valve output detects when the ouput mismatches expectation.
Effect	Can result in under- or over-flow of gas, or leak of gas mixture into environment.
FailureMode	Most common failure is stuck valve.
MTBF	8000
MTBF_TimeUnits	hours
Probability	1E-6
RecommendedActior	Backup valve should engage automatically and alarm should be raised to the physician
ResponsibleParty	Valve engineer
RiskPriorty	5
Severity	4

Quick Add

Name: Value: Add

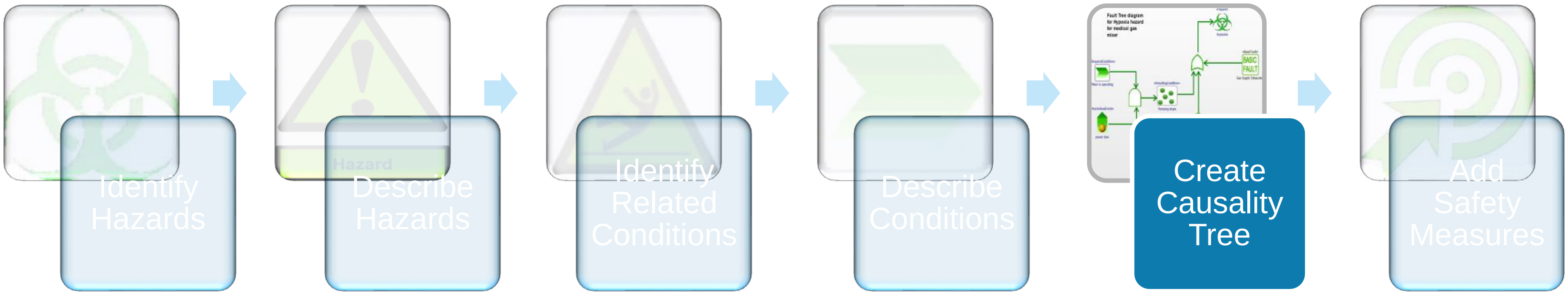
Locate OK Apply

Failure mode should include (but shouldn't be limited to):

- Open,
- Short,
- Parameter shift,
- out of adjustment, dielectric breakdown
- Intermittent operation
- Spurious operation
- Wear
- Mechanical failure
- Sticking
- Loose
- Fracture

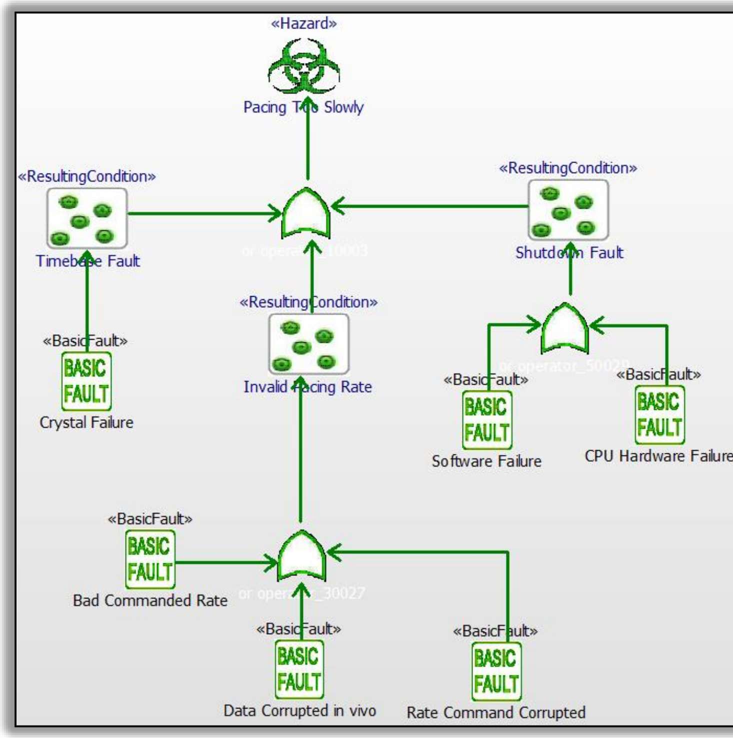
(ARP4761)

How to build a Safety Analysis

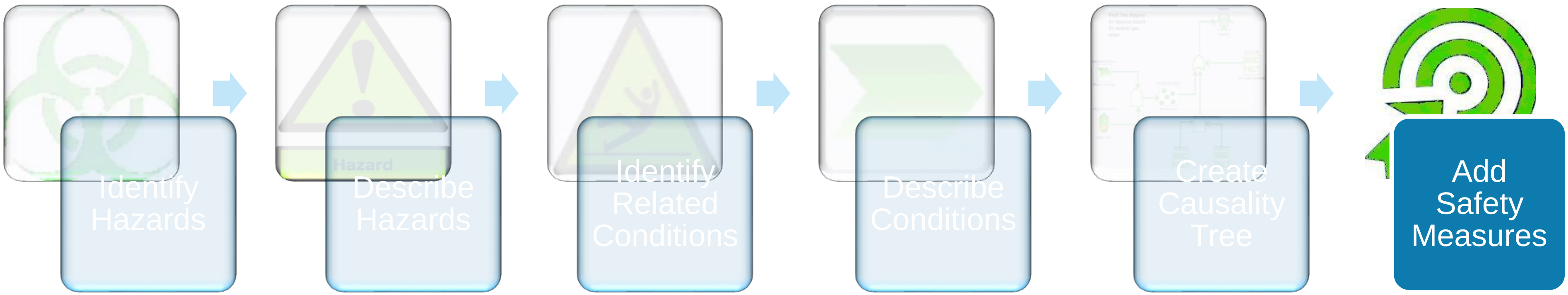


The FTA shows the relation – using logical operators such as AND, OR and NOT – among faults, events, and conditions.

These result in resulting conditions that may be further logically combined to result in manifested hazards.



How to build a Safety Analysis



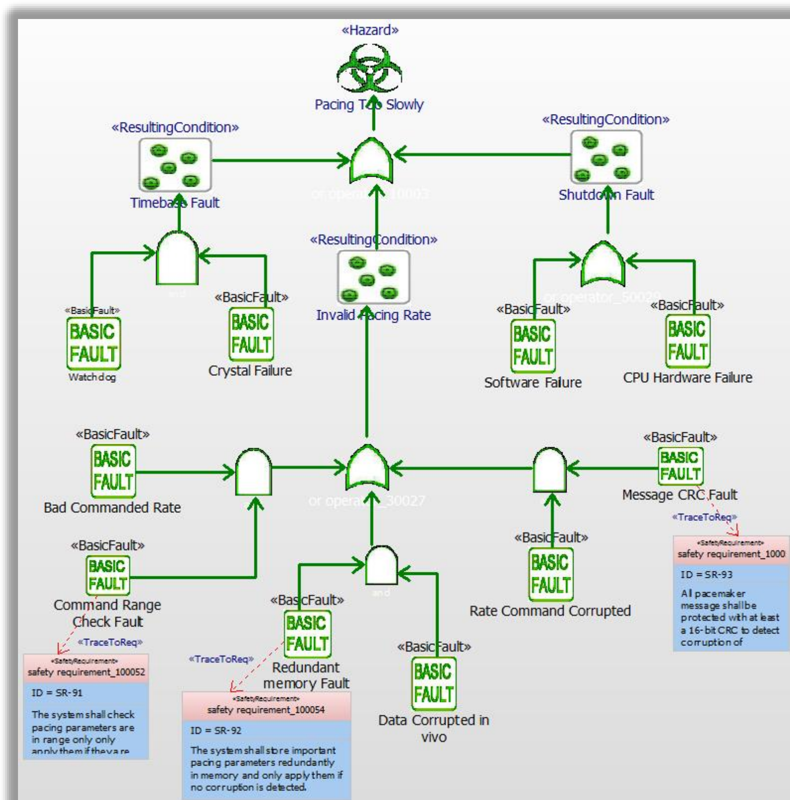
Safety measures reduce either

- The likelihood of a fault
- The severity of a fault

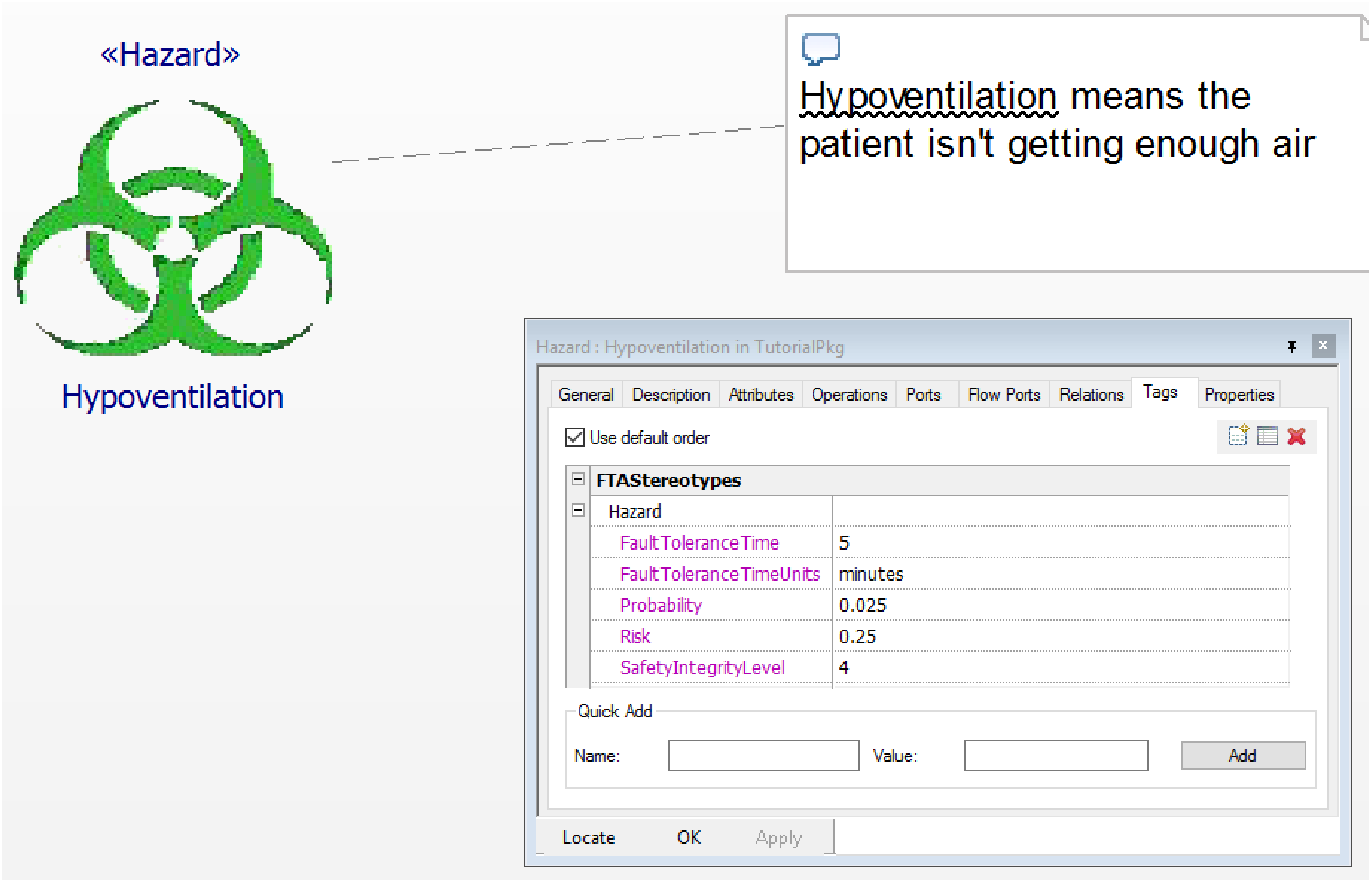
The measure works because for the hazard to manifest the original fault must occur AND the safety measure must also fail

These will be represented in

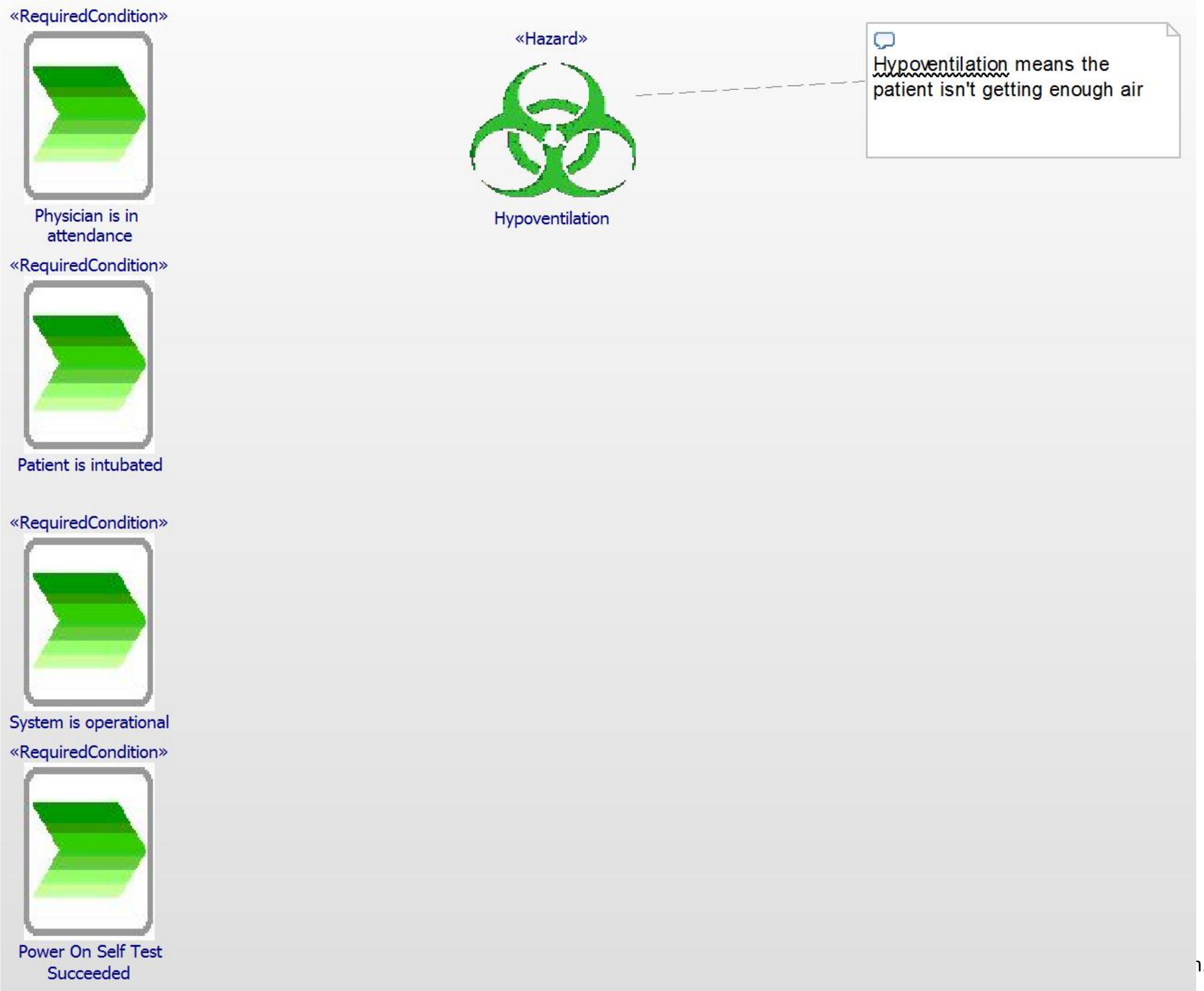
- Safety requirements
- Safety design elements



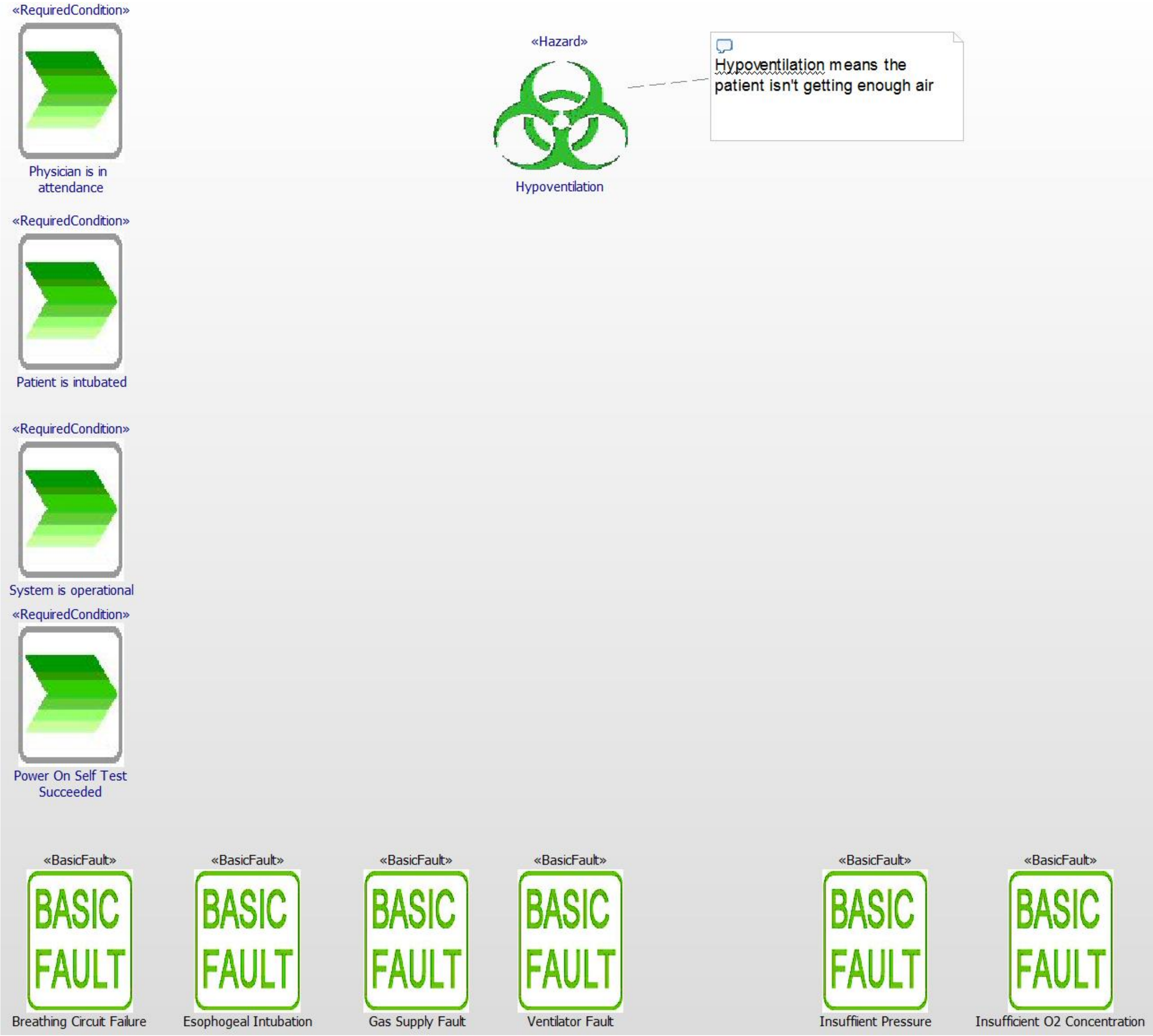
Example Fault Tree Analysis: The Hazard



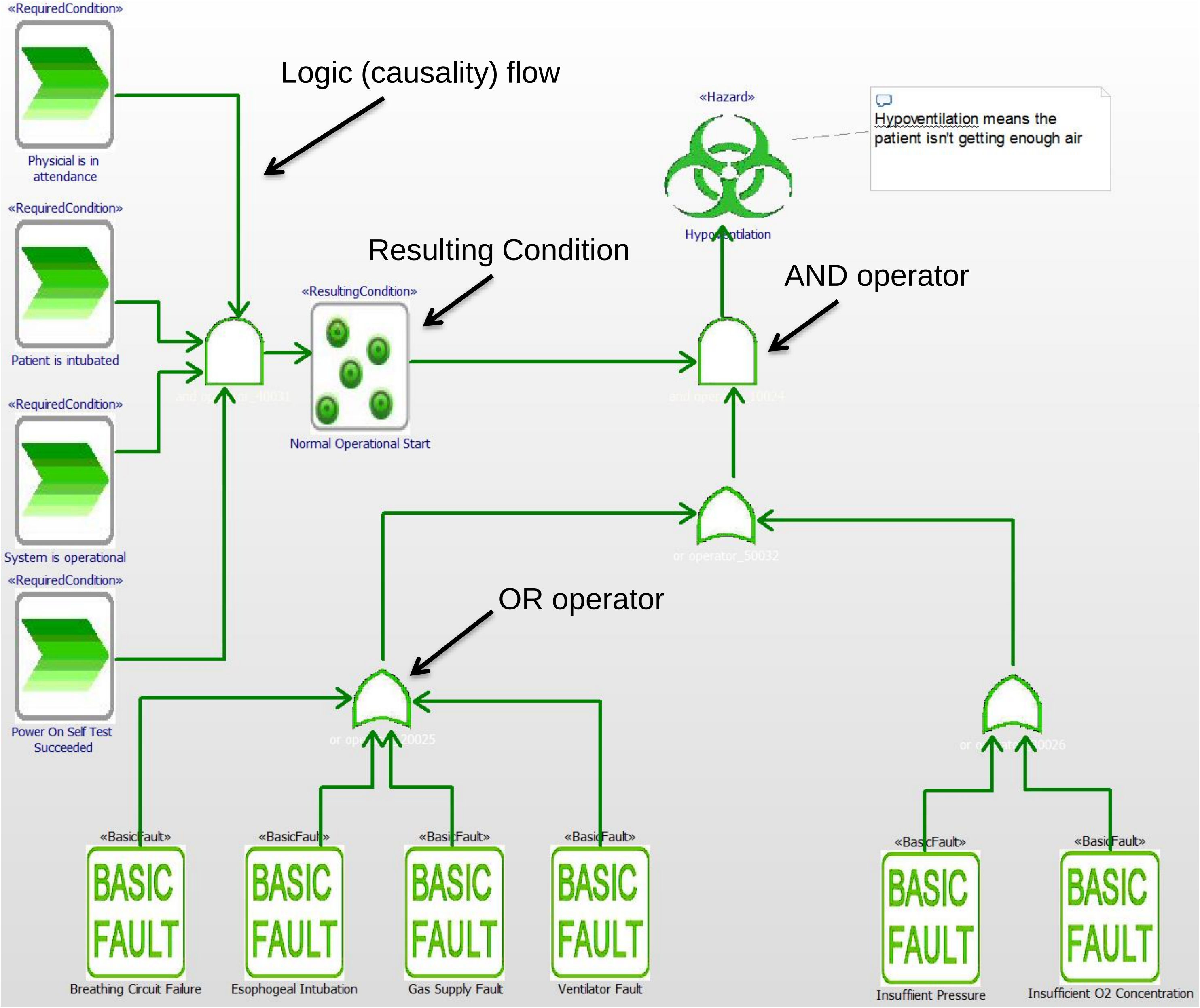
Example Fault Tree Analysis: Assumptions and Required Conditions



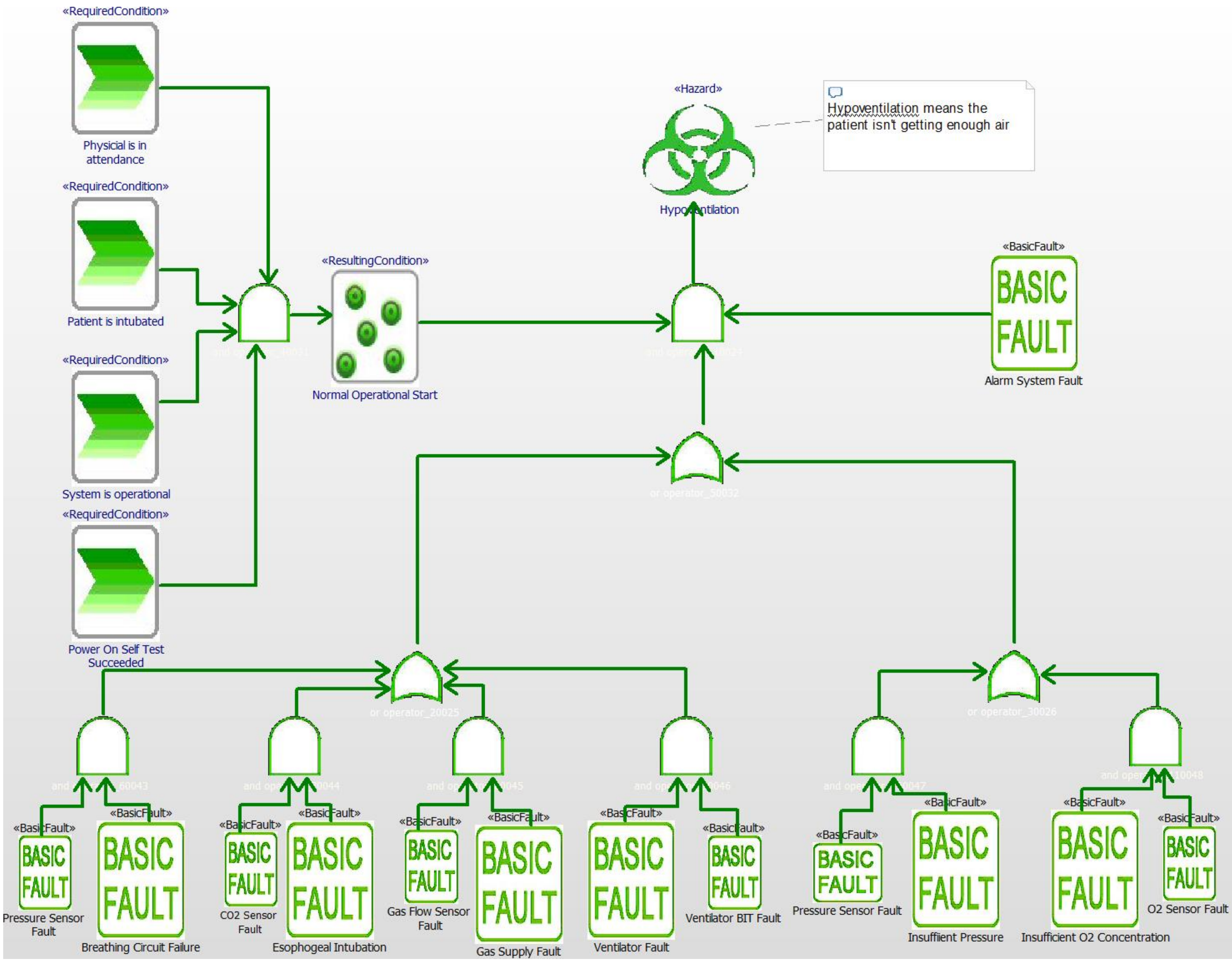
Example Fault Tree Analysis: Add Underlying causes



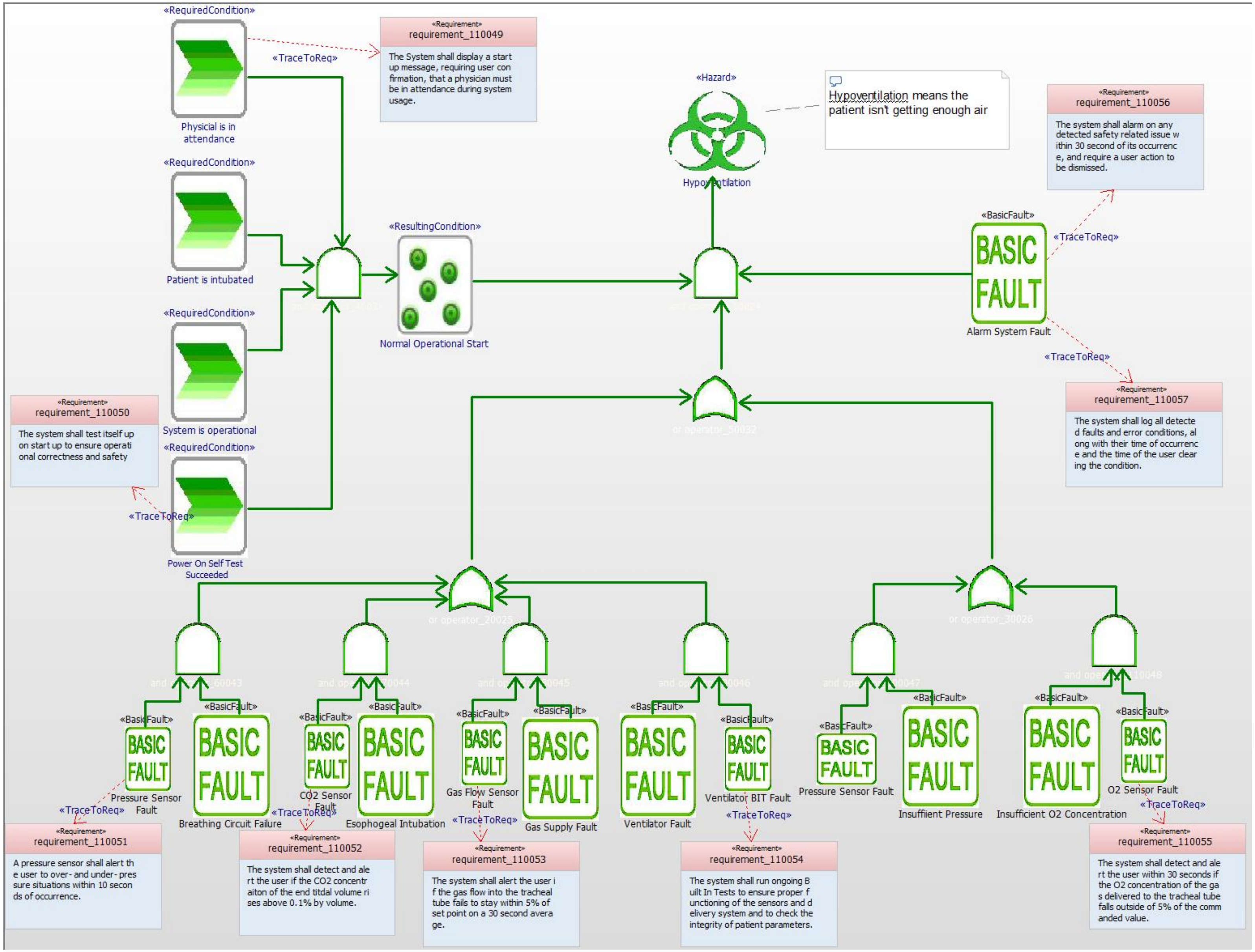
Example Fault Tree Analysis: Add logical operators and flows



Example Fault Tree Analysis: Add Control Measures



Example Fault Tree Analysis: Add Safety Requirements



Exercise: Identify Hazards and Faults

- An “E-Bike” (bicycle with an optional-use electric motor) is being designed. It is a standard bicycle but the user can also engage an electric motor to augment the force provided by pedaling. The motor can – by itself – power the bike up to 20 kph for up to 3 hours.
- Identify at least 5 hazards and 6 possible safety-relevant faults that could lead to those hazards

20 min

Exercise: Automotive braking system

- A braking system is being designed, activated by the driver depressing the pedal.
  - The amount of braking force applied is a function of the speed of the pedal movement, the force with which it is depressed, and the position of the pedal.
  - The braking controller monitors the vehicle speed and speed of the individual wheels (to determine slip and lock) as well as the brake pedal position, velocity, and acceleration.
  - Braking force is applied to the individual wheels via the braking actuation system.

- Step 1:
  - Review the simple design with all relevant elements on a SysML block diagram on the next page
- Step 2:
  - Hazard Identification
    - Identify at least three hazards of this system.
    - Fill in the hazard metadata for each hazard

10 min

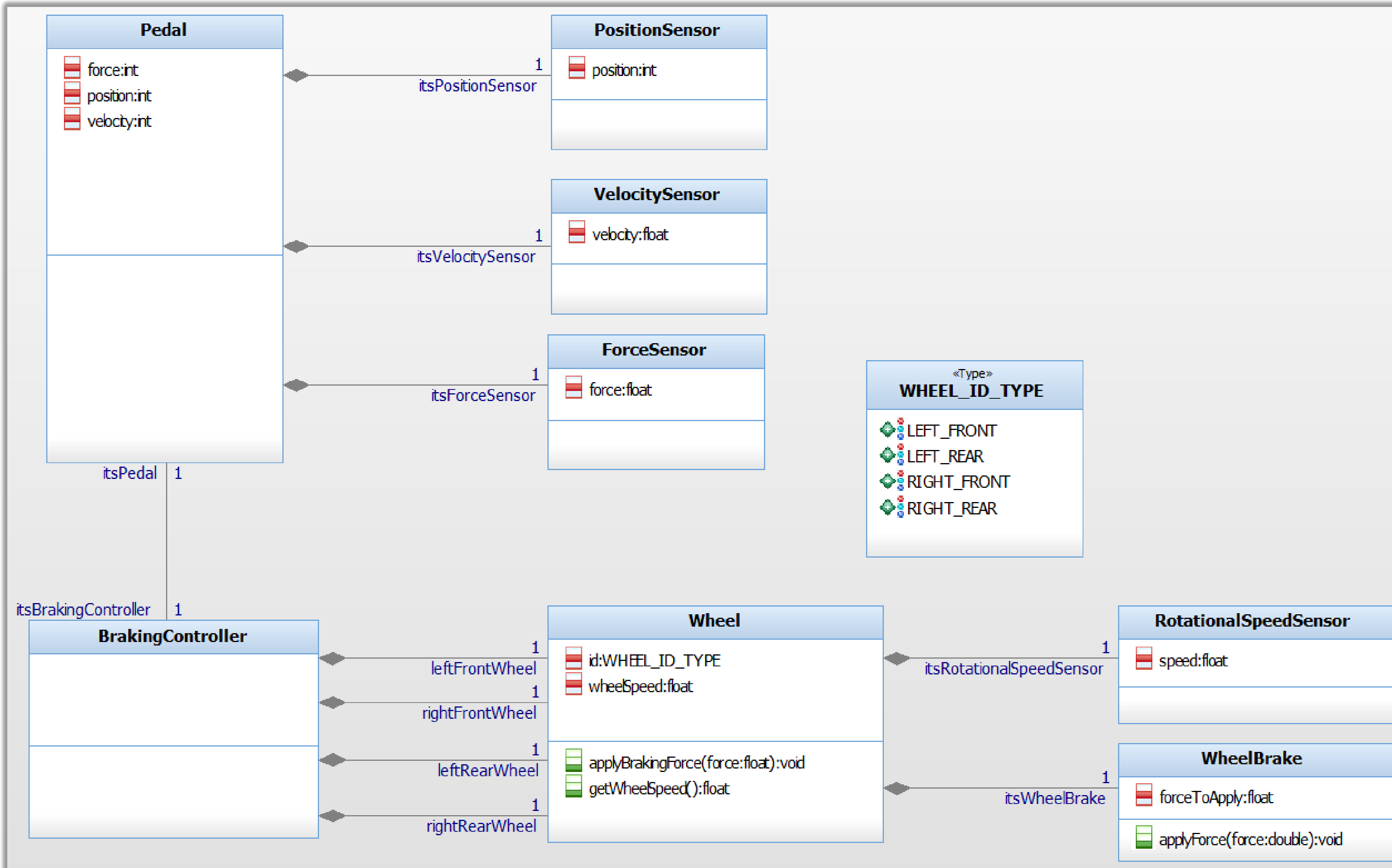
- Step 3: Create an FTA diagram for one such hazard, identifying
  - Hazard
  - Basic faults (at least five)
  - Required conditions

20 min

- Step 4: Add safety measures to address each basic fault (at least three in total)
  - Resulting safety requirements (at least three)

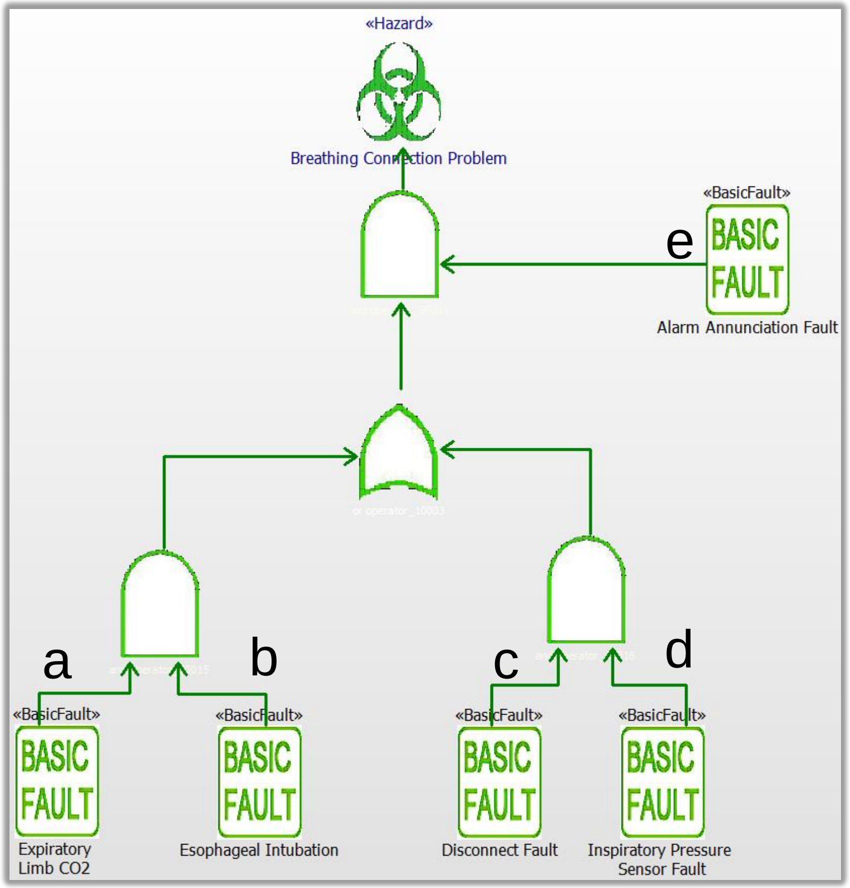
20 min

Braking Safety: Design: Step 1



Cut sets

- A **Cut Set** (aka *Minimal Cut Set*) is a collection of faults which, when taken together, can lead to a hazard
- **Cut Set Analysis** is the discovery of the complete set of cut sets
- There are *many* cut sets to be considered
  - In general, if you are considering n binary (present/non-present) conditions, then there are 2^n cut sets to be considered.
- Cut set analysis is done to ensure that there is no means by which the hazard condition can be attained that is unmitigated so that it is either
  - Unlikely enough
  - Not severe enough
- Consider the combination of faults in the figure:



Cut sets

Basic Fault/ Condition	a	b	c	d	e	Hazard
1	T	T	F	F	T	T
2	F	F	T	T	T	T
3	T	T	T	T	T	T
4	T	F	F	F	T	F
5	F	T	F	F	T	F
6	F	F	T	F	T	F
7	F	F	F	F	T	F
8	T	T	T	T	F	F
9	F	T	T	T	F	F
10	F	F	T	T	F	F
(22 more…)						

Hazard Risk

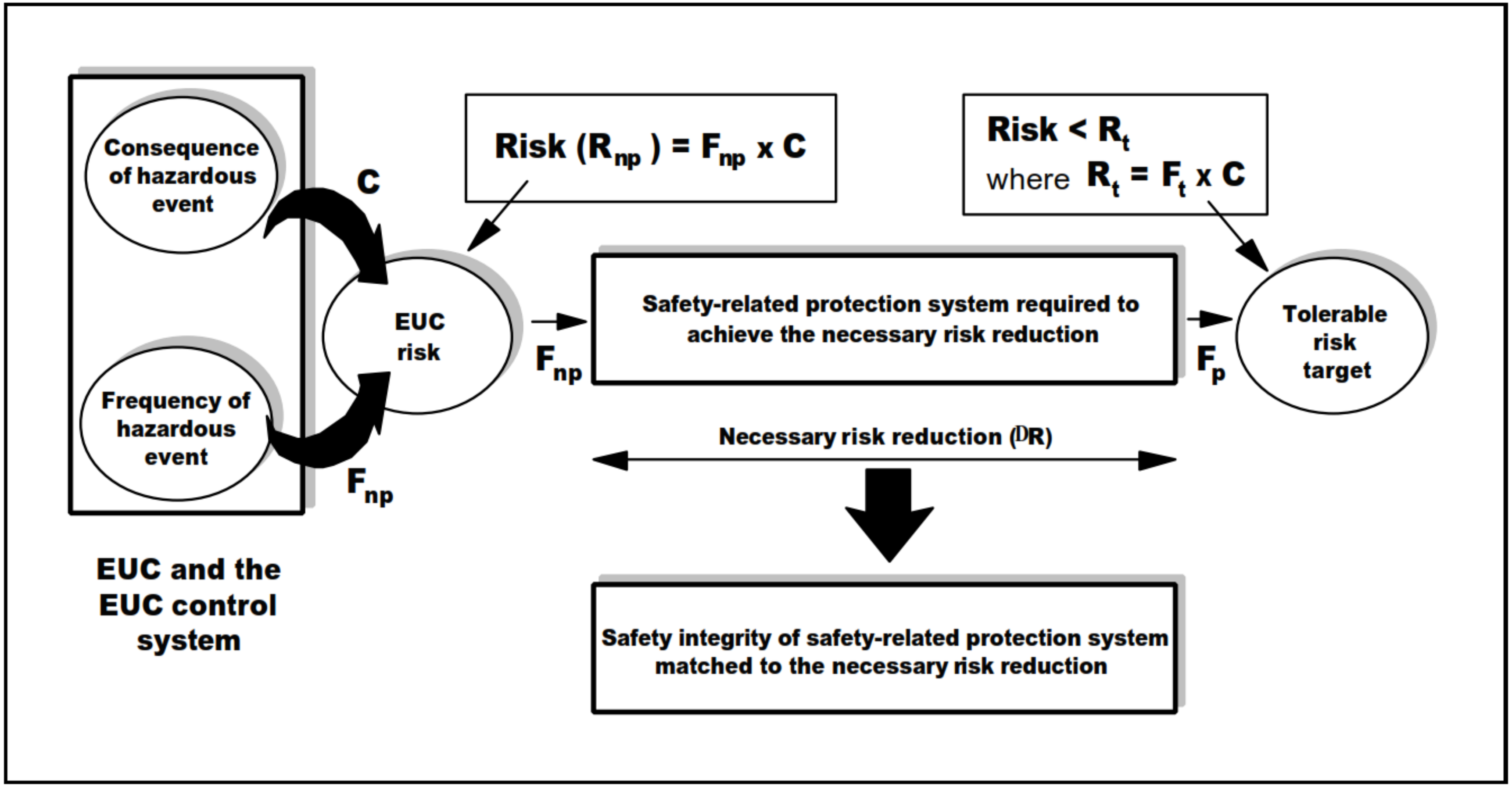
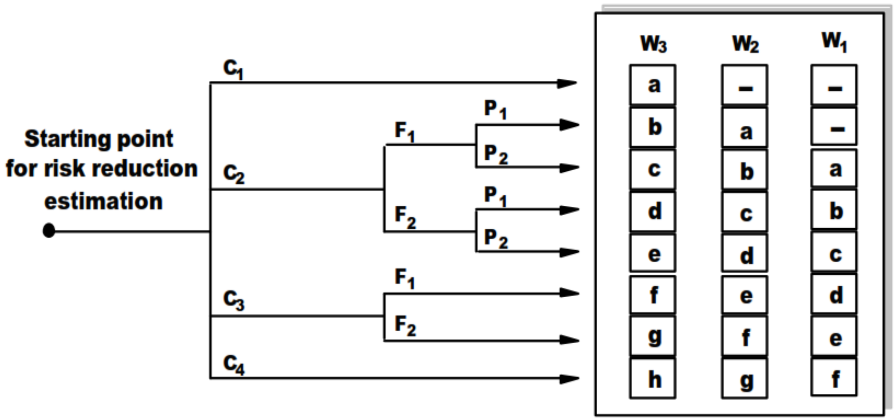


Figure C.1 — Safety integrity allocation: example for safety-related protection system

From: IEC 61508-5: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems

Risk Graph



a, b, c, d, e, f, g, h represent the necessary minimum risk reduction. The link between the necessary minimum risk reduction and the safety integrity level is shown in the table.

C = Consequence risk parameter

F = Frequency and exposure time risk parameter

P = Possibility of avoiding hazard risk parameter

W = Probability of the unwanted occurrence

a, **b**, **c** ... **h** = Estimates of the required risk reduction for the SRSs

Necessary minimum risk reduction	Safety integrity level
–	No safety requirements
a	No special safety requirements
b, c	1
d	2
e, f	3
g	4
h	An E/E/PE SRS is not sufficient

Determine SIL

Figure D.2 — Risk graph: example (illustrates general principles only)

From: IEC 61508-5: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems

Explanation of Risk Graph

Table D.1 — Example data relating to example risk graph (figure D.2)

Risk parameter		Classification	Comments
Consequence (C)	C_1	Minor injury	1 The classification system has been developed to deal with injury and death to people. Other classification schemes would need to be developed for environmental or material damage.
	C_2	Serious permanent injury to one or more persons; death to one person	2 For the interpretation of C_1, C_2, C_3 and C_4, the consequences of the accident and normal healing shall be taken into account.
	C_3	Death to several people	
	C_4	Very many people killed	
Frequency of, and exposure time in, the hazardous zone (F)	F_1	Rare to more often exposure in the hazardous zone	3 See comment 1 above.
	F_2	Frequent to permanent exposure in the hazardous zone	
Possibility of avoiding the hazardous event (P)	P_1	Possible under certain conditions	4 This parameter takes into account: — operation of a process (supervised (ie operated by skilled or unskilled persons) or unsupervised); — rate of development of the hazardous event (for example suddenly, quickly or slowly); — ease of recognition of danger (for example seen immediately, detected by technical measures or detected without technical measures); — avoidance of hazardous event (for example escape routes possible, not possible or possible under certain conditions); — actual safety experience (such experience may exist with an identical EUC or a similar EUC or may not exist).
	P_2	Almost impossible	
Probability of the unwanted occurrence (W)	W_1	A very slight probability that the unwanted occurrences will come to pass and only a few unwanted occurrences are likely	5 The purpose of the W factor is to estimate the frequency of the unwanted occurrence taking place without the addition of any safety-related systems (E/E/PE or other technology) but including any external risk reduction facilities.
	W_2	A slight probability that the unwanted occurrences will come to pass and few unwanted occurrences are likely	6 If little or no experience exists of the EUC, or the EUC control system, or of a similar EUC and EUC control system, the estimation of the W factor may be made by calculation. In such an event a worst case prediction shall be made.
	W_3	A relatively high probability that the unwanted occurrences will come to pass and frequent unwanted occurrences are likely	

From: IEC 61508-5: Functional Safety of Electrical/ Electronic/ Programmable Electronic Safety-Related Systems

IEC 61508 Risk Targets

Low demand operation

SIL	Probability of Failure per Hour	Risk Reduction Factor
1	10^{-1} to 10^{-2}	10 – 100
2	10^{-2} to 10^{-3}	100 – 1000
3	10^{-3} to 10^{-4}	1000 – 10,000
4	10^{-4} to 10^{-5}	10,000 – 100,000

Note that 100,000 hours is 4167 days or 11 years, 5 months of operation before a fault would be expected

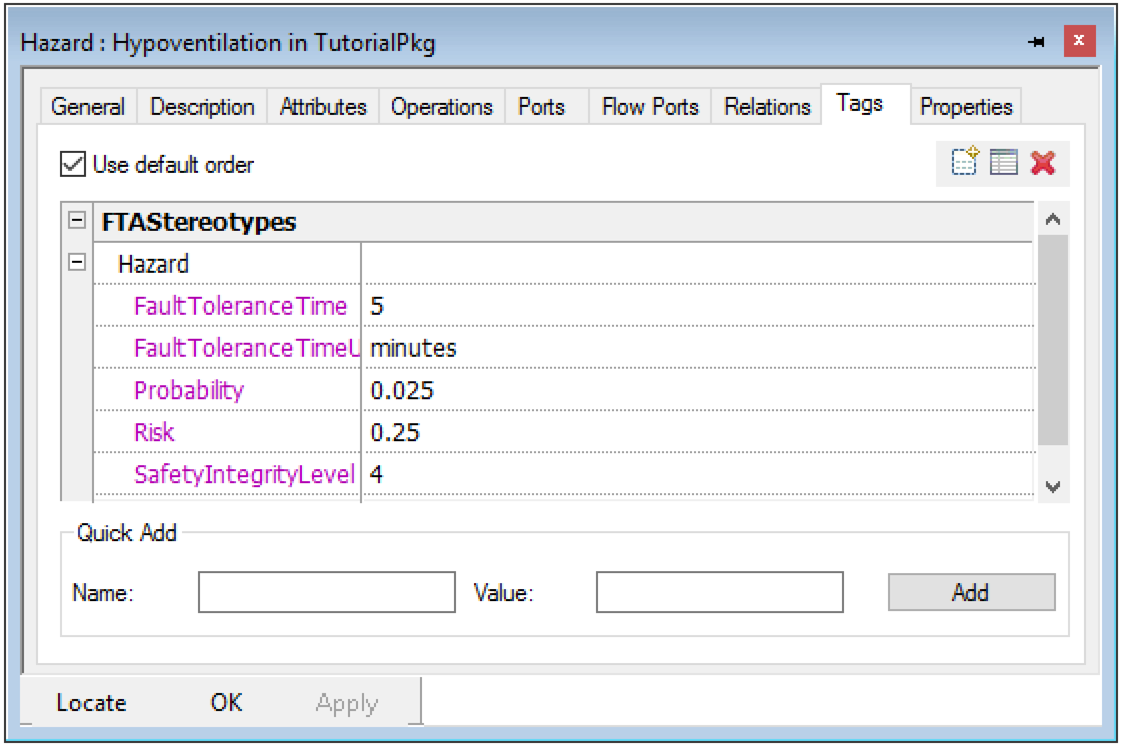
Continuous demand operation

SIL	Probability of Failure per Hour	Risk Reduction Factor
1	10^{-5} to 10^{-6}	100,000 – 1,000,00
2	10^{-6} to 10^{-7}	1,000,000 – 10,000,000
3	10^{-7} to 10^{-8}	10,000,000 – 100,000,000
4	10^{-8} to 10^{-9}	100,000,000 – 1,000,000,000

Note that 1,000,000,000 hours 114,155 years of operation before a fault would be expected

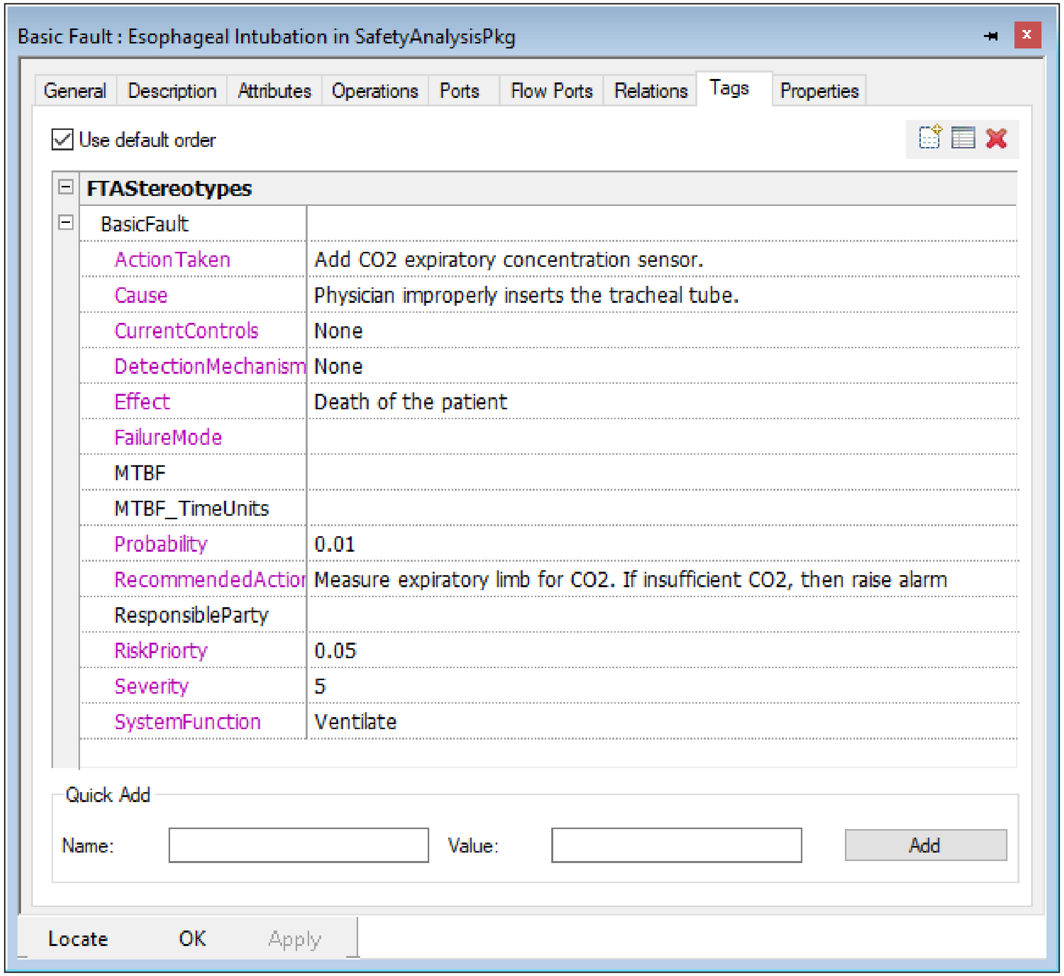
Hazard Severity and Probability

- Hazards can not, in general, be completely obviated. That means *they can, and will occur*
- Safety standards dictate acceptable levels of severity and likelihood for faults.
- This safety data is captured in the hazard metadata



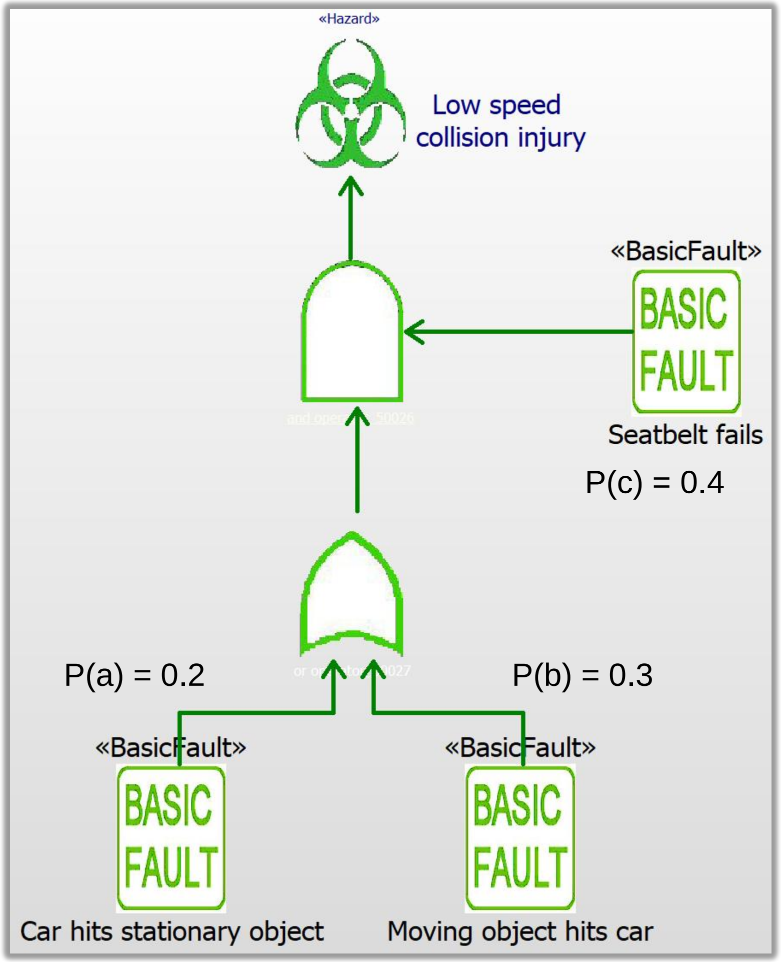
Fault Severity and Probability

- Faults similarly have probability
  - Their severity is that of the worse hazard severity in a cut set in which the fault participates



Calculating the likelihood of hazards

- Assuming two conditions, a and b are independent and not mutually exclusive then
  - For a AND b, the likelihood of a TRUE outcome is p(a AND b) = p(a) * p(b)
  - For a OR b, the likelihood of a TRUE outcome is p(a OR b) = p(a) + p(b) – p(a AND b)



Analysis

P(a OR b) = .2 + .3 - .06 = .44

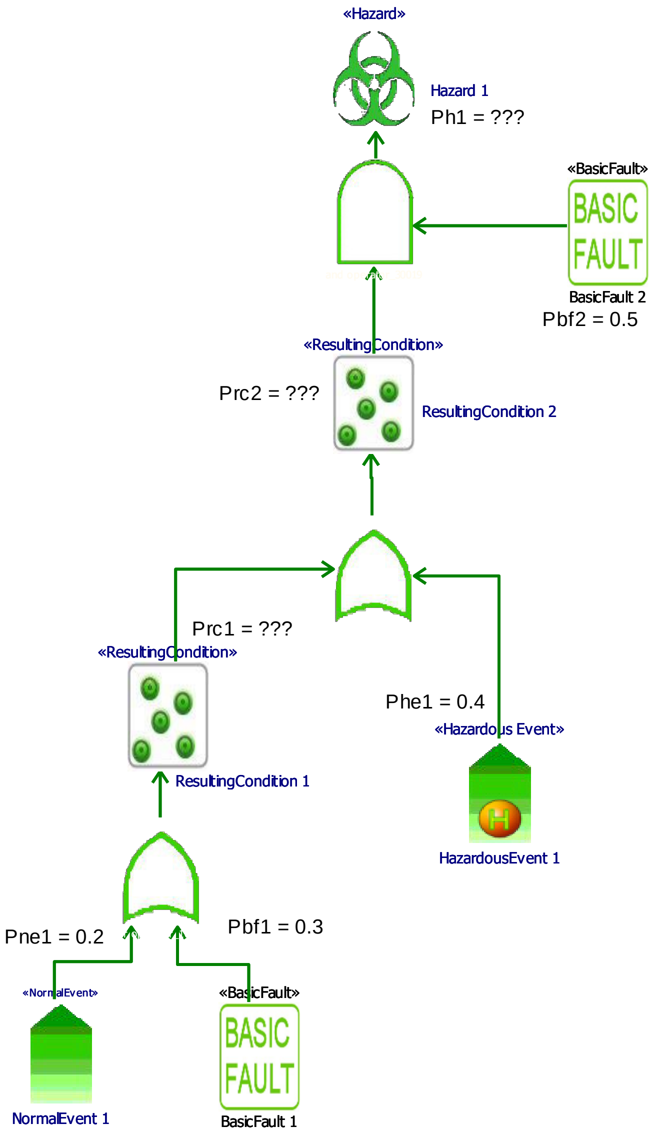
P((a OR b) AND c) = .44 * 4 = .176

Generally, the probabilities dealt with in safety critical systems are between 10^{-4} and 10^{-9}

Calculating the likelihood of hazards

- You can calculate the hazard probability via "propagation of probabilities" by performing computations up the causal chain.
- Probability Computation
  - Step 1: Create FTA
  - Step 2: Document primitive fault probabilities
    - Assume **Required Conditions** and **Required Events** have probability 1.0
  - Step 3: Write the FTA as a succession of equations
    - AND: $P_{AND} = P_1 * P_2$ where P_1 is the probability of input 1 & P_2 is the probability of input 2
    - OR: $P_{OR} = P_1 + P_2 – P_1 * P_2$
    - NOT: $P_{NOT} = 1.0 - P_1$
    - NAND: $P_{NAND} = 1.0 - P_1 * P_2$
    - NOR: $P_{NOR} = 1.0 - P_1 + P_2 – P_1 * P_2$
    - XOR: Remember: P_{XOR} = (P_1 AND (NOT P_2)) OR ((NOT P_1) AND P_2)
      so $P_{XOR} = (P_1 * (1.0-P_2)) + ((1.0-P_1) * P_2) - (P_1 * (1.0-P_2)) * ((1.0-P_1) * P_2)$
  - Step 4: Do the math
  - Step 5: Repeat in the next step of the causal chain

Calculating the likelihood of hazards: Doing the math

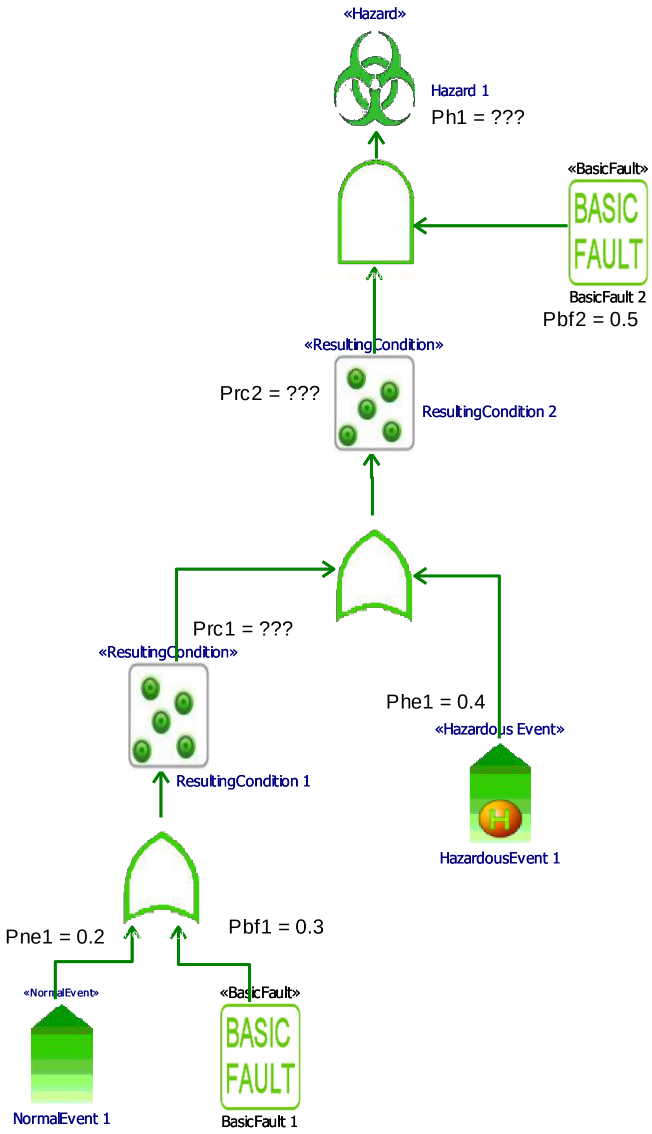


- Prc1 = Pre1 + Pbf1 – Pre1*Pbf1
  = 0.2 + 0.3 – 0.2*0.3 = 0.44
- Prc2 = Prc1 + Phe1 – Prc1*Phe1
  = 0.44 + 0.4 – 0.44*0.4 = 0.664
- Ph1 = Prc2 * Pbf2
  = 0.664 * 0.5 = 0.332
- So the probability of the hazard is 0.332

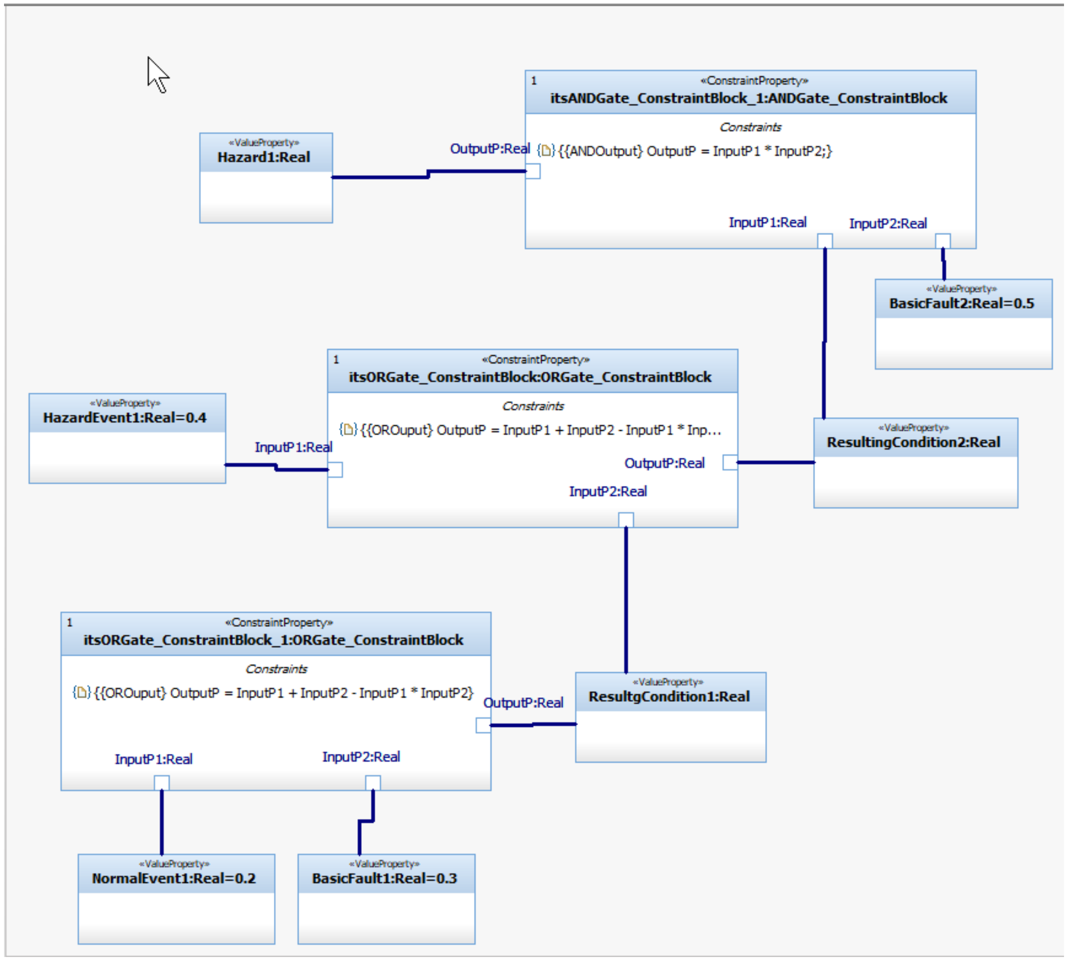
- As previously mentioned, the probabilities are usually more in the range of 10^{-4} to 10^{-9}

- Recompute the hazard risk for the following probabilities:
  – Pre1 = 0.1
  – Pbf1 = 0.2×10^{-6}
  – Pbf2 = 0.25×10^{-6}
  – Phe1 = 0.15×10^{-7}
- What is
  – Prc1
  – Prc2
  – Ph1

Calculating the likelihood of hazards: Doing the math

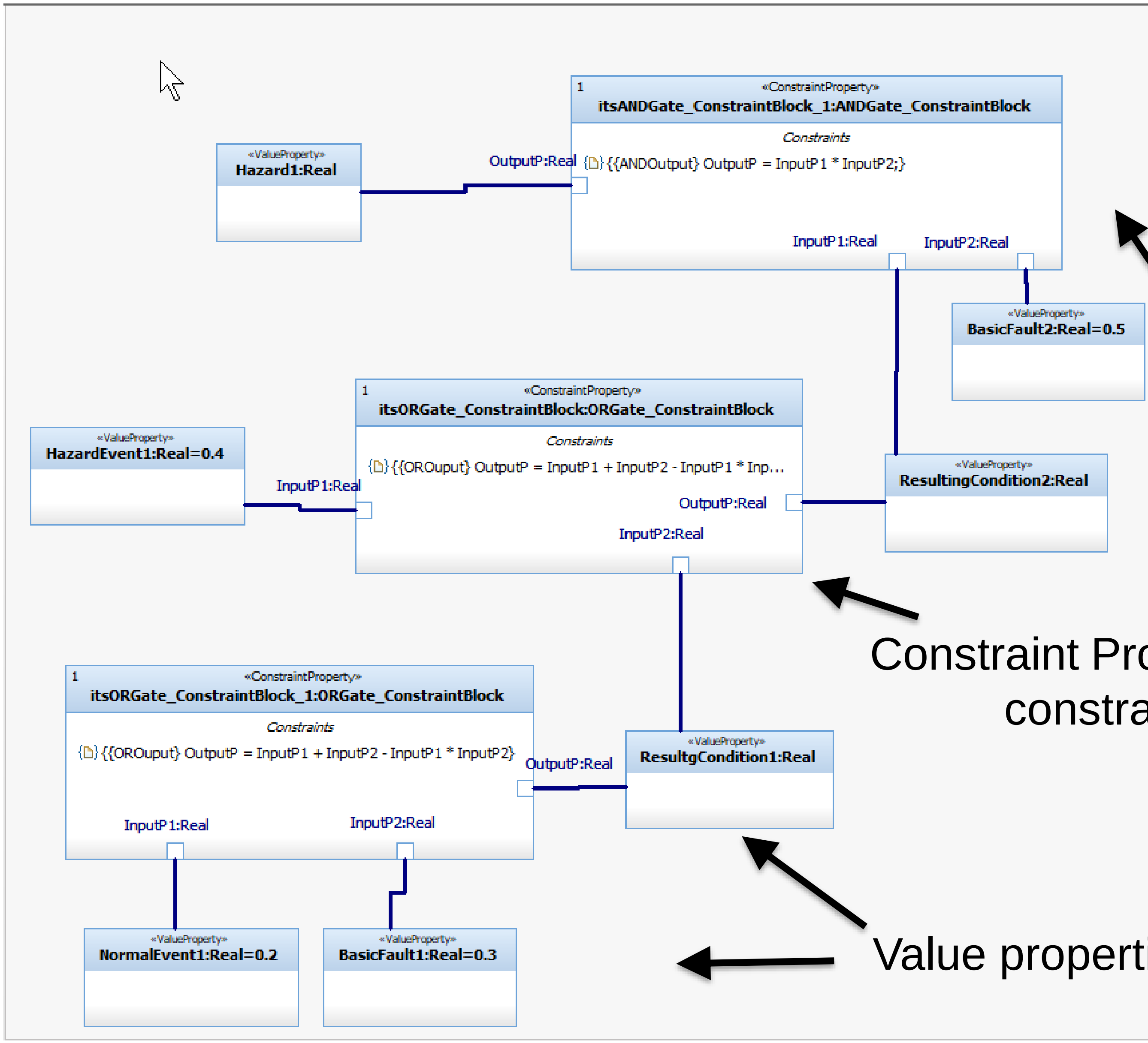


=



Doing the math with a parametric diagram

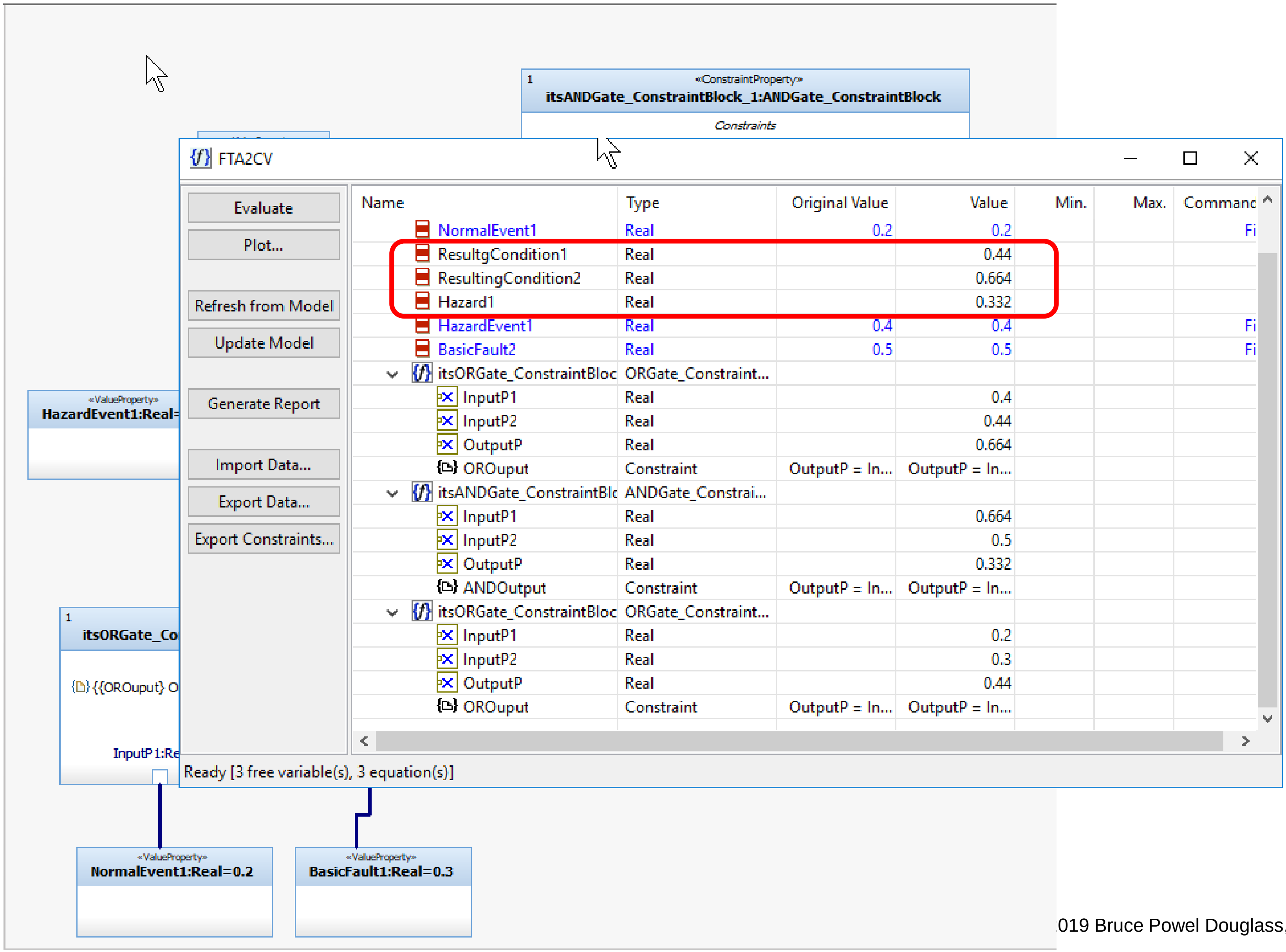
Doing the Math with a Parametric Diagram



Constraint Properties (from the constraint blocks)

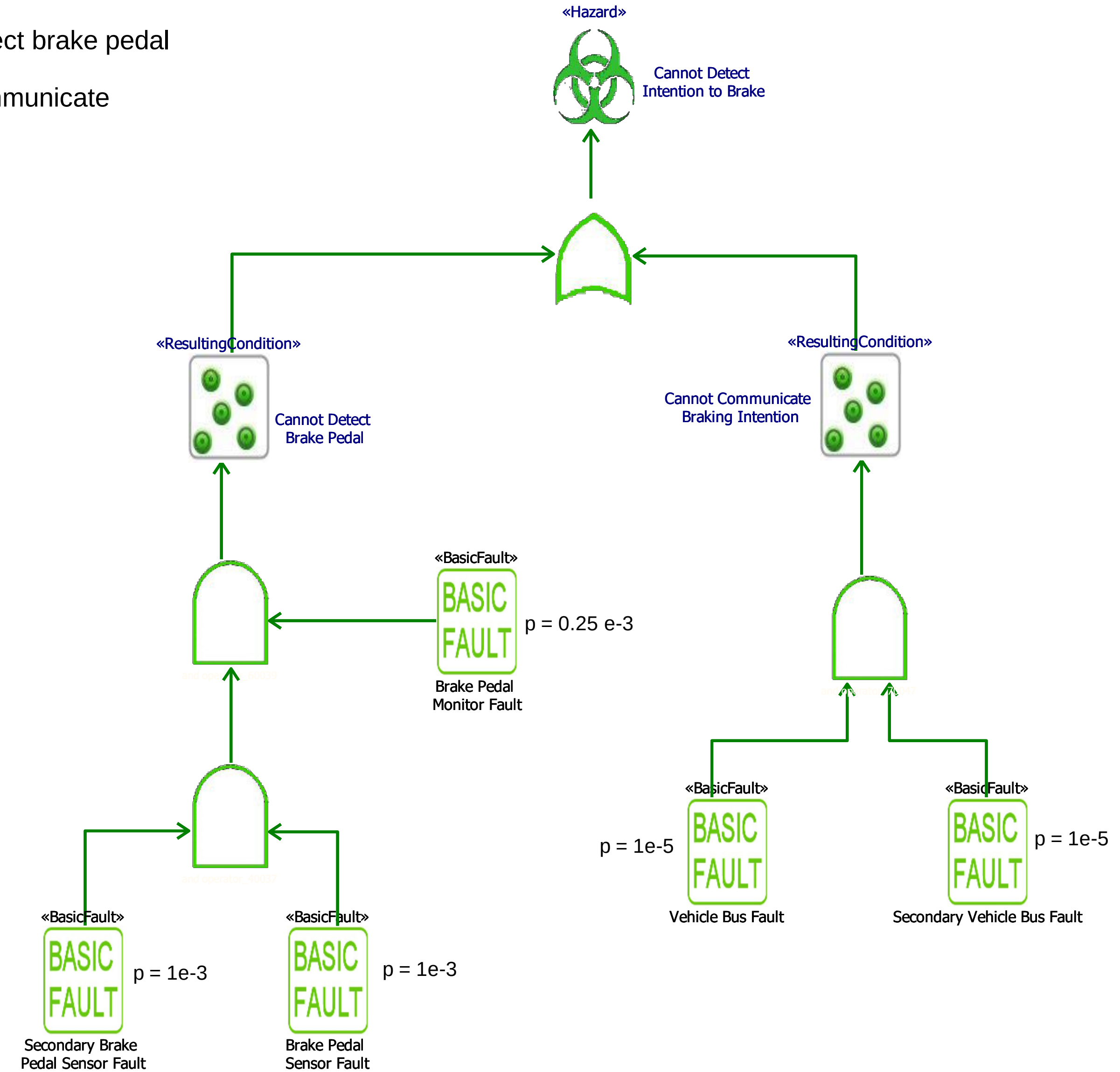
Value properties

Doing the Math with a Parametric Diagram



Exercise: Calculate the Hazard Probability

- Compute
  - $P_{\text{cannot detect brake pedal}}$
  - $P_{\text{cannot communicate}}$
  - P_{hazard}



20 min

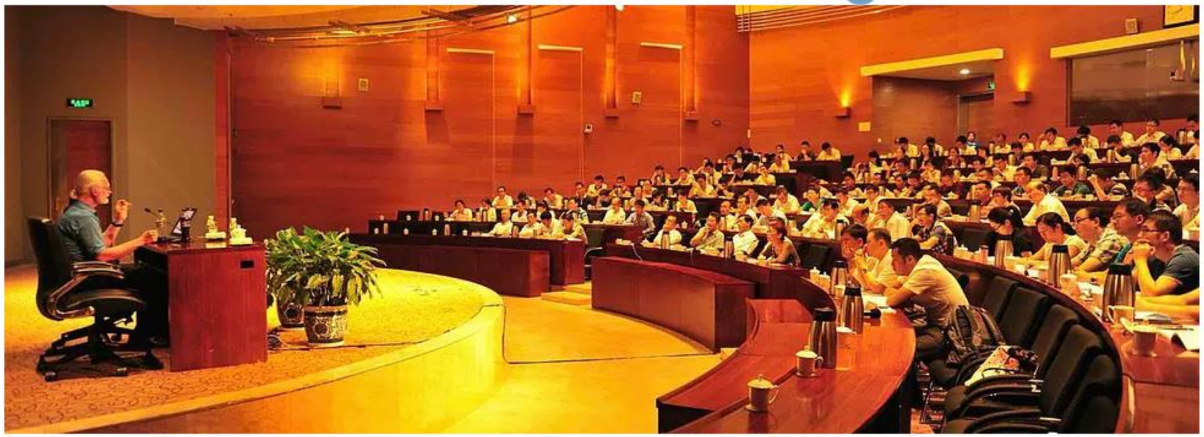
Bruce Powel Douglass, Ph.D.

Log In

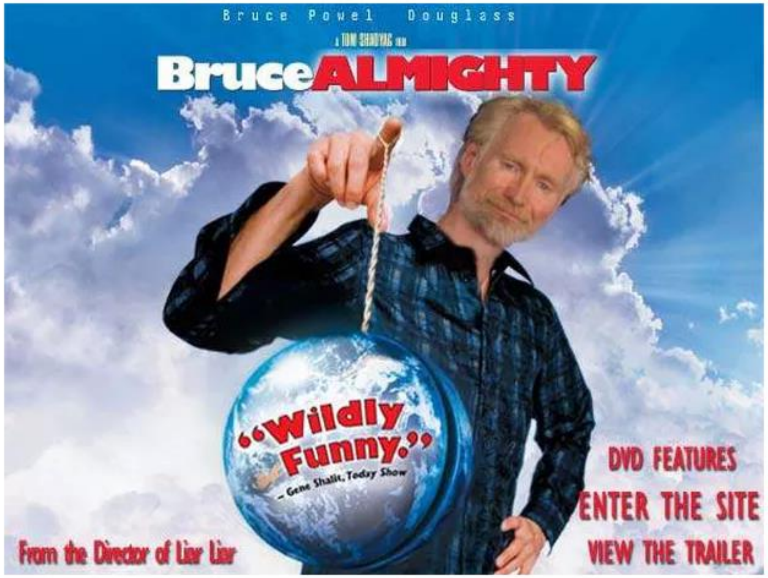
Content | Services | Public Interest | Blog | What's New | Forum | About | Comments | Site Map | Geekosphere | Member

Real-Time Agile Systems and Software Development

Welcome to **www.bruce-douglass.com**



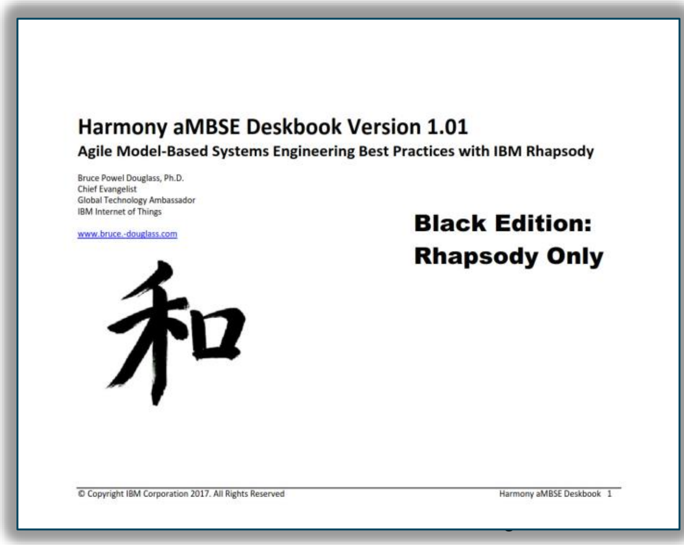
Site Map



You've found yourself on **www.bruce-douglass.com,** my web site on all things real-time and embedded.

On this site you will find papers, presentations, models, forums for questions / discussions, and links (lots of links) to areas of interest, such as

- Developing Embedded Software
- Model-Driven Development for Real-Time Systems
- Model-Based Systems Engineering
- Safety Analysis and Design
- Agile Methods for Embedded Software
- Agile Methods for Systems Engineering
- The Harmony agile Model-Based Systems Engineering process
- The Harmony agile Embedded Software Development process
- Models and profiles I've developed and authored
- List and links to many of my books.



Harmony aMBSE Deskbook Version 1.01

Agile Model-Based Systems Engineering Best Practices with IBM Rhapsody

Bruce Powel Douglass, Ph.D.
Chief Evangelist
Global Technology Ambassador
IBM Internet of Things

www.bruce-douglass.com

Black Edition: Rhapsody Only

和

MBSE and Safety Analysis:
Answers to Exercises

Bruce Powel Douglass, Ph.D.
Chief Evangelist, IBM IoT
www.bruce-douglass.com
Twitter: @IronmanBruce

E-Bike Hazards and Faults

Hazards

- Inability to steer
- Inability to brake
- Motor speed too fast
- Inability to disengage motor
- Fire
- Electrical shock

Faults

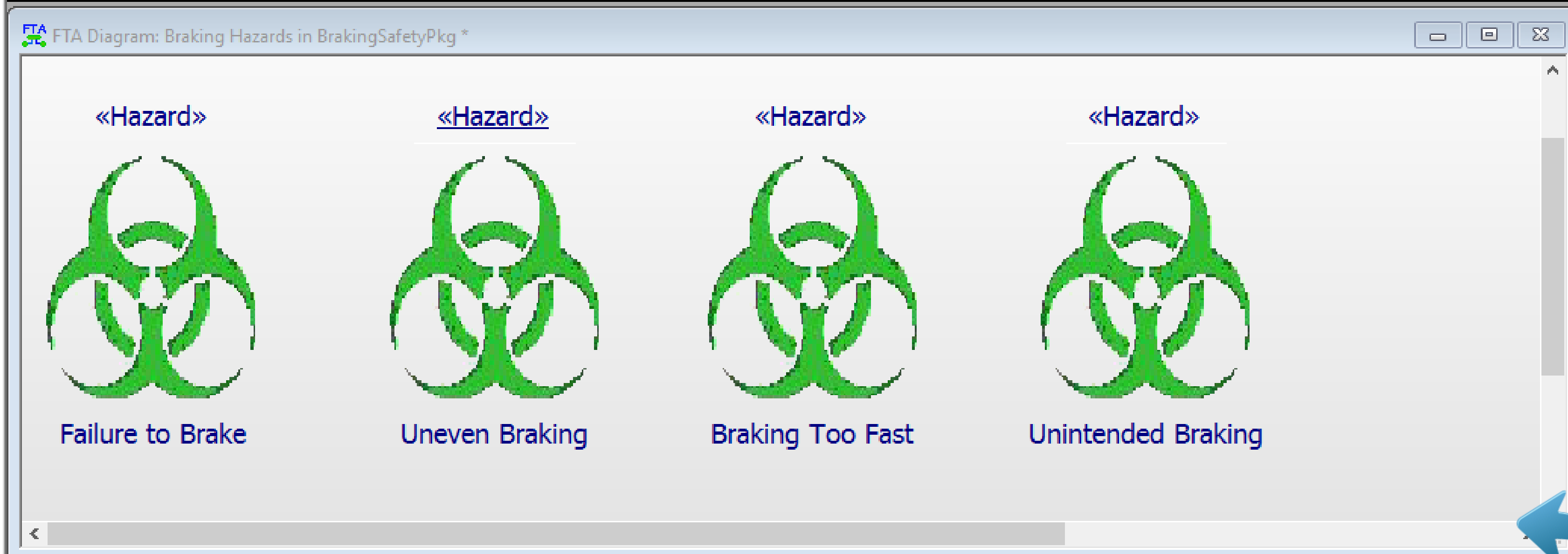
- Steering tube freezes
- Steering tube loosens
- Braking caliper failure
- Braking cable freezes
- Braking cable slips
- Electrical short (casing)
- Electrical short (internal)
- User motor control knob fault
- Motor controller fault

Braking Safety: Hazards: Step 2

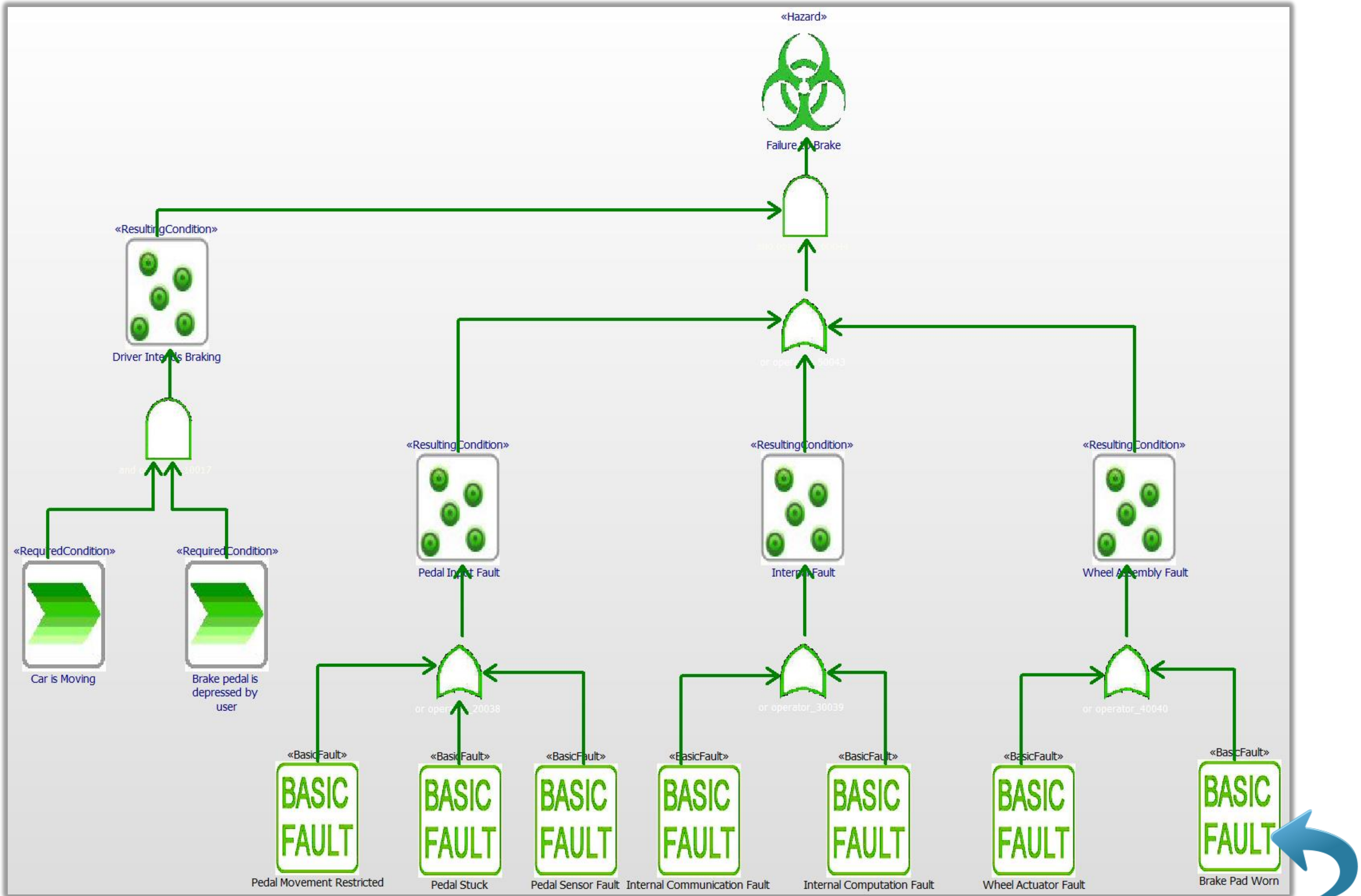
hazard table_9

Found 4 elements

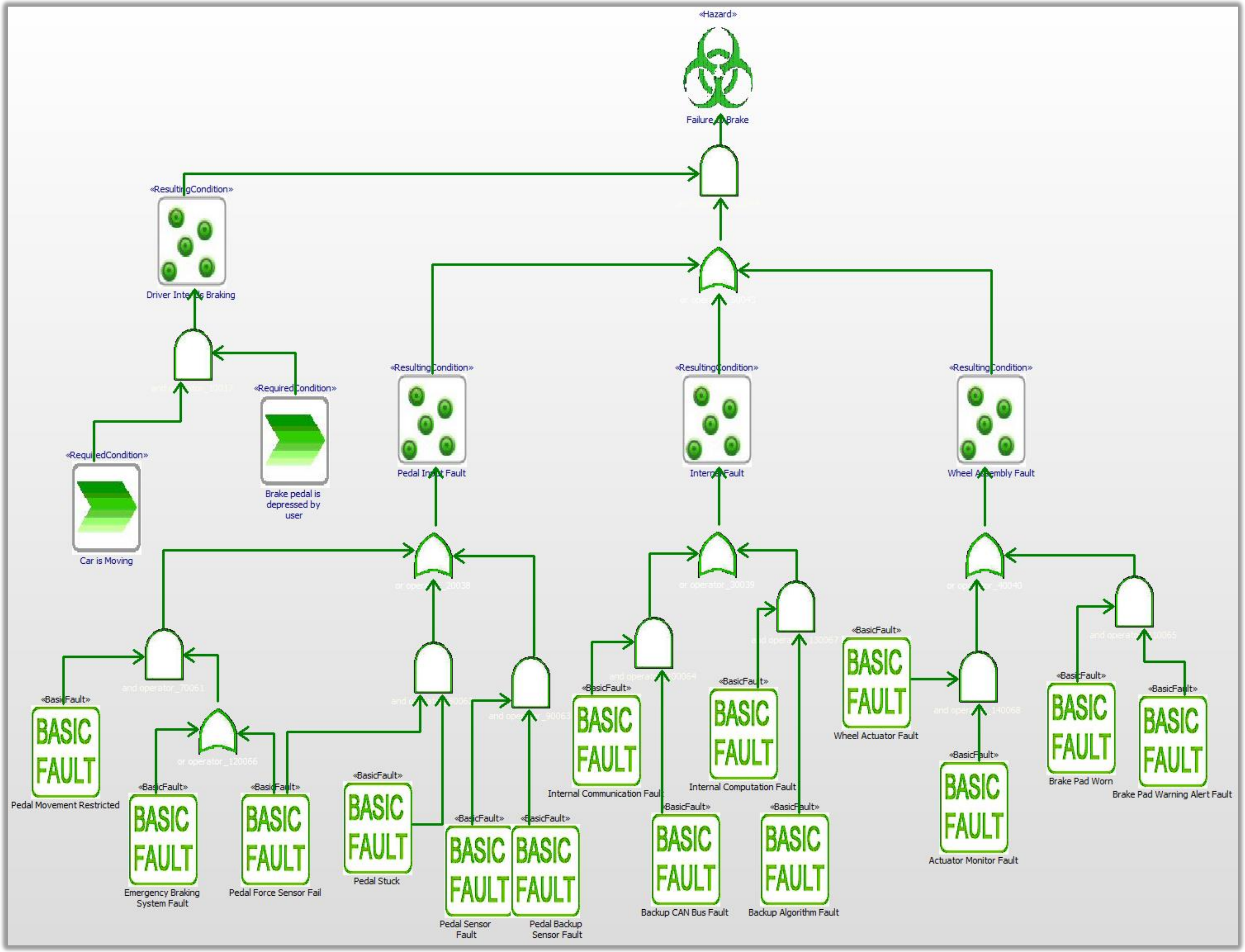
Name	Description	Probability	Severity	Risk	SafetyIntegrityLevel	FaultToleranceTime	FaultToleranceTimeUnits
Braking Too Fast	This hazard occurs when the application of braking force is too rapid or too strong causing the loss of control of the vehicle or damage to occupants of the car.	1e-10	6	6e-10	4	0.5	
Failure to Brake	This hazard occurs when the driver wants to brake but the breaking does not occur with sufficient force or operate within the sufficient timeframe to avoid a collision	1e-9	6	6e-9	4	1	
Uneven Braking	This hazard occurs when the braking force is applied unevenly to the wheels so as to induce a loss of vehicular control.	1e-7	6	6e-7	3	200	miliseconds
Unintended Braking	This hazard occurs when braking forces are applied when this is not the driver intent, causing a loss of vehicular control.	1e-9	7	7e-9	4	250	miliseconds



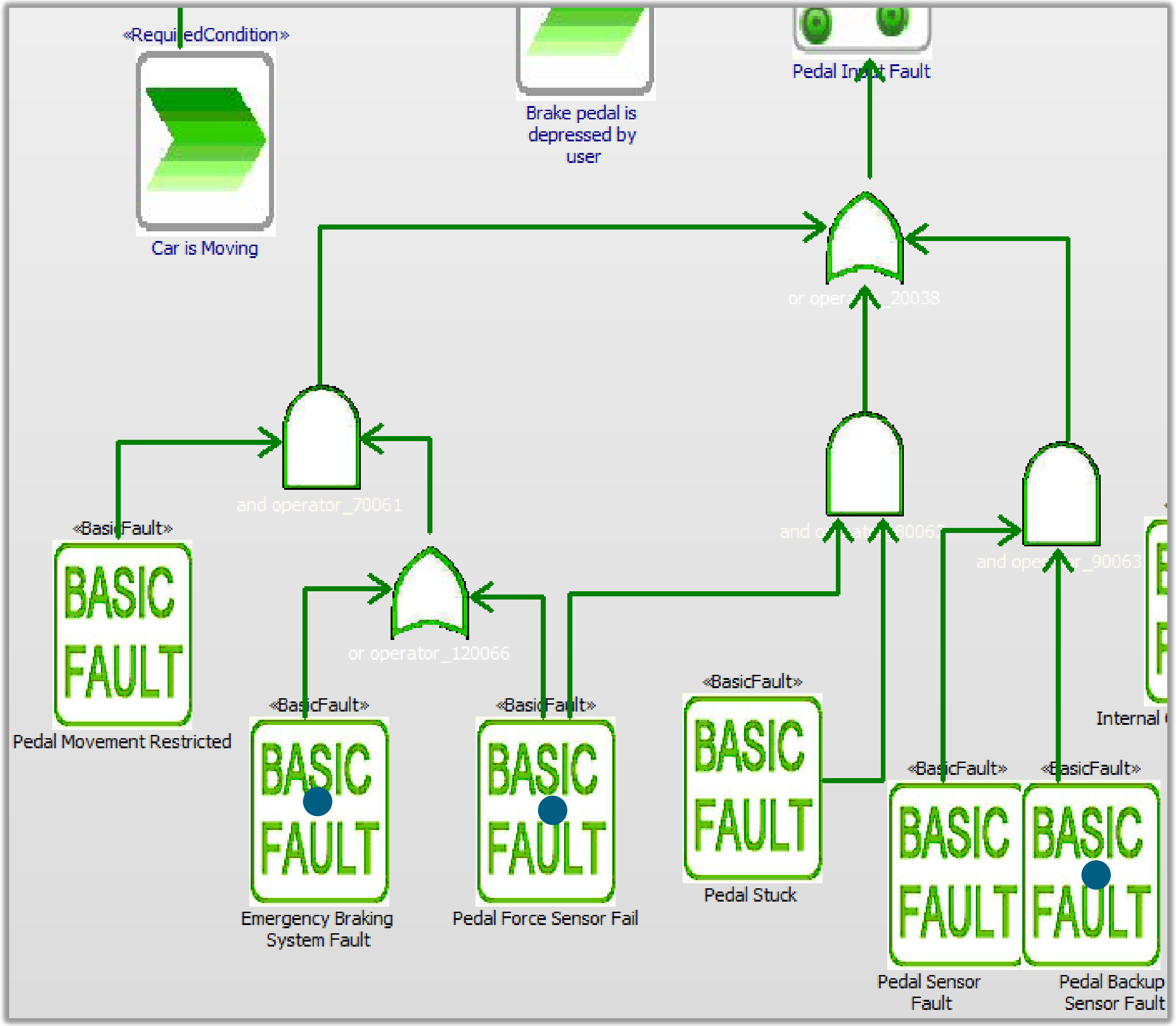
Braking Safety: FTA Step 3



Braking Safety: FTA Step 4

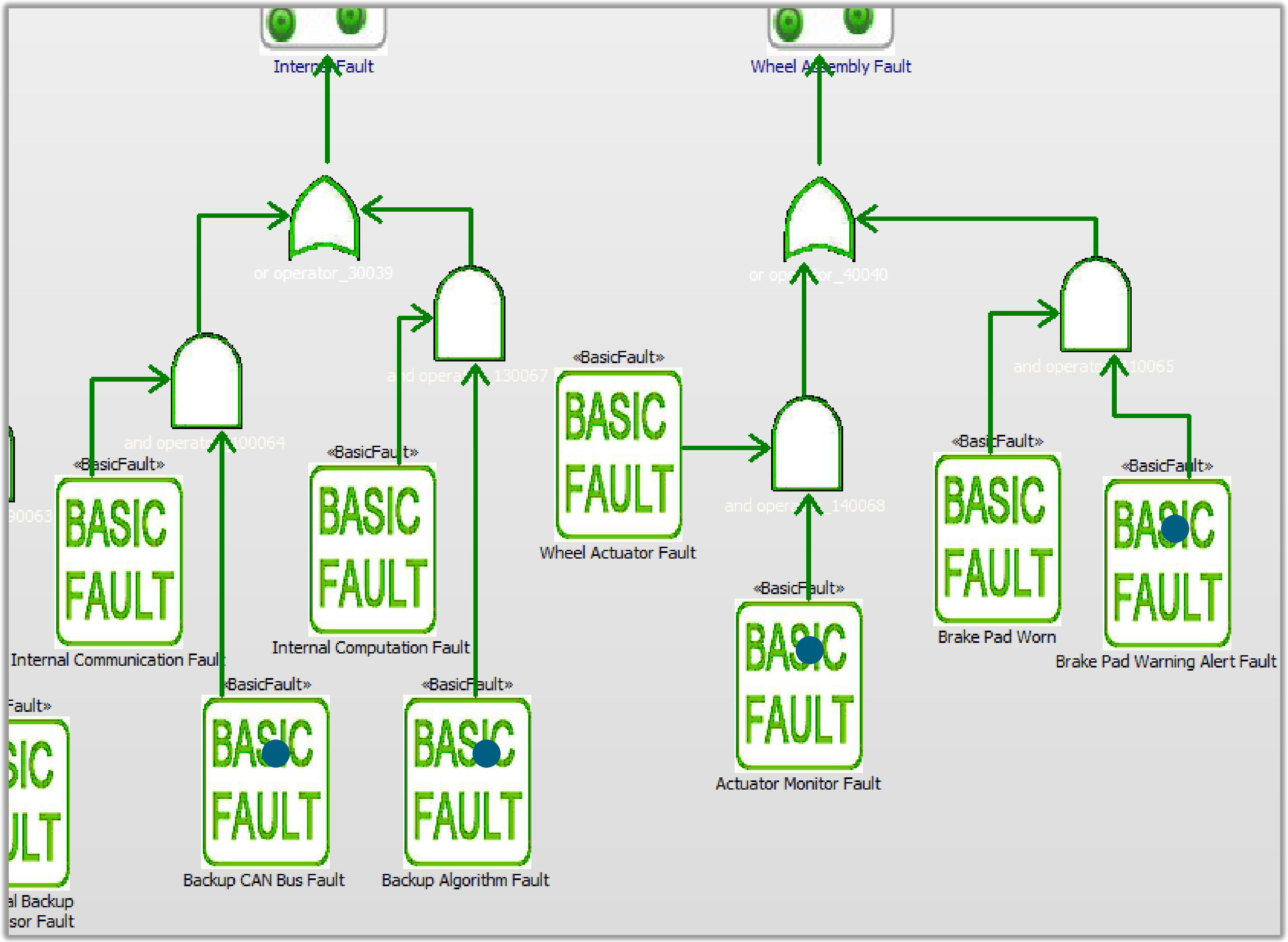


Braking Safety: FTA Step 4



- Highlights added control measure

Braking Safety: FTA Step 4



Braking Hazard Probabilities

"Show Formula" View

1	Brake Sensor Fault	2nd Brake sensor fault	Monitor Fault	Bus Fault	2nd Bus Fault	Cannot Detect	Cannot Comm	Hazard
2	=0.001	=0.001	0.00025	0.00001	0.00001	=A2*B2*C2	=D2*E2	=F2+G2-F2*G2

"Show Value" View

	A	B	C	D	E	F	G	H
1	Brake Sensor Fault	2nd Brake sensor fault	Monitor Fault	Bus Fault	2nd Bus Fault	Cannot Detect	Cannot Comm	Hazard
2	0.001	0.001	2.50E-04	1.00E-05	1.00E-05	2.50E-10	1.00E-10	3.50E-10