Understanding control effectiveness requires structured hazards

Phil Cook, Neil Robinson, and Tim McComb
RGB Assurance

Australian System Safety Conference 2024
Brisbane, Queensland

23 October 2024

Background

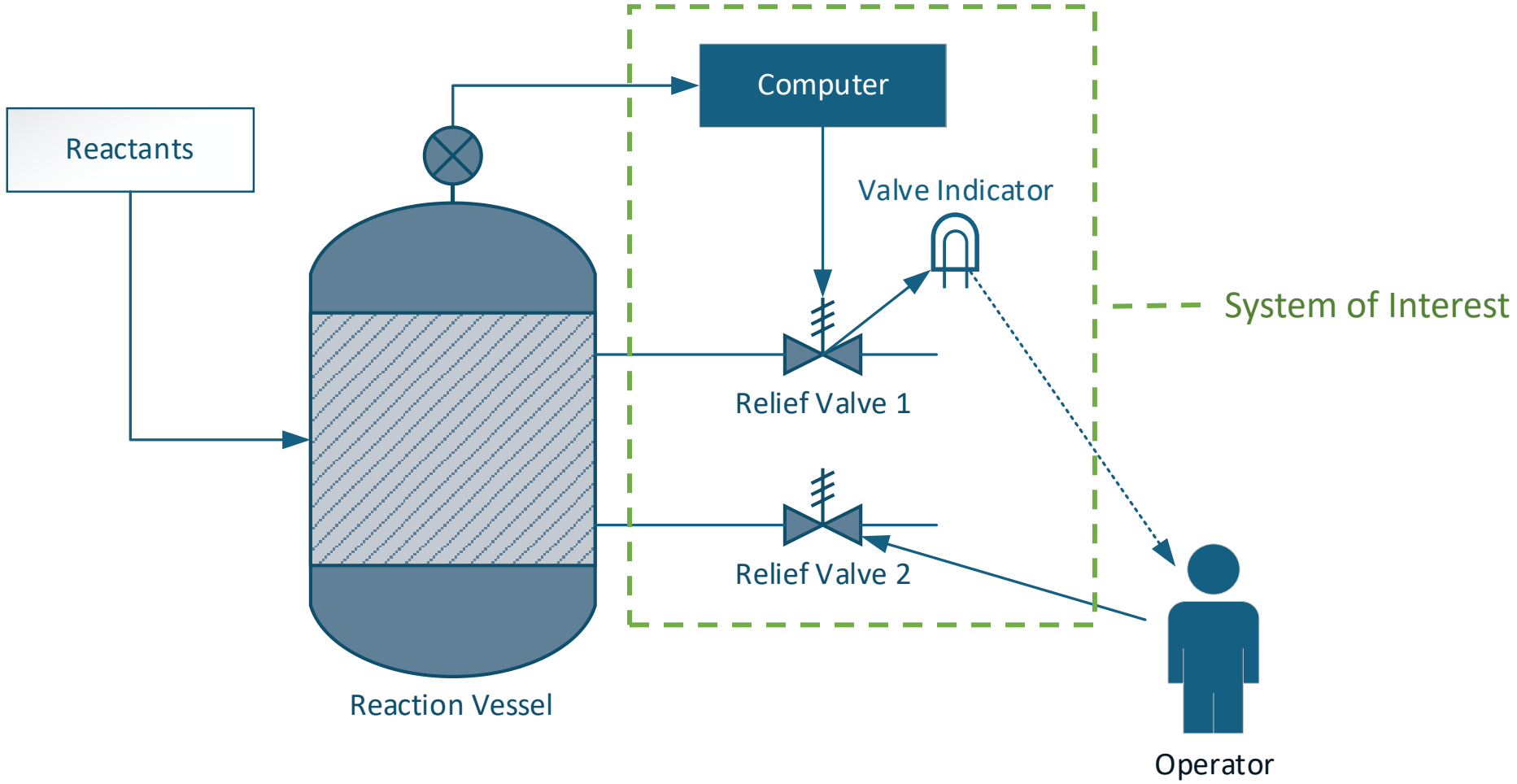
- Attempts to “rate” hazard controls in terms of (perceived) “effectiveness” are common
  - Especially in WHS contexts, but increasingly in System Safety Engineering
- Not unreasonable to ask:
  - Is this control (or set of controls) good enough?
  - [Conversely: Is it too much?]
- Alternatively:
  - Have we done everything we can or should to reduce safety risk?
  - Are we getting good “bang for buck” out of our hazard controls?

- These are not easy questions to answer…
- In attempting to do so, we need to think about:
  - How do we measure effectiveness?
  - How should we articulate hazards to enable us to do this?

Outline

- Running Example; Example Hazard Log Entry
- The Problem; What do we mean by “Control Effectiveness”?
- A Structured Approach to Hazard Logs
- Control Effectiveness – Take 2
- Using Fuzzy Logic to Assess Control Coverage
- Further Thoughts
- Conclusions

Example



Adapted from Leveson (1995): *Safeware: system safety and computers*

Example Hazard Log Entry

Hazard	Causes	Accident	Controls
Failure to manage high pressure	• Valve 1 failure • Valve 2 failure • Computer does not open valve 1 • Indicator failure • Operator inattentiveness	Explosion	• Valve reliability • Valve maintenance • Safety integrity of computer • Indicator reliability • Operator fatigue management

The Problem

Controls

- Valve reliability
- Valve maintenance
- Safety integrity of computer
- Indicator reliability
- Operator fatigue management

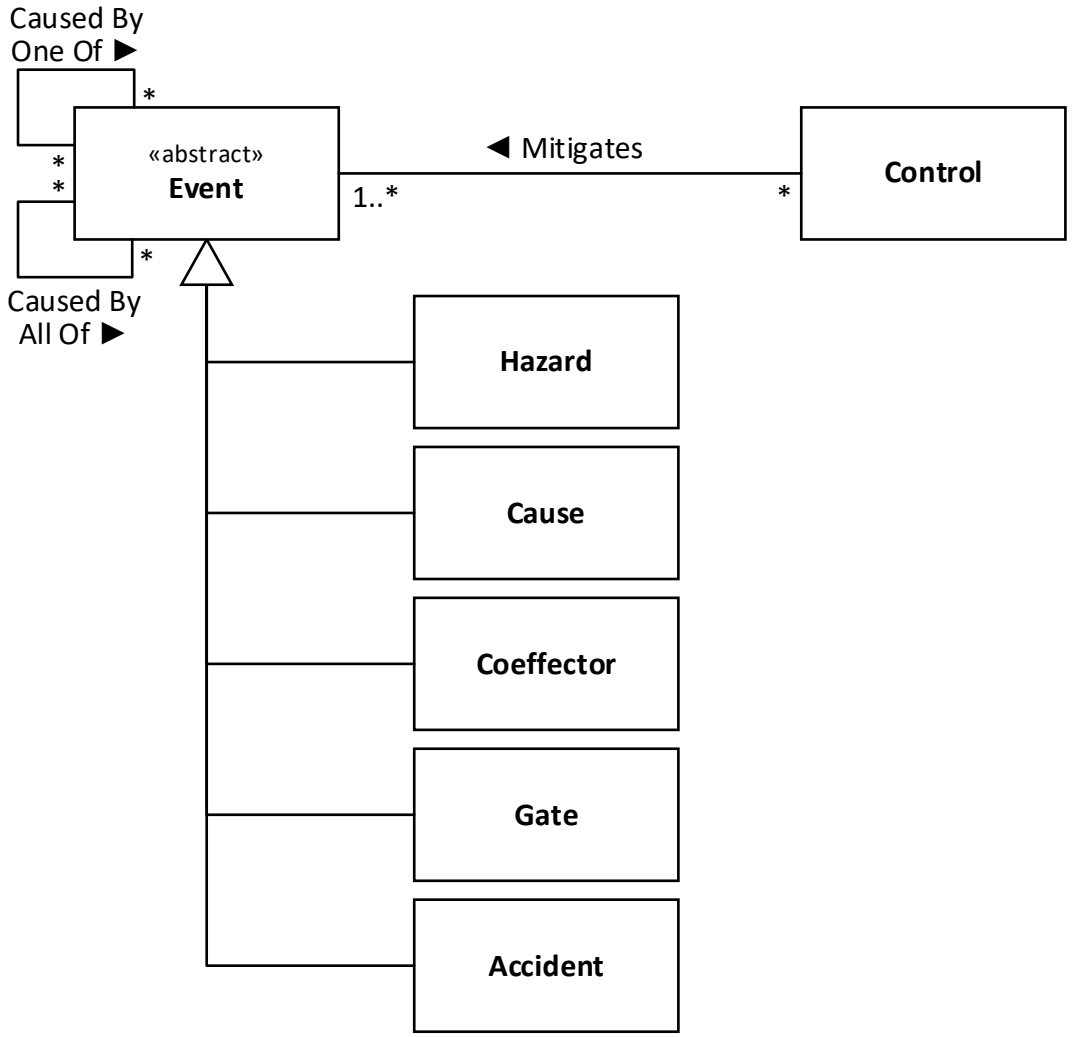
How can we estimate the effectiveness of each of these controls?

Control Effectiveness

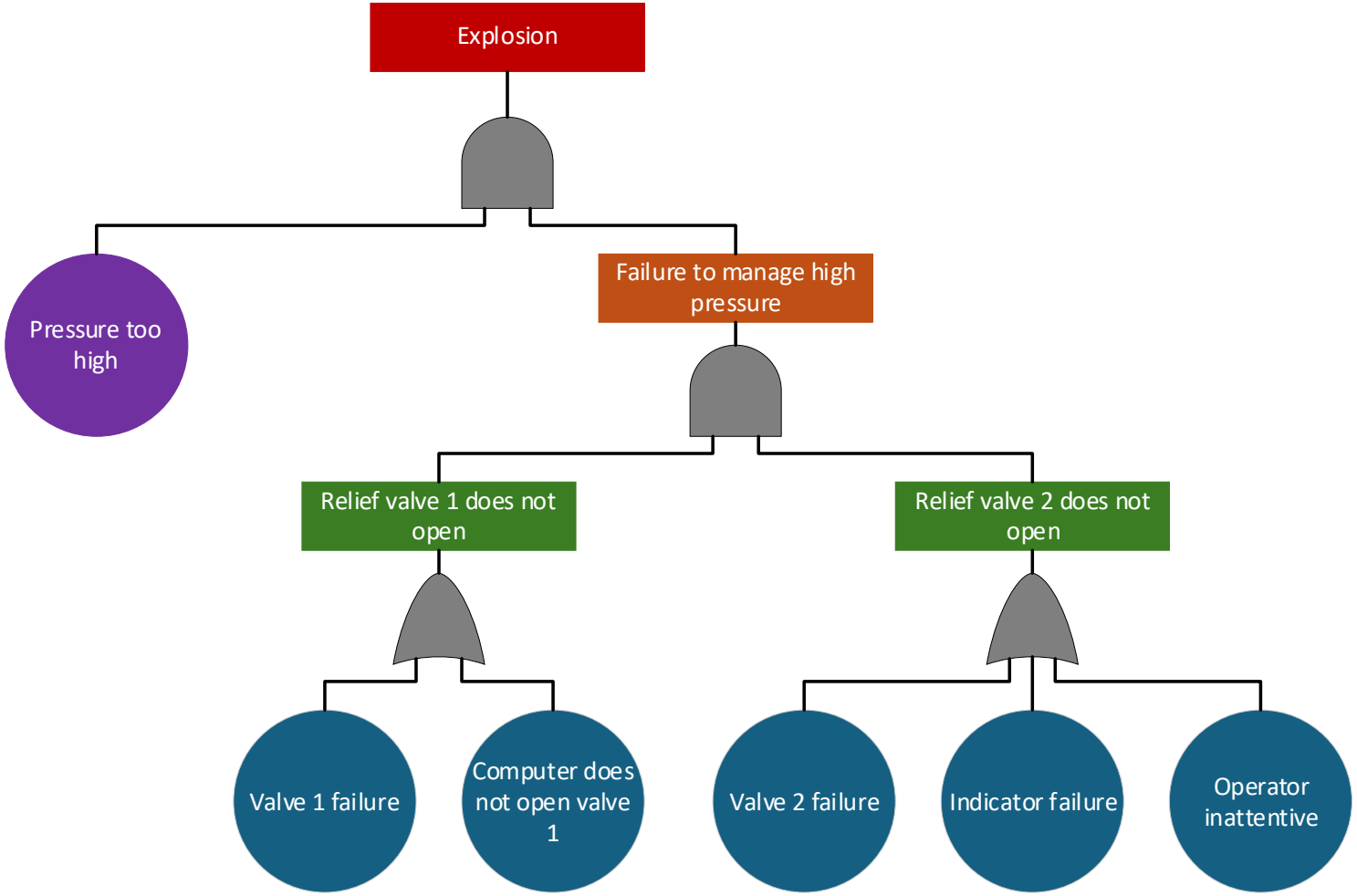
- How can we measure it?
  - A probability?
  - “T-shirt sizing”? – e.g., *Very Effective*, *Effective*, *Partially Effective*, *Ineffective*
- Effective relative to what?
  - Cause
  - Hazard
  - Accident
- Necessity vs sufficiency

A Structured Approach to Hazard Logs

- Hazard Log consists of two main types of objects:
  - Events
  - Controls
- Events
  - Include Hazards, Accidents, Causes, Coeffectors, and Gates
  - Have causal relationships
    - Caused by One Of / Caused by All Of
    - Sufficient to Cause / Necessary to Cause
- Controls
  - Associated with Events
- Although we show five event types here, this is just “convention”
  - The model supports multiple layers of hazards, where hazards at one level act as causes at a higher level
- Effectively equivalent to *fault trees*

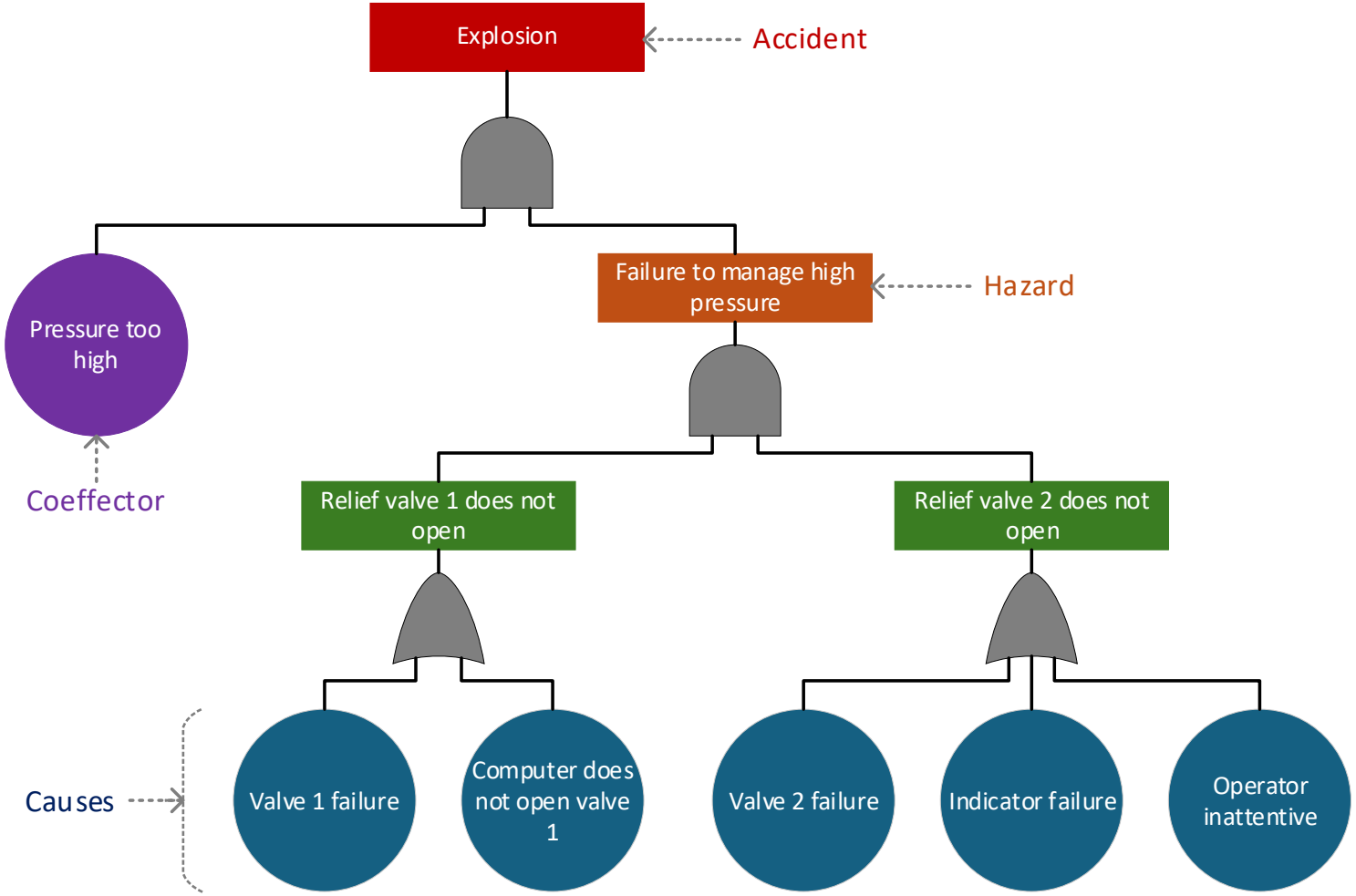


Example Hazard as a Fault Tree

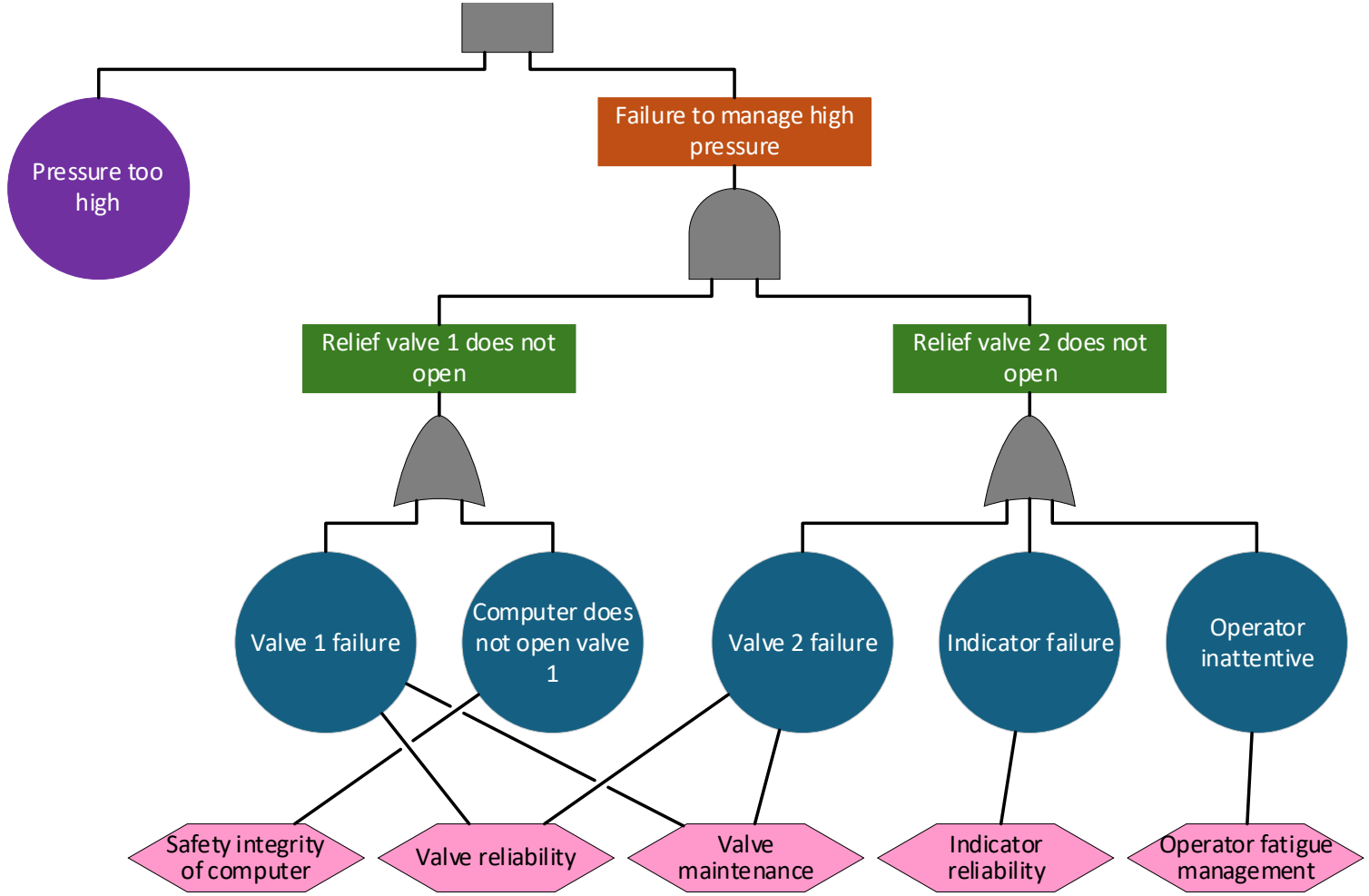


Adapted from Leveson (1995): *Safeware: system safety and computers*

Example Hazard as a Fault Tree



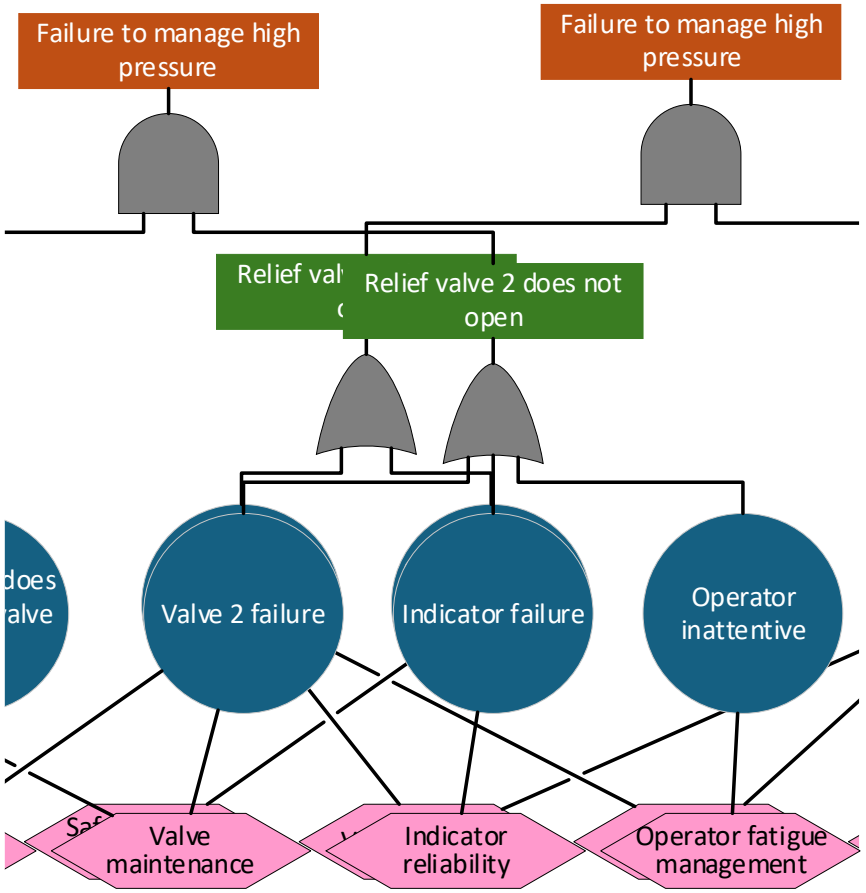
Example Hazard as a Fault Tree



Control Effectiveness – Take 2

- How effective is “Safety integrity of computer”…
  - … against “Computer does not open valve 1”?
    - Perhaps “*Very Effective*”
  - … against “Relief valve 1 does not open”?
    - ??? – only as good as controls against “Valve 1 failure”; depends on relative likelihood of causes
  - … against “Failure to manage high pressure”?
    - ??? – as above

- How effective is “Operator fatigue management”…
  - … against “Operator inattentive”?
    - Maybe only “*Partially Effective*”
  - … against “Relief valve 2 does not open”?
    - ??? – only as good as controls against “Valve 2 failure”, “Indicator failure”; depends on relative likelihood of causes
  - … against “Failure to manage high pressure”?
    - ??? – as above



Control Effectiveness – Take 2

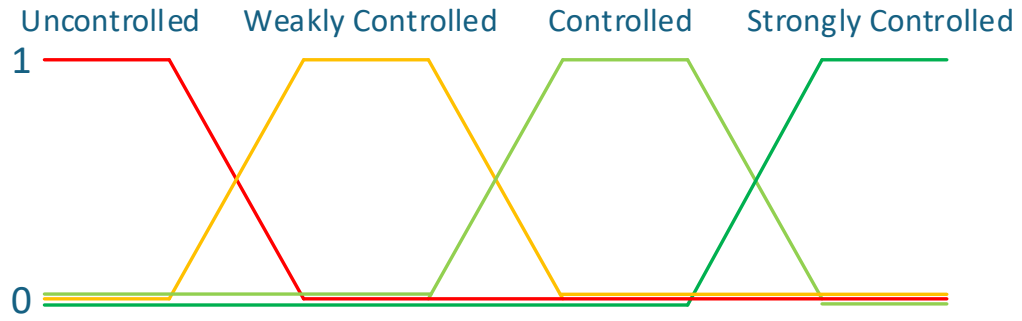
- It seems that we cannot really answer the question “how effective is this control?”
  - … except in the simplest of cases

- Instead we should ask…

How effectively controlled is this event?

Using Fuzzy Logic to Assess Control Coverage

- Fuzzy Logic enables “computing with words”, making deductions with inexact knowledge
- A Fuzzy Set is a class of objects with a continuum of grades of membership
  - E.g.: We could define a Fuzzy Set to represent control coverage:
    - *Strongly Controlled*, *Controlled*, *Weakly Controlled*, *Uncontrolled*
    - Work in terms of “degree of membership”

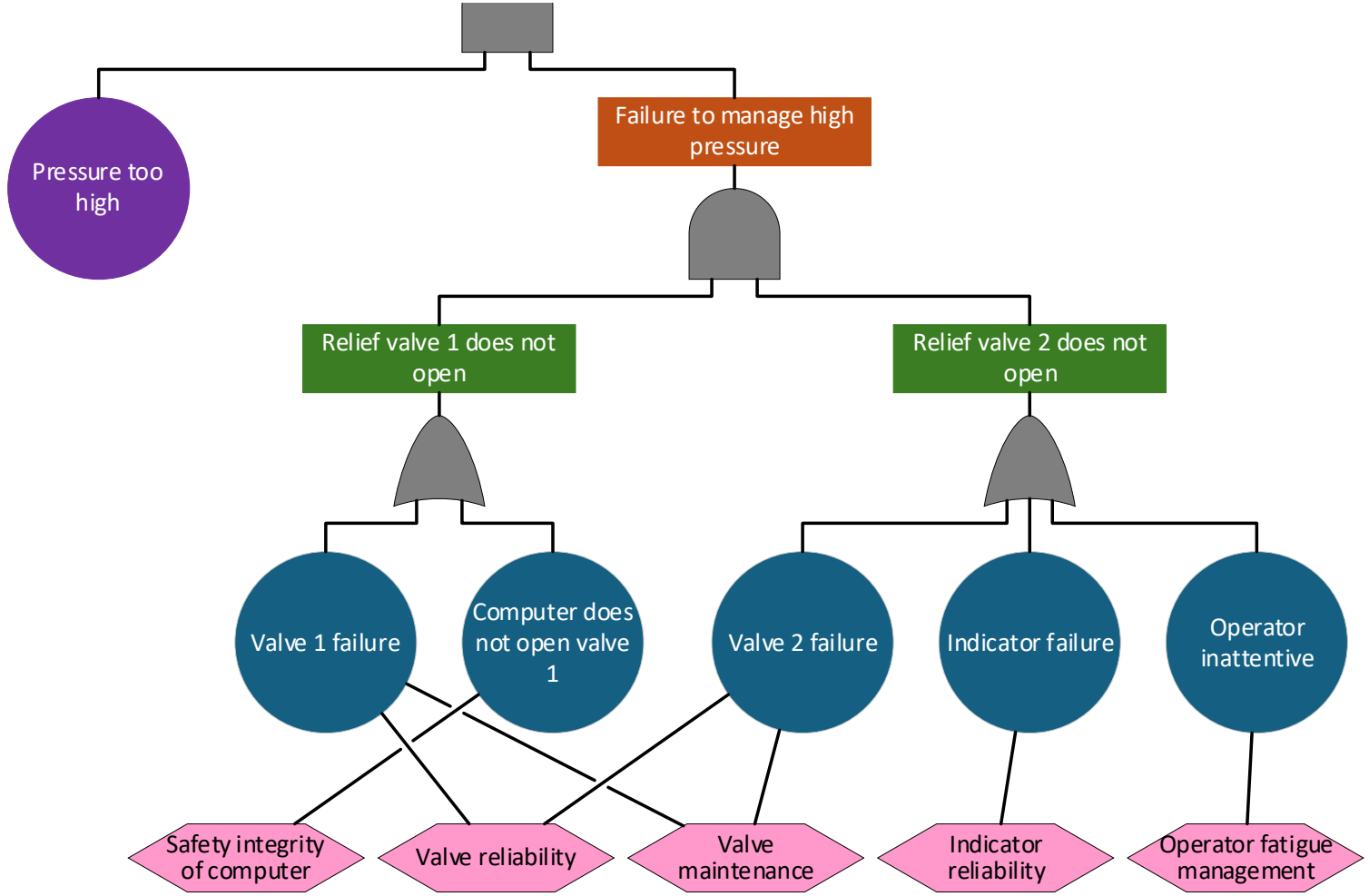


Using Fuzzy Logic to Assess Control Coverage

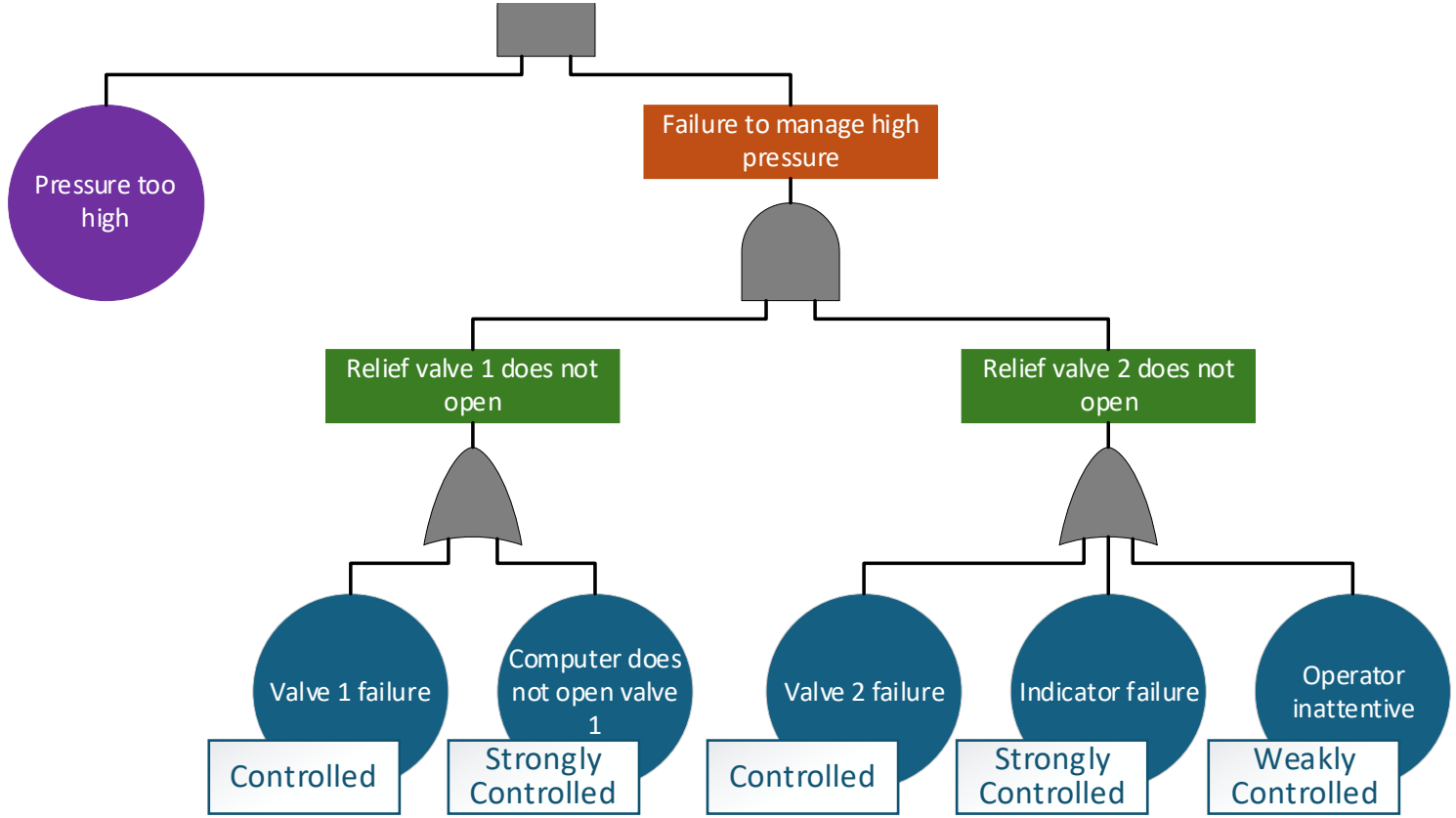
1. Evaluate how effectively each basic event is controlled
   - Use “T-shirt sizes” like *Strongly Controlled, Controlled, Weakly Controlled, Uncontrolled*
2. Propagate estimates “up” the tree, using fuzzy logic to evaluate each node
   - AND gate: Take the maximum measure from antecedent events
   - OR gate: Take the minimum measure from antecedent events

   - These are referred to as the “Zadeh operators”
     - (Actually… what is described here is dual to the Zadeh operators)

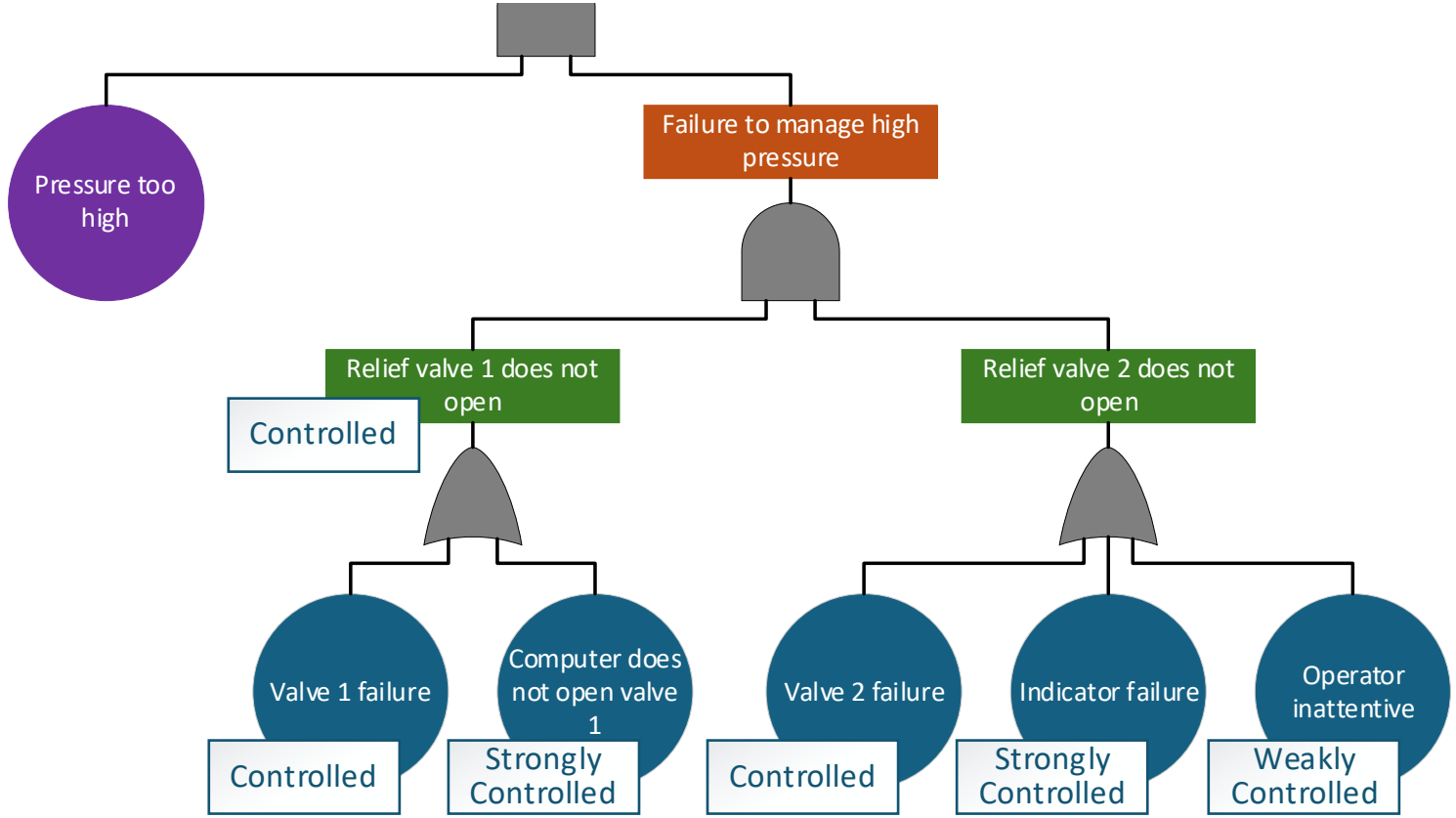
Using Fuzzy Logic to Assess Control Coverage



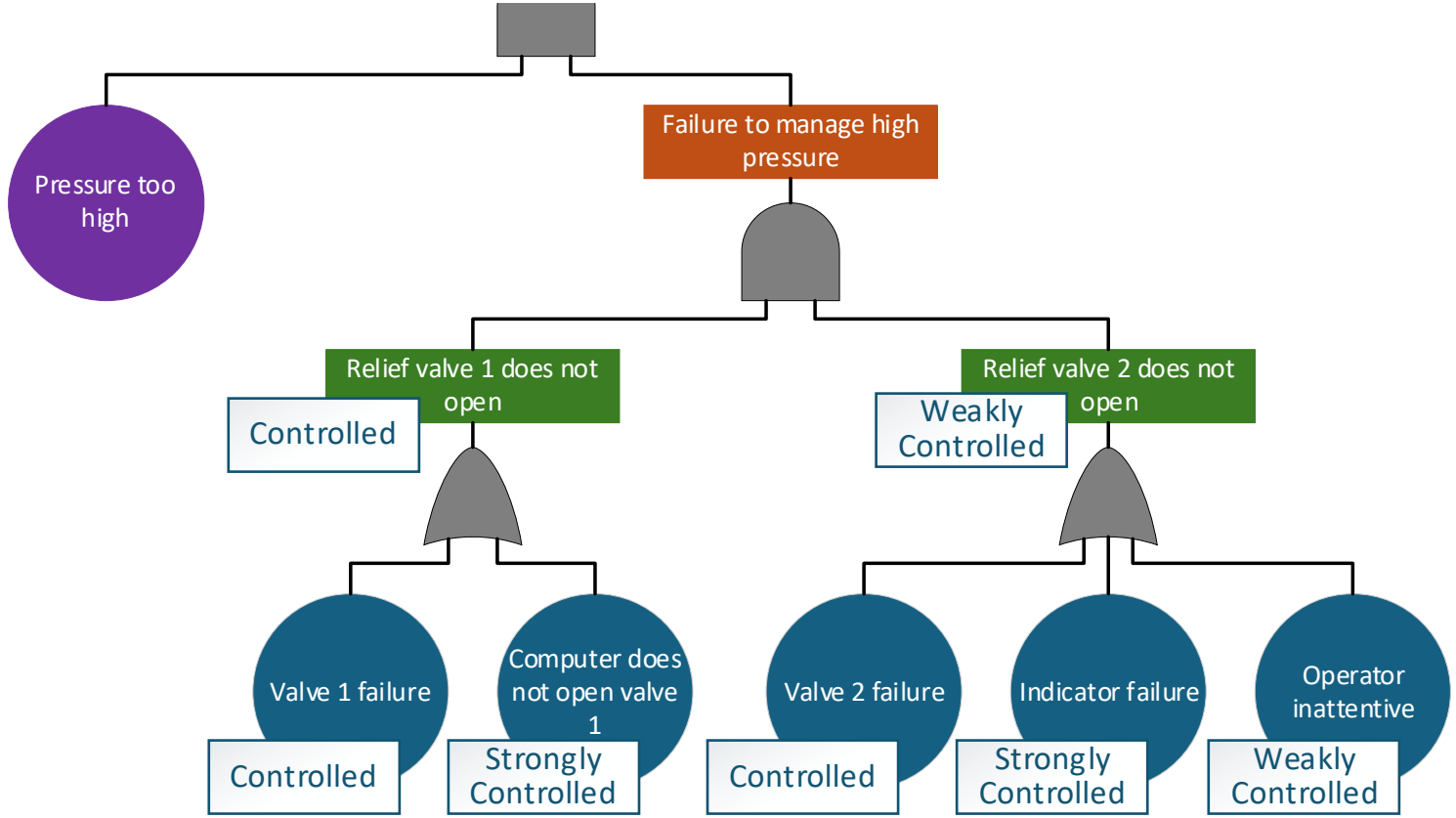
Using Fuzzy Logic to Assess Control Coverage



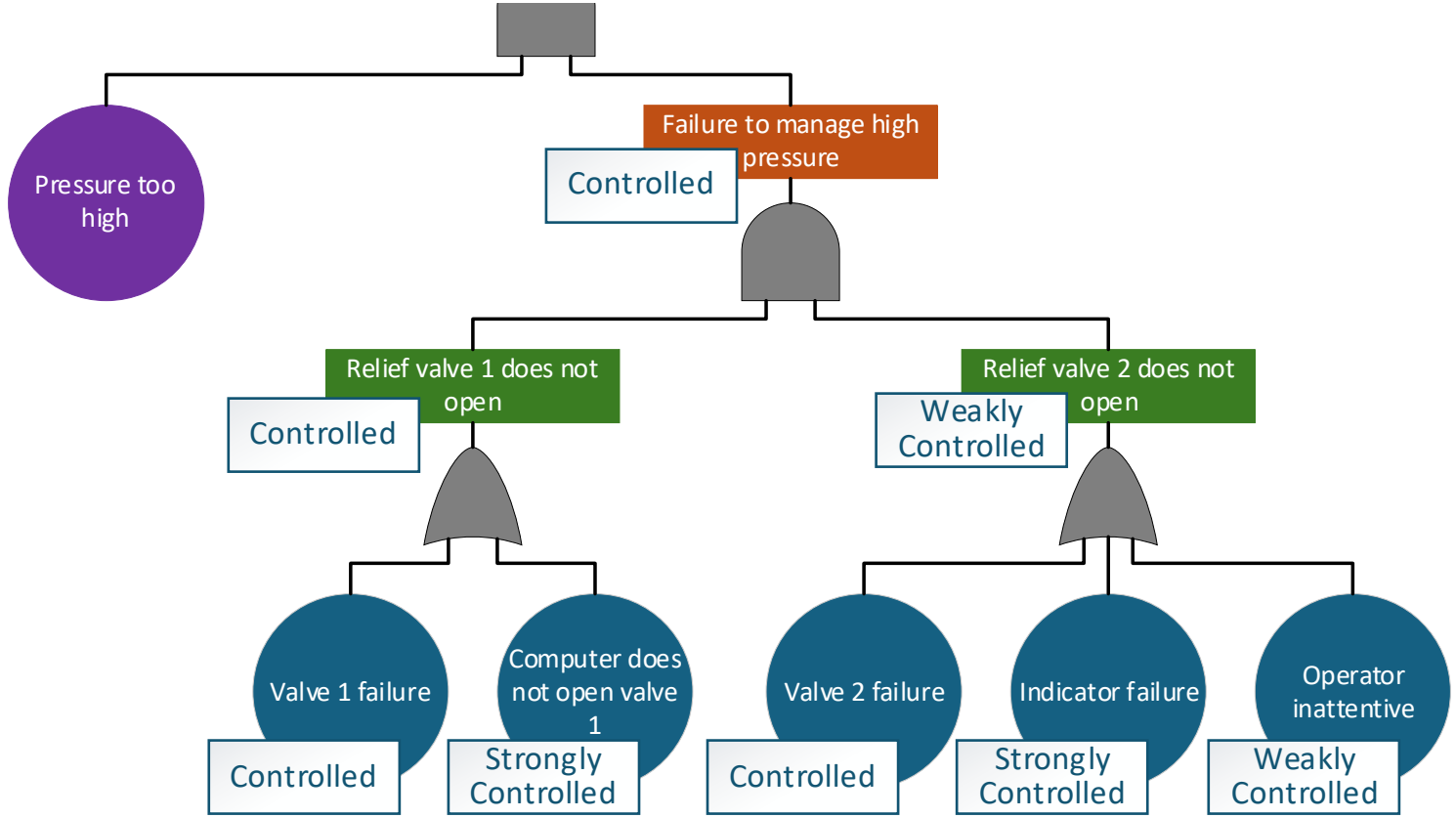
Using Fuzzy Logic to Assess Control Coverage



Using Fuzzy Logic to Assess Control Coverage



Using Fuzzy Logic to Assess Control Coverage



Using Fuzzy Logic to Assess Control Coverage

- Note: The measure applied to the hazard is not a measure of risk
  - But can inform the assessment of Residual Risk

- Can we do better?
  - There are alternatives to the Zadeh operators
  - However, these would require more information:
    - Relative likelihood of antecedents of OR gates
    - Propensity for common cause events among antecedents of AND gates
  - We would also need to much more carefully calibrate our Fuzzy Set

  - This would still be a lot easier than full quantification of fault trees

Further Thoughts

- This is a relatively simple method that can be applied to a Hazard Log
- … But it requires the Hazard Log to be suitably structured
  - The generic Hazard Log structure presented here has worked well on a variety of projects
- The structured approach to Hazard Logs has many other benefits
  - Well-suited to “systems-of-systems”
  - Amenable to quantification of risk
- We believe that storing such structure *in* the Hazard Log itself is important
  - Different “views” of Hazard Log information can be developed if needed
  - E.g., We have developed software to transform this structure into bow-tie diagrams
- When in the project lifecycle should this structure be developed?
  - We view this as part of the transition from *Preliminary Hazard Analysis* to *System Hazard Analysis*
  - It is hard to apply this sort of structure “after the fact”
- The process of reasoning about control coverage is perhaps as valuable as the outcome

Conclusions

- Reasoning about control effectiveness is not as simple as labelling controls “Effective”, “Partially Effective”, etc.
- Better to ask “How well controlled is this hazard (or event)?”
- Symbolic/semi-quantitative approaches to systematically answering this question are possible
  - One such method, based on Fuzzy Logic, was presented
  - It requires hazards be suitably structured
- Simple and general approach to structured Hazard Logs
  - We have used this approach successfully on a number of projects
  - We plan to continue developing (software-supported) methods of viewing and reasoning about the contents of such Hazard Logs