Emerging Health & Safety Issues from Changing Workplaces
– A Canadian Discussion –

Emerging Technologies and Processes

Presented by

Catherine Burns

Associate Professor
Systems Design Engineering, University of Waterloo

Waterloo ON Canada

Challenges as Complexity Grows

- Harder to find the problem
- Problems interact
- Solutions are less clear
- Proving a solution works becomes very difficult

Catherine Burns
c4burns@uwaterloo.ca

Anticipate your failure points

Catherine Burns
c4burns@uwaterloo.ca

A Story

In the morning you wake up late because your alarm clock volume was too low (you didn't hear it). You managed to still get the kids to the bus when you get back and you realize you forgot a form they needed for the upcoming school trip. You drop it off before work and are a few minutes late getting into work. Unfortunately your boss had scheduled a meeting at the start of the day. You normally would have been in in time to read your email and make the meeting, but instead you walk into the meeting late. The meeting doesn't go well.

Adapted from Perrow's "Normal Accidents", 1999.

Catherine Burns
c4burns@uwaterloo.ca

The meeting didn't go well because…

The failure of your alarm clock, or the fact the radio station wasn't broadcasting the signal as loud as the night before

Your human error in setting the volume too low

Your procedures and practices such as not packing all the kids' stuff the night before

The procedures and practices of the school in requiring too many forms

External factors in the environment such as your manager calling the meeting without enough notice

The poor design of your alarm clock which didn't catch your error

Catherine Burns
c4burns@uwaterloo.ca

Three Mile Island

Babcock and Wilcox (builders of the equipment) blamed the operators - human error.

Metropolitan Edison (the utility) blamed the equipment - mechanical failure.

The NRC (Nuclear Regulatory Commission) blamed the design of the system.

The operators blamed the procedures.

The president's commission blamed everyone.

Catherine Burns
c4burns@uwaterloo.ca

Challenges as Complexity Grows

- Harder to find the problem
- Problems interact
- Solutions are less clear
- Proving a solution works becomes very difficult

Catherine Burns
c4burns@uwaterloo.ca

Finding the Problem: Accidents Happen Because…

- Systems fail in unexpected ways.
- Failed parts can’t be isolated.
- Parts have complex interactions that can’t be anticipated.

Catherine Burns
c4burns@uwaterloo.ca

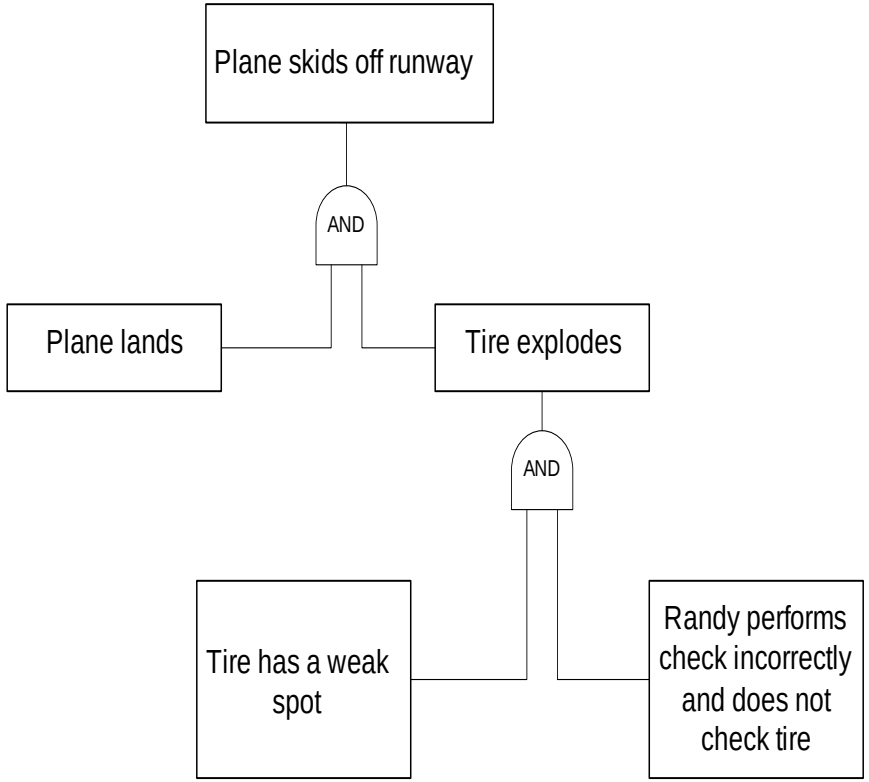
Anticipating Problems

- Failure prediction approaches
  - Failure Modes and Effects Criticality Analysis
  - Fault Tree Analysis
- Try to find weak spots before they occur
- Analyze problems after they happened

Catherine Burns
c4burns@uwaterloo.ca

Example

Randy who was tired was preparing the plane for take-off when he forgot to check the condition of the tires on the landing gear. On landing, one of the tires punctured, sending the plane skidding off the runway. The tire showed a weak spot in the sidewall when analyzed after the accident.



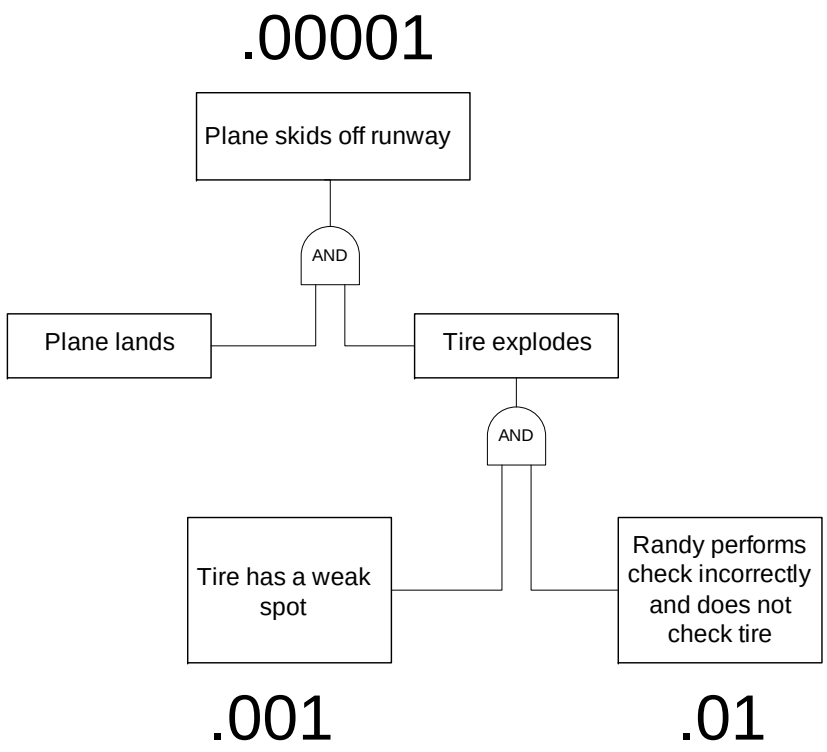
Catherine Burns
c4burns@uwaterloo.ca

FTA

Observation: 1 in 100 times pilots fail to check the tires

Manufacturer: 1 in 1000 times the tire has a weak spot

This accident: can occur in 1 of 100 000 flights



Catherine Burns
c4burns@uwaterloo.ca

FMECA

- Thoroughly step through the process
- Anticipate all possible failures at each step
- Prioritize to capture the most frequent or severe failures
- Strategy for process and system improvement

Catherine Burns
c4burns@uwaterloo.ca

Alarm Clock Failures

- Not set
- Set but for pm not am
- Set but radio volume is too low
- Set but not on a radio frequency
- Set but not on a strong enough radio frequency
- Set but power failure occurs that resets time
- Set but user turns off when it goes off
- Set but user uses snooze button too many times

Catherine Burns
c4burns@uwaterloo.ca

Why It Works

A systematic thorough process reveals future failures you would not otherwise see.

Catherine Burns
c4burns@uwaterloo.ca

Strategy 1

Anticipate your failure points.

Catherine Burns
c4burns@uwaterloo.ca

Reduce the complexity.

Catherine Burns
c4burns@uwaterloo.ca

Why Complexity Causes Accidents

Events become accidents when:

- they go unnoticed
- the system is tightly coupled and the event causes other events
- the system is complex

The more complex the system is and the more tightly coupled the system is, the more sensitive it is to events.

Catherine Burns
c4burns@uwaterloo.ca

In Complex Systems

- Interactions and interconnections make it hard for a user to understand all the connections and to foresee the consequences of an action
- Processes are time dependent, one event causes another somewhere else, processes may be uninterruptable
- In high gain complex systems, small failures cause big problems

Catherine Burns
c4burns@uwaterloo.ca

Why Systems Are Complex

- Design
- Design for efficiency
- Design with automation
- Design with safety systems

There are lots of “good” reasons why we build complex systems.

Catherine Burns
c4burns@uwaterloo.ca

How Systems Become More Complex

Systems become more complex over time due to:

- failure
- ageing
- maintenance
- redesign
- retrofits

Systems become more complex as accidents occur.

Catherine Burns
c4burns@uwaterloo.ca

Recognizing When a System is Complex

- more time dependent processes
- invariant sequences (X must come before Y)
- the process only works in one way (no alternative paths)
- little slack, require precise quantities and timing
- High gain: a small event can cause a big reaction

Catherine Burns
c4burns@uwaterloo.ca

High Gain

Virginia Electric Power, 1980

While a worker was cleaning the floor in an auxiliary building, his shirt caught on a 3 inch handle of a circuit breaker. Pulling it free he activated the breaker, which shut off current to the control rods in the reactor. The reactor shut down automatically and it took 4 days to bring it up again, costing hundreds of thousands of dollars

Small failure = BIG PROBLEM

Catherine Burns
c4burns@uwaterloo.ca

Changing a light bulb in California, 1978

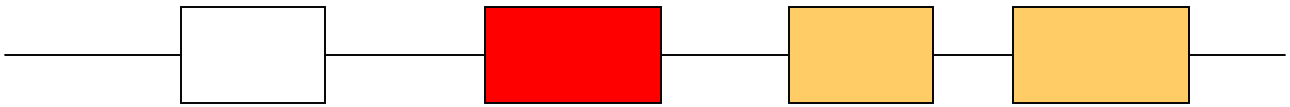
A worker changing a light bulb on a control panel in the control room dropped the bulb. The dropped bulb created a short circuit in some sensors and controls. The reactor automatically shut down. The loss of the sensors meant the operators could not monitor the plant. The shutdown caused the core to cool too rapidly. The operators came very close to cracking the reactor vessel and causing a major meltdown.

Small failure = BIG PROBLEM

Catherine Burns
c4burns@uwaterloo.ca

Understanding Complexity

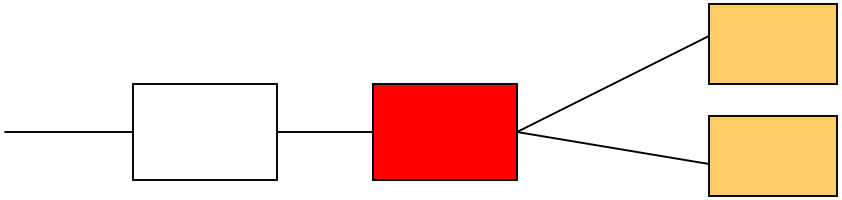
Linear interactions: a process is carried out in a sequence of steps. One failure affects the entire system “downstream”.



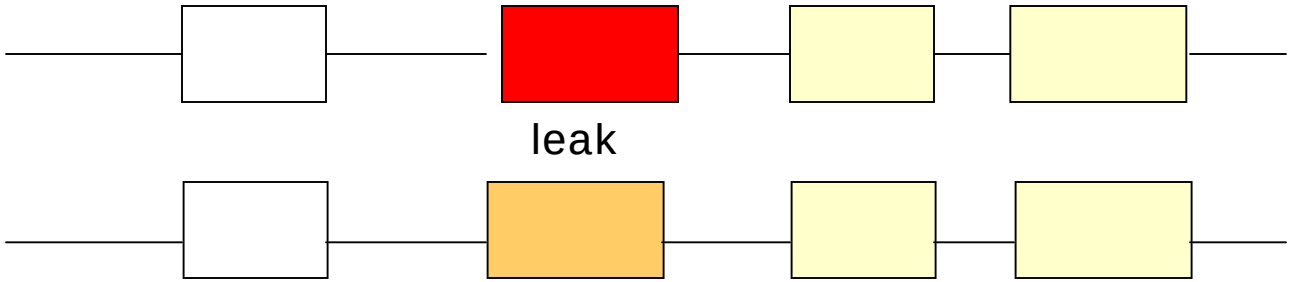
Catherine Burns
c4burns@uwaterloo.ca

Complex Nonlinear Interactions:

Common mode interaction: One component services two or more parts. Common mode failure.



Proximity interaction: two components that don't normally interact, interact solely because of location



Catherine Burns
c4burns@uwaterloo.ca

- Most systems are highly linear (>99%)
- Systems with only 90% linear interactions and 10% complex nonlinear interactions are at a significantly higher risk of accidents

Catherine Burns
c4burns@uwaterloo.ca

Recognizing (more) Linear Systems

- Spatially spread out to reduce proximity interactions
  - Units that are not part of the same process are not housed in the same building
- People have less specialized jobs and can take over each other's positions
- Materials do not have to meet stringent specs and can be substituted
- Feedback loops are local
- Control is decentralized

Catherine Burns
c4burns@uwaterloo.ca

Complex Systems

- House parts from different subsystems in the same building or location
- Have common mode connections between parts that are not in the same production sequence
- Employees are specialized, highly trained, and can not easily switch to other roles
- Materials are specific and stringently monitored
- Feedback loops are global
- Control is centralized

Catherine Burns
c4burns@uwaterloo.ca

2003 Power Grid Failure Events

Context: August afternoon, moderate loads due to air conditioning, 2 units down

1:31 another unit goes down, loads are high

3:05 another line goes down (buffer was now gone)

2:14-3:59 computer failures in the FE control room (loss of situation awareness)

3:15-3:39 3 more lines go down due to tree contact

3:39-3:58 7 more lines trip due to overloading

4:05-4:08 4 major lines trip due to overloading cascading across eastern North America

Catherine Burns
c4burns@uwaterloo.ca

Power Grid Failure

- Linear interaction: 1 minor line trips and then a connected major line trips
- Common mode interaction: 1 major line trips and cascades to 2 or more minor lines
- Proximity interaction: tree branch hits wire
- Tight coupling:
  - Events couldn't be stopped
  - Events cascaded causing other events
  - Events happened very quickly

Catherine Burns
c4burns@uwaterloo.ca

2003 Power Grid Failure Events

Context: August afternoon, moderate loads due to air conditioning, 2 units down

1:31 another unit goes down, loads are high

3:05 another line goes down (buffer was now gone)

2:14-3:59 **computer failures** in the FE control room (loss of situation awareness)

3:15-3:39 3 more lines go down due to tree contact

3:39-3:58 7 more lines trip due to overloading

4:05-4:08 4 major lines trip due to overloading cascading across eastern North America

The system is becoming more complex as the accident is evolving!

Catherine Burns
c4burns@uwaterloo.ca

Peanut Butter

Company says moisture in peanut butter plant spread salmonella bacteria - Apr. 05, 2007

Provided by: Canadian Press
Written by: JOSH FUNK

OMAHA, Neb. (AP) - ConAgra Foods said Thursday that moisture from a leaky roof and faulty sprinkler was the source of the salmonella bacteria that contaminated peanut butter at its Georgia plant last year, sickening more than 400 people nationwide.

The Omaha-based company conducted a nearly two-month investigation into the contamination and pledged to ensure that Peter Pan peanut butter is safe when it returns to stores in mid-July.

Catherine Burns
c4burns@uwaterloo.ca

How It Happened

- Childs said the company traced the salmonella outbreak to three problems at its Sylvester, Ga., plant last August.
- The plant's roof leaked during a rainstorm, and the sprinkler system went off twice because of a faulty sprinkler, which was repaired.
- The moisture from those three events mixed with dormant salmonella bacteria in the plant that Childs said likely came from raw peanuts and peanut dust.

Catherine Burns
c4burns@uwaterloo.ca

The Result

ConAgra recalled all its peanut butter in February after U.S. health officials linked it to cases of salmonella infection. At least 425 people in 44 states were sickened, and numerous lawsuits have been filed against the company.

Peanuts grow underground and salmonella is present in the dirt, but generally any bacteria are killed when raw peanuts are roasted.

Catherine Burns
c4burns@uwaterloo.ca

Solution

Experts had speculated that salmonella would be most likely to contaminate the peanut butter as it cools and is placed in jars. At most plants, those steps take just minutes.

The company plans to redesign the plant to provide greater separation between raw peanuts and the finished product, Childs said. The plant will also receive a new roof.

ConAgra plans to reopen the plant in early August.

Catherine Burns
c4burns@uwaterloo.ca

Why It Works

Separating the process reduces the complexity.

Catherine Burns
c4burns@uwaterloo.ca

Strategy 2

Reduce the complexity

Catherine Burns
c4burns@uwaterloo.ca

Build in a margin of safety

Catherine Burns
c4burns@uwaterloo.ca

Working with the Human Factor

- People make errors
- People misjudge risk and probability
- People take short term benefits over longer term benefits
- People monitor less vigilantly over time
- People over-trust and under-trust automation

Catherine Burns
c4burns@uwaterloo.ca

A “Margin of Safety” for the Human Factor

- Design within and away from the limits of:
  - human perception
  - human attention
  - human physical abilities
- Design and assume people work under:
  - stress
  - workload/fatigue

Catherine Burns
c4burns@uwaterloo.ca

A Story

In the morning you wake up late because your alarm clock volume was too low (you didn't hear it). You managed to still get the kids to the bus when you get back and you realize you forgot a form they needed for the upcoming school trip. You drop it off before work and are a few minutes late getting into work. Unfortunately your boss had scheduled a meeting at the start of the day. You normally would have been in in time to read your email and make the meeting, but instead you walk into the meeting late. The meeting doesn't go well.

Adapted from Perrow's "Normal Accidents", 1999.

Catherine Burns
c4burns@uwaterloo.ca

Margins of Safety Would…

- Set the alarm clock earlier
- Set a second clock or warning system
- Set volume extra high
- Pack the form the night before

Catherine Burns
c4burns@uwaterloo.ca

Everyday…

We all use margins of safety everyday when we:

- leave a little early
- make sure the gas tank is full
- do it now rather than late
- buy a little extra for the party
- talk to a colleague about what's coming up in their work area

Catherine Burns
c4burns@uwaterloo.ca

In Work

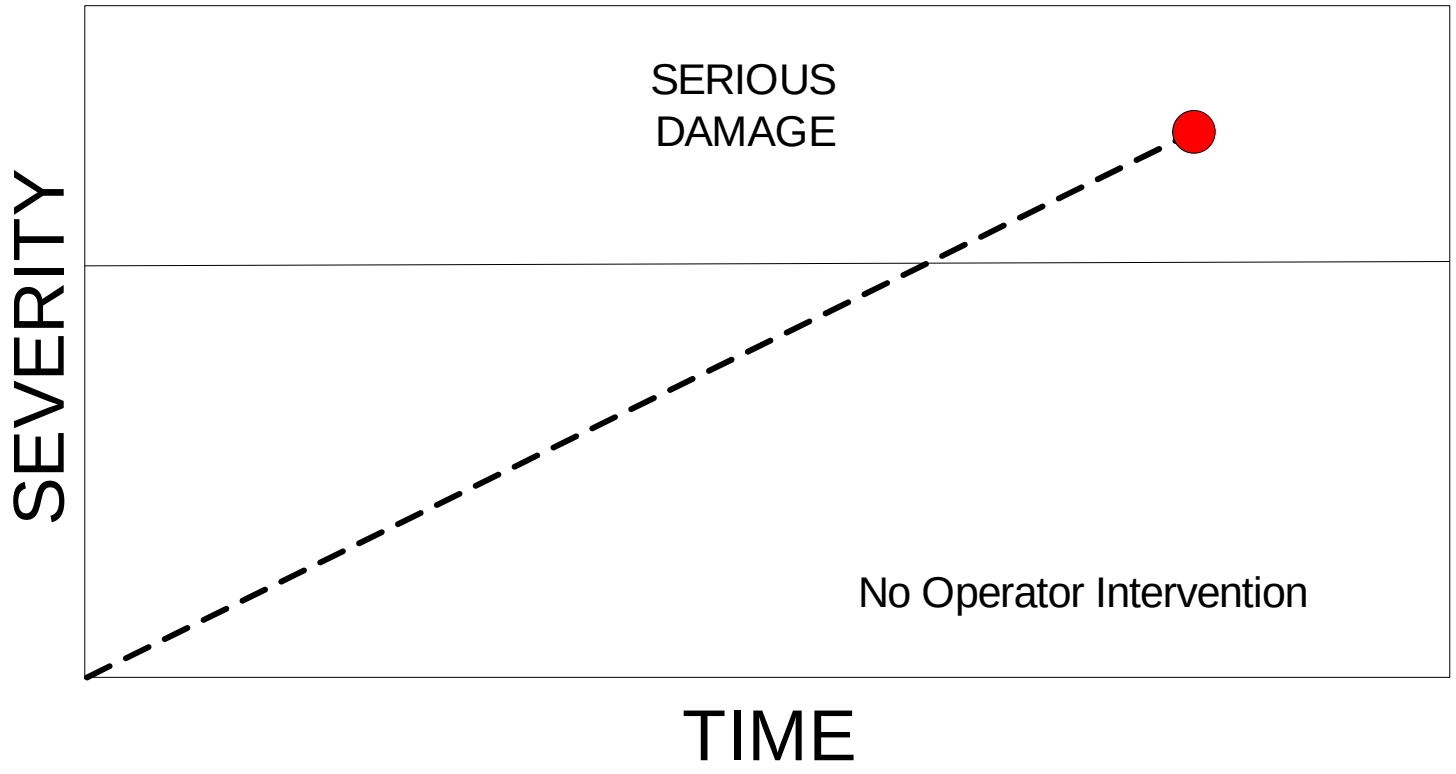
Help people see ahead

Give them a little extra time

Have some spare capacity

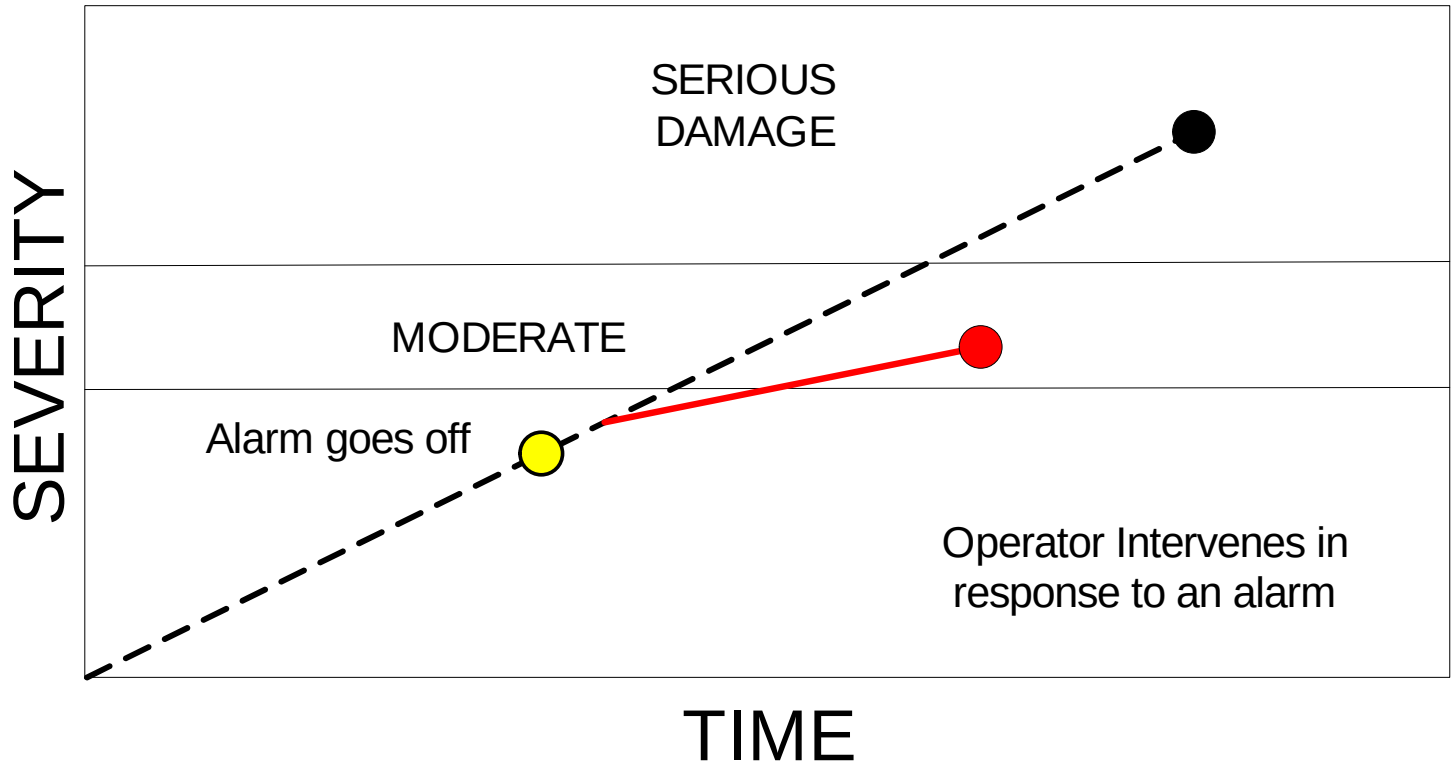
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



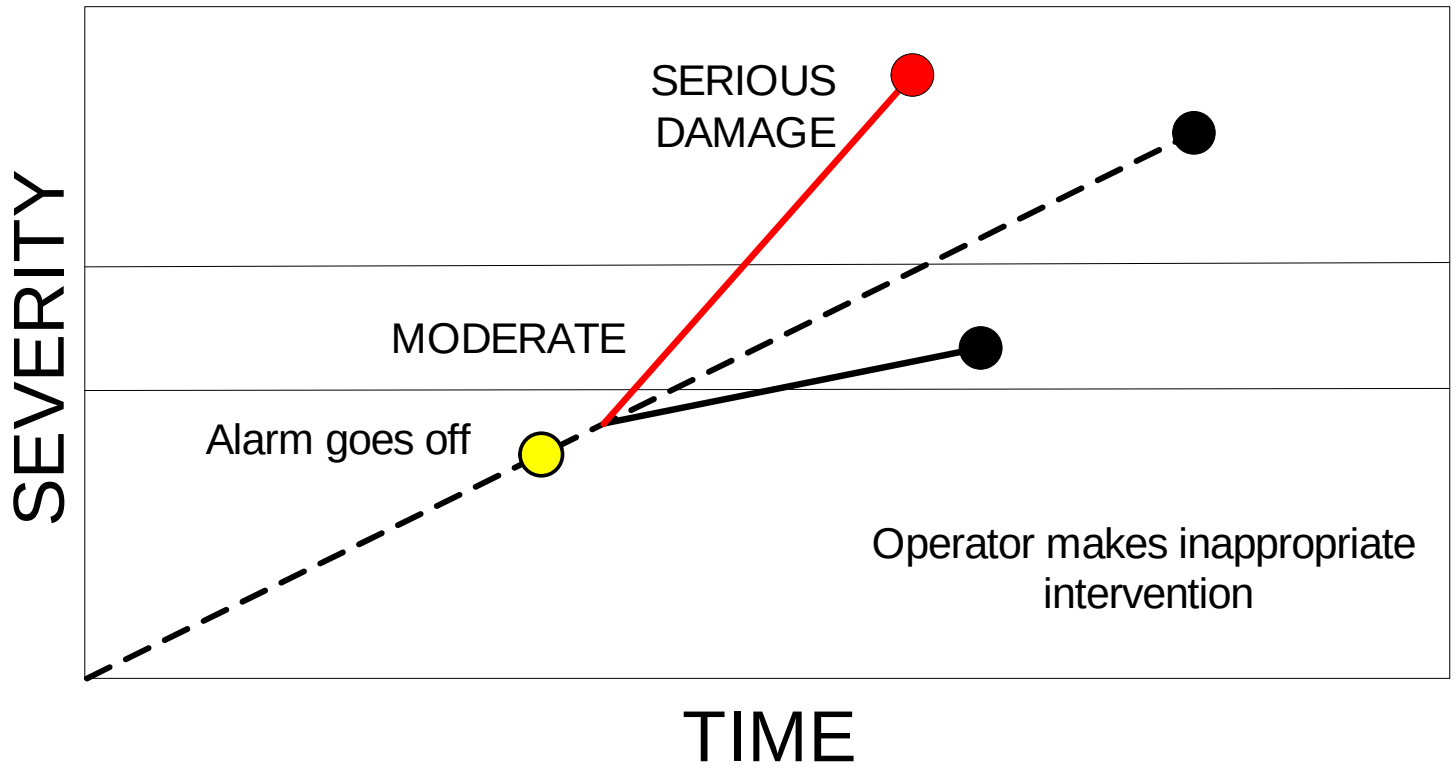
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



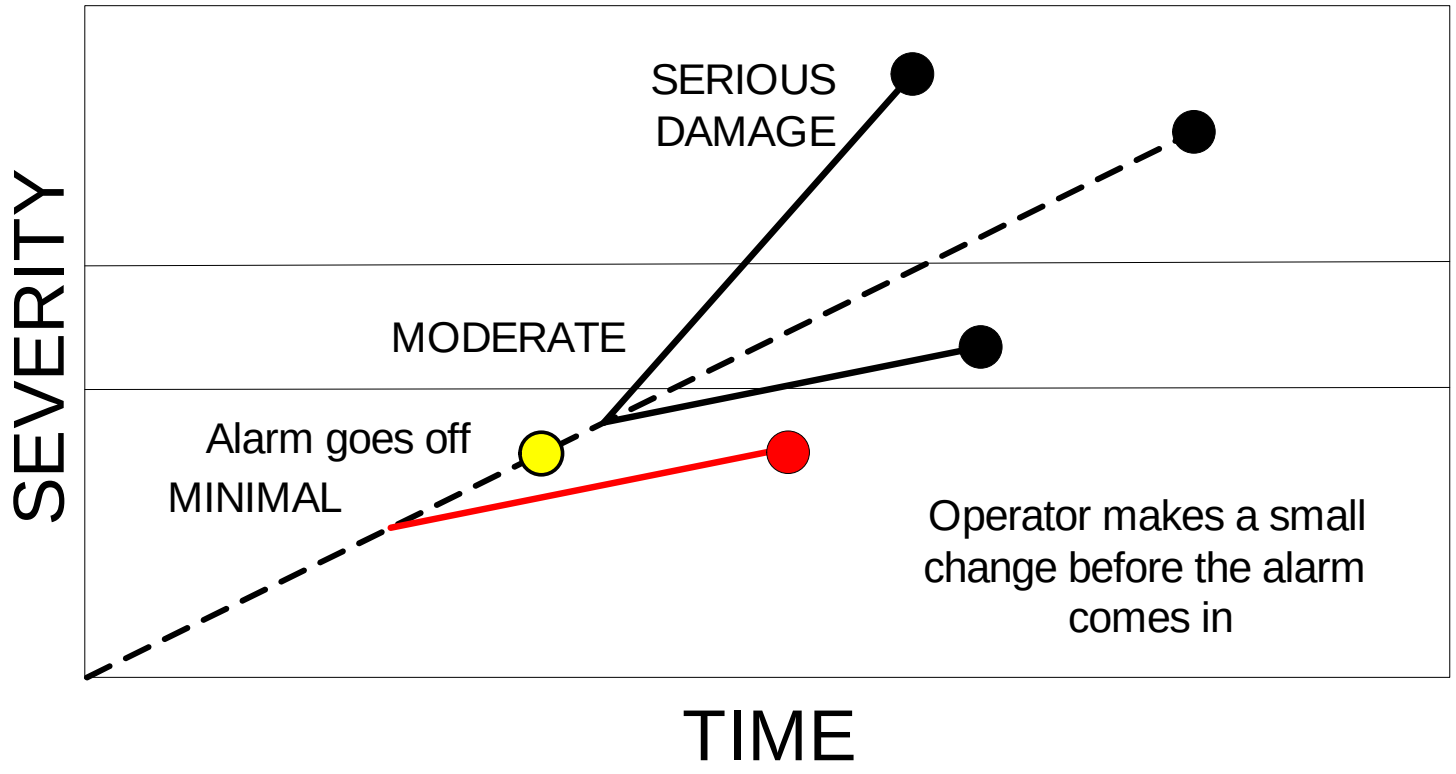
Emerging Technologies and Processes
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



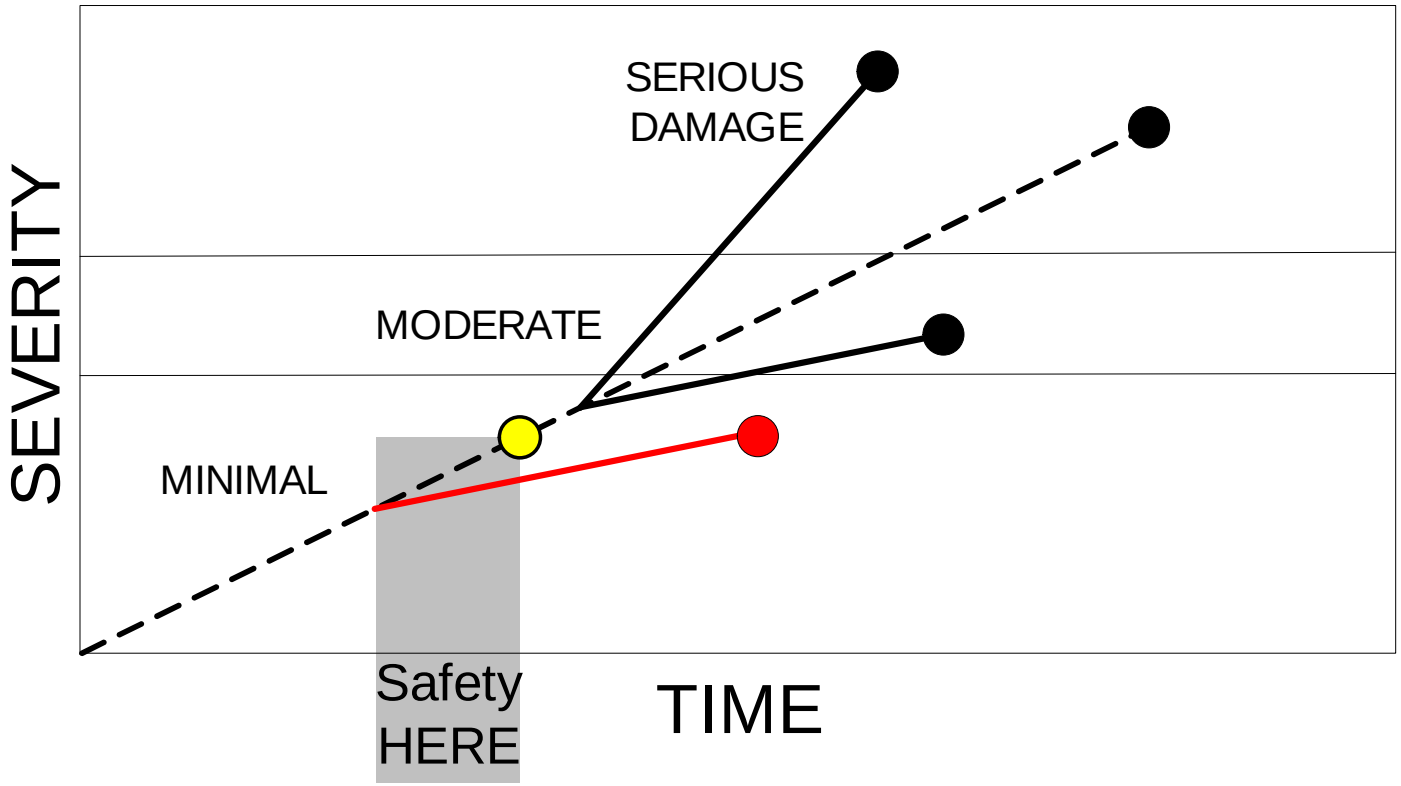
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



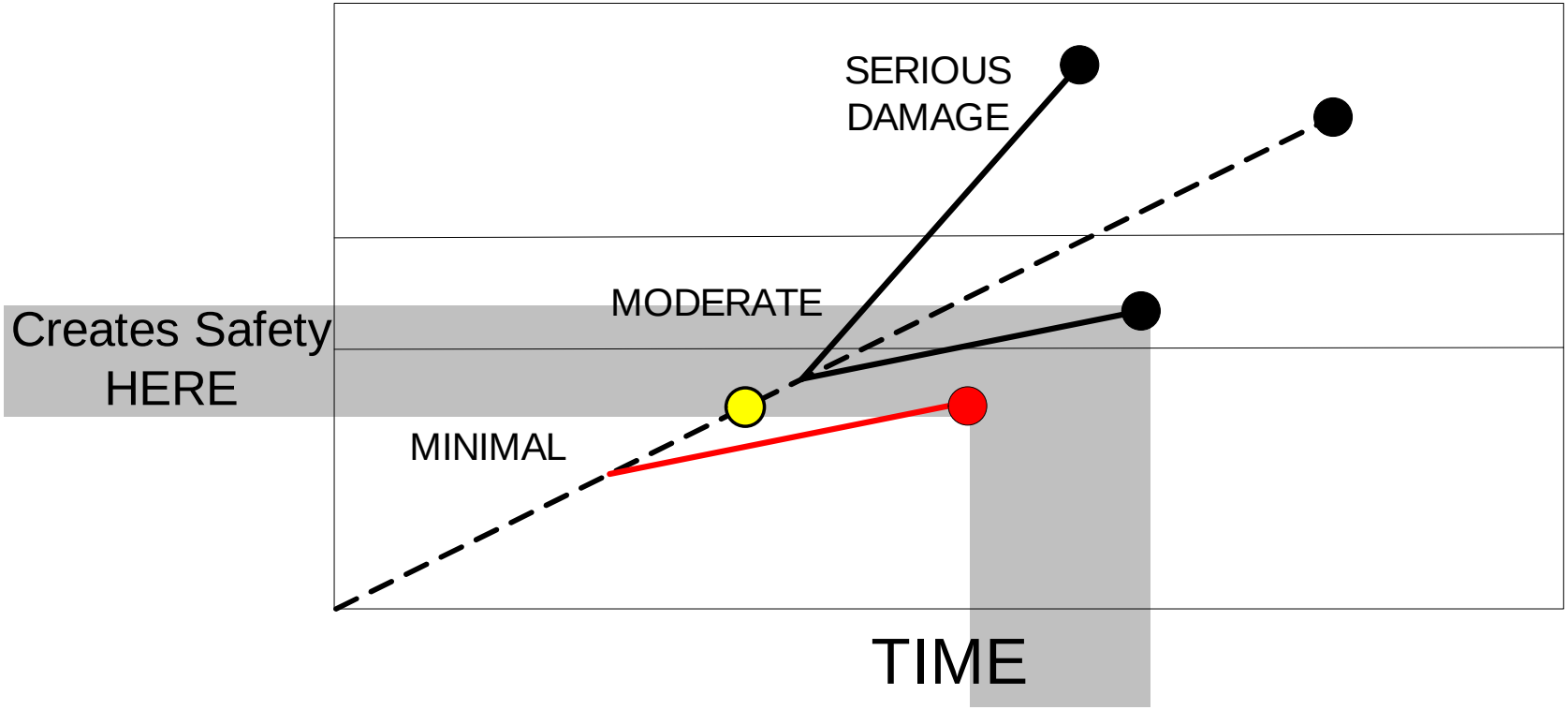
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



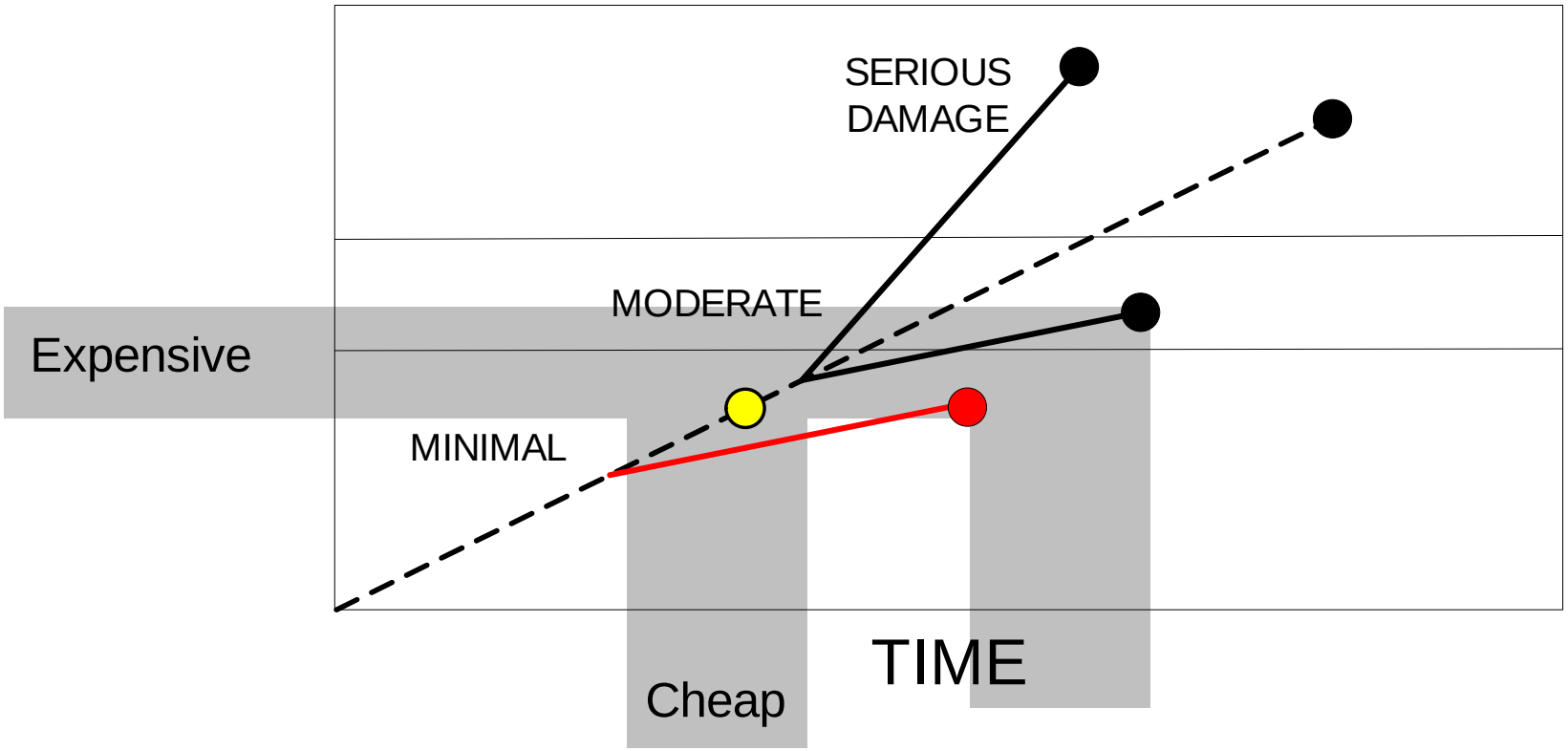
Emerging Technologies and Processes
Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



Catherine Burns
c4burns@uwaterloo.ca

Being Proactive Fights Complexity



Catherine Burns
c4burns@uwaterloo.ca

Helping People See Ahead

1. Improve their vision of the situation
    - Design better displays

2. Reduce the noise that clouds the situation
    - Advanced alarm management techniques

Catherine Burns
c4burns@uwaterloo.ca

Air France Overrun

- Thunderstorms, surface winds, 2 flights before reported poor braking conditions (passed from ATC to the plane)
- Crew changed brakes from low to medium
- Alignment ok, speed ok, crew followed procedures fine
- Aircraft drifted up off glide path (100 ft vs 50 ft), speed increased
- Heavy showers reduced visibility
- Wind direction changed to tailwind and runway had ¼ inch of standing water on it in seconds
- Landed at 4000 ft on 9000 ft runway

Catherine Burns
c4burns@uwaterloo.ca

ACTUAL LANDING DISTANCE (from 50 feet above ground to complete stop)						
Runway Conditions	Dry		Wet		6.3 mm (1/4 inch) of water	
	metres	feet	metres	feet	metres	feet
No wind	1155	3788	1502	4927	1987	6519
5-knot tailwind	1264	4148	1682	5518	2265	7432
No wind, reversers operative	1155	3788	1397	4582	1768	5802
5-knot tailwind, reversers operative	1264	4148	1564	5132	2016	6614

Tailwind plus ¼ inch of water = 6614 ft to stop the plane

They had 5000 ft.

Catherine Burns
c4burns@uwaterloo.ca

Proper display design

- Would tell the crew the amount of runway length left
- Would tell the crew the expected stopping distance required
- Would tell the crew the plane could not land

Catherine Burns
c4burns@uwaterloo.ca

Situation Awareness

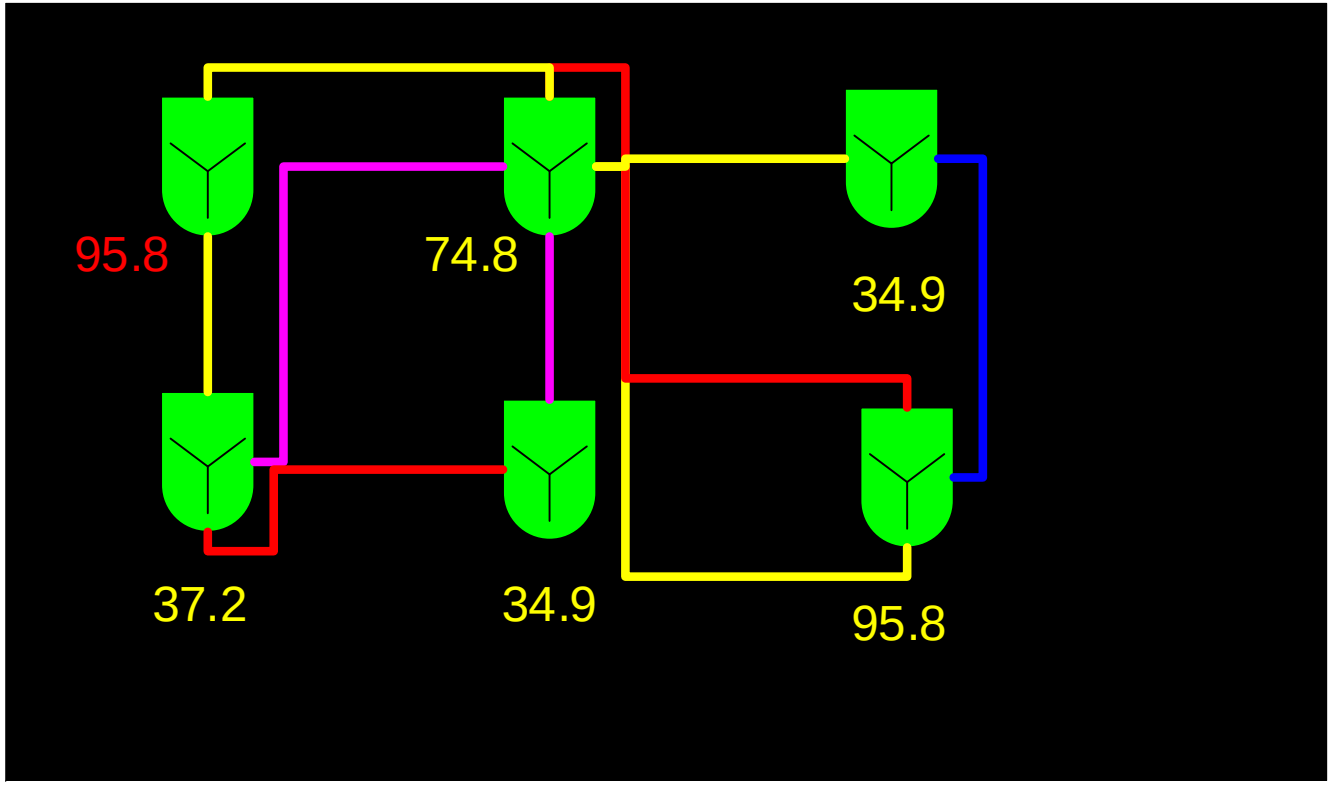
Improve Perception: Would tell the crew the amount of runway length left

Improve Understanding: Would tell the crew the expected stopping distance required

Improve Prediction: Would tell the crew the plane could not land

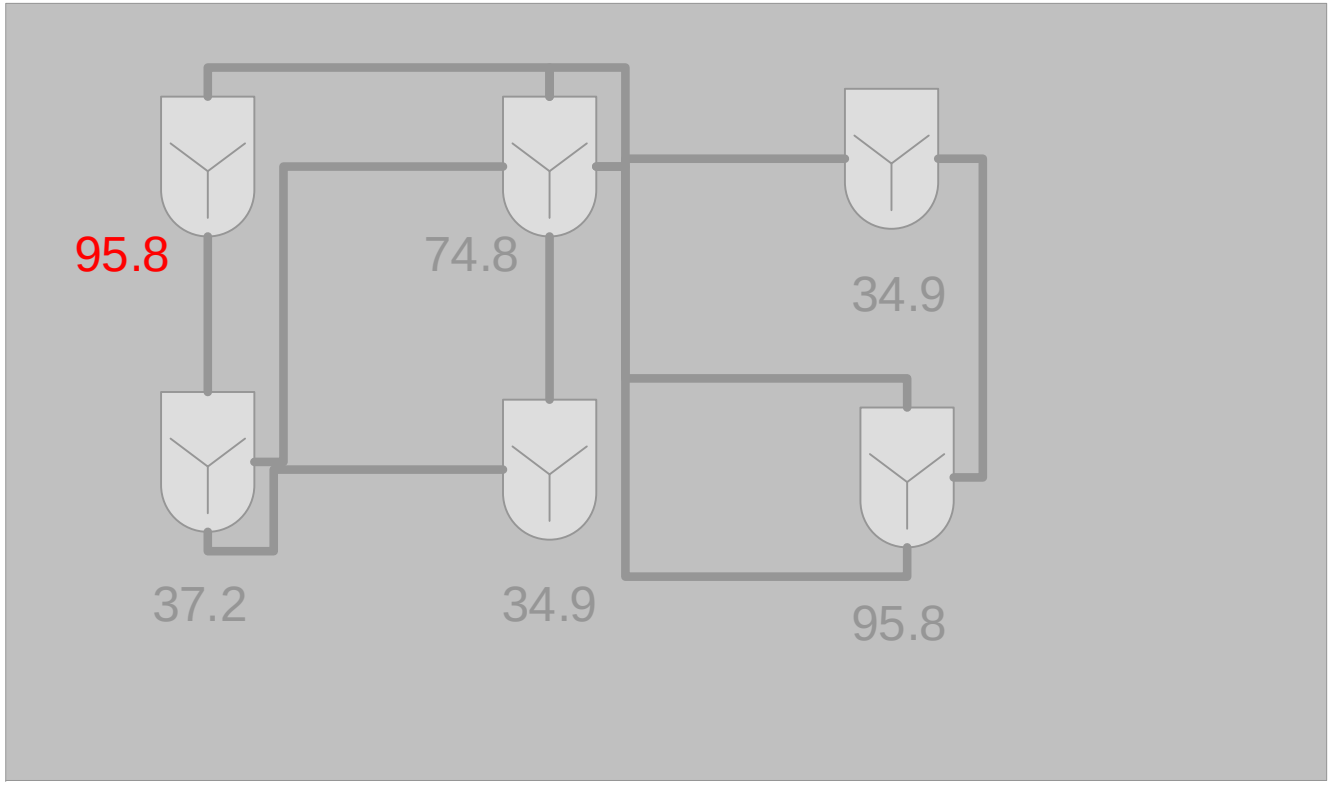
Catherine Burns
c4burns@uwaterloo.ca

Improve the Design



Catherine Burns
c4burns@uwaterloo.ca

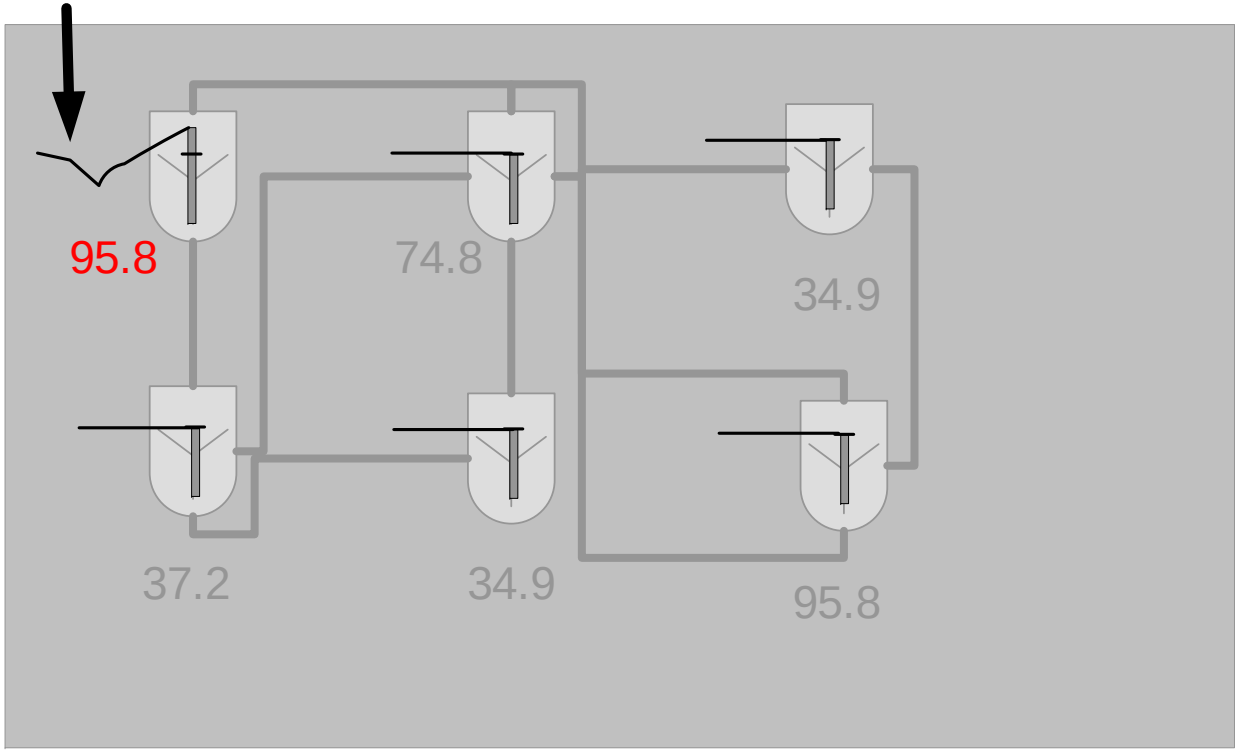
Make the problem standout



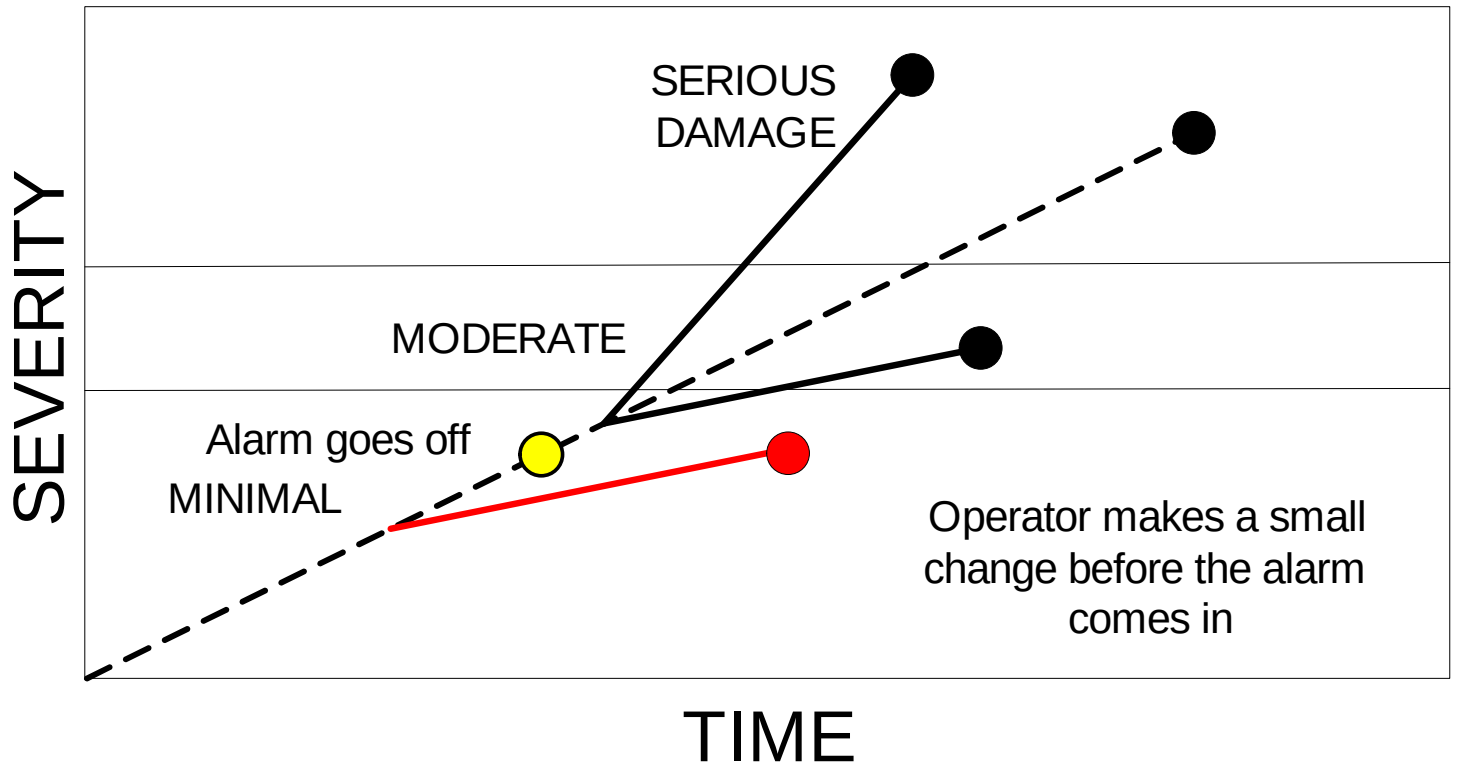
Catherine Burns
c4burns@uwaterloo.ca

Catch It Early

Operator notices the problem here



Catherine Burns
c4burns@uwaterloo.ca



Catherine Burns
c4burns@uwaterloo.ca

Why It Works

The better design builds in a margin of safety by helping people see the problem sooner.

Catherine Burns
c4burns@uwaterloo.ca

Strategy 3

Build in a Margin of Safety

Catherine Burns
c4burns@uwaterloo.ca

Challenges as Complexity Grows

- Harder to find the problem
- Problems interact
- Solutions are less clear
- Proving a solution works becomes very difficult

Catherine Burns
c4burns@uwaterloo.ca

Strategies

1. Anticipate failure points
2. Reduce the complexity
3. Build in a margin of safety

Catherine Burns
c4burns@uwaterloo.ca

Contact Info

Catherine Burns
Systems Design Engineering
University of Waterloo
Waterloo ON N2L 3G1

c4burns@uwaterloo.ca