Rethinking risk within complex systems – the Swiss Cheese Model

Andrew Brown

exploeo

Think bold, act reliable

HUNGARIAN TESTING BOARD

Photo by Roel Baardman on unsplash.com

Photo by Brandon Pierson on unsplash.com

Photo by Fabian Joy on unsplash.com

Photo by Ekansh Saxena on unsplash.com

Photo by Lance Anderson on unsplash.com


N88DN
X8


AIR CANADA
Singapore '85

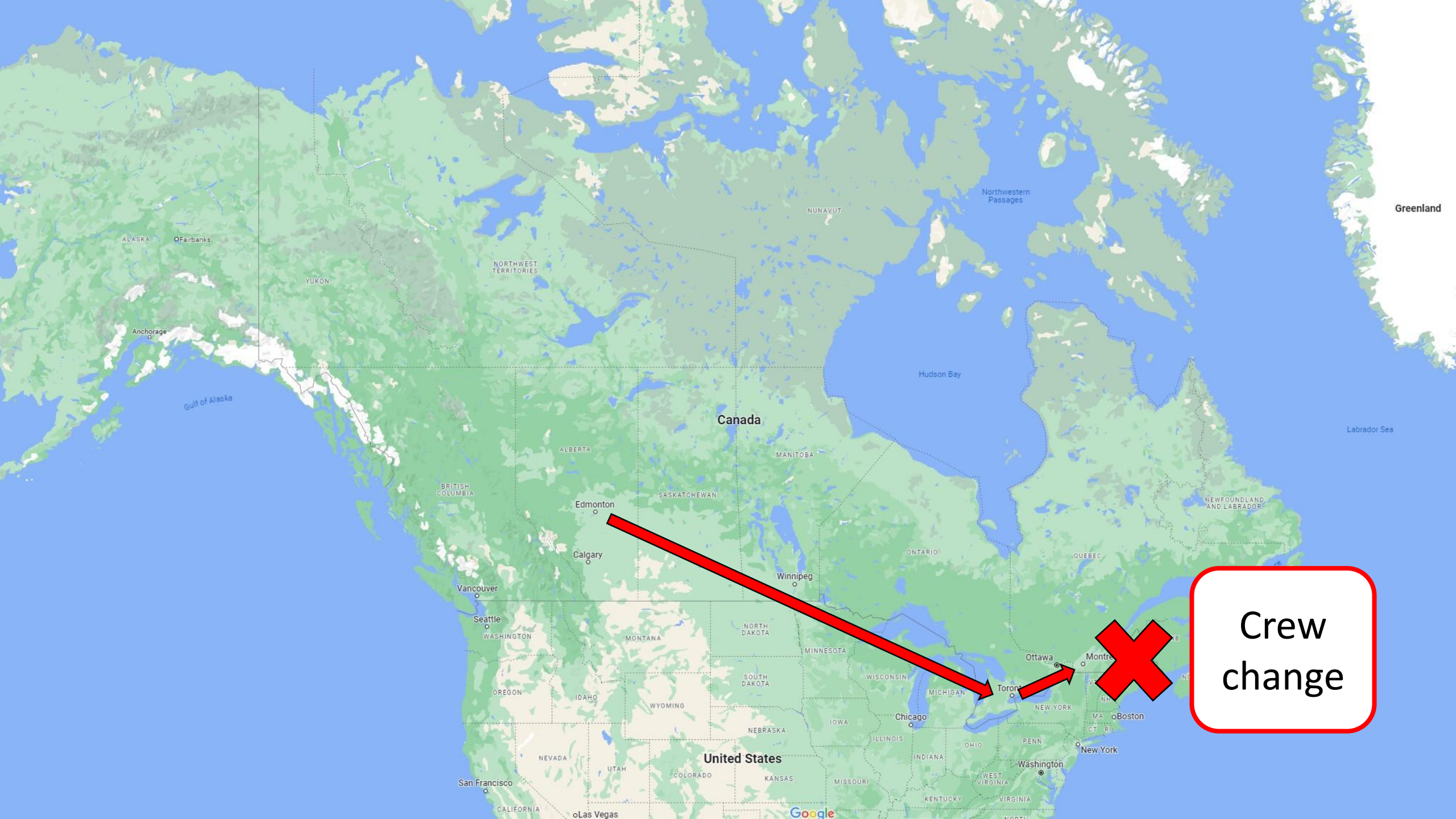
By FAA - https://lessonslearned.faa.gov


VLIEGSCHOOL HILV
LS-6b


CANADA

The Gimli Glider

The Gimli Glider


Crew change
Canada
United States
Edmonton
Calgary
Winnipeg
Vancouver
Seattle
Toronto
Ottawa
Chicago
Boston
New York
Washington
San Francisco
Las Vegas
Anchorage
Fairbanks
Greenland
Hudson Bay
Gulf of Alaska
Labrador Sea
Northwestern Passages
NUNAVUT
NORTHWEST TERRITORIES
YUKON
ALASKA
ALBERTA
SASKATCHEWAN
MANITOBA
ONTARIO
QUEBEC
NEWFOUNDLAND AND LABRADOR
BRITISH COLUMBIA
WASHINGTON
OREGON
CALIFORNIA
NEVADA
IDAHO
MONTANA
WYOMING
UTAH
COLORADO
ARIZONA
NEW MEXICO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
MINNESOTA
IOWA
MISSOURI
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
WEST VIRGINIA
VIRGINIA
PENN
NEW YORK
MA
CT
Google


Gimli
Crew change
Canada
United States
Edmonton
Calgary
Vancouver
Seattle
Ottawa
Toronto
Chicago
Boston
New York
Washington
San Francisco
Las Vegas
Anchorage
Fairbanks
Greenland
Hudson Bay
Labrador Sea
Gulf of Alaska
Northwestern Passages

How did it run out of fuel?

#1	#2	#3	#4
Blank fuel measurement	Attempted fix in Montreal	Pilot misunderstands fault	Metric conversion Kg to lb

4 factors present

Any absent: Accident would not occur

How did it run out of fuel?

#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- 2 channel fuel measurement
- Channel 2 had intermittent problem
- Switch off channel 2

How did it run out of fuel?

#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- Re-activated channel 2
- (Fuel gauges now blank)
- Distracted by another task
- Channel 2 left activated

How did it run out of fuel?

#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- Crew change at Montreal
- Sees blank fuel gauges
- Consults minimum requirements list
- (Boeing 767 new to fleet: list changed 55 times in 4 months)
- Consults maintenance list: Sees fuel problem, but with approval to fly
- Asks Outgoing pilot: “It’s okay!”

#4
Metric conversion
Kg to lb

- NASA's favourite error

NASA/KSC, Public domain, via Wikimedia Commons

How did it run out of fuel?

#1	#2	#3	#4
Blank fuel measurement	Attempted fix in Montreal	Pilot misunderstands fault	Metric conversion Kg to lb

- Pressure to convert Canada Air to metric
- 1st batch of metric aircraft
- Fuel contents measured with drip-stick
- Kg to lb conversion done wrong
- (Done by ground crew – 767 has no flight engineer)
- Believed: 22,300 Kg
- Actual: 10,000 Kg

How did it run out of fuel?

#1	#2	#3	#4
Blank fuel measurement	Attempted fix in Montreal	Pilot misunderstands fault	Metric conversion Kg to lb

- All 4 factors had to be present for accident to occur
- Factors are inevitable in normal operation

How did it run out of fuel?

#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- Complex systems inevitably run with faults

How did it run out of fuel?

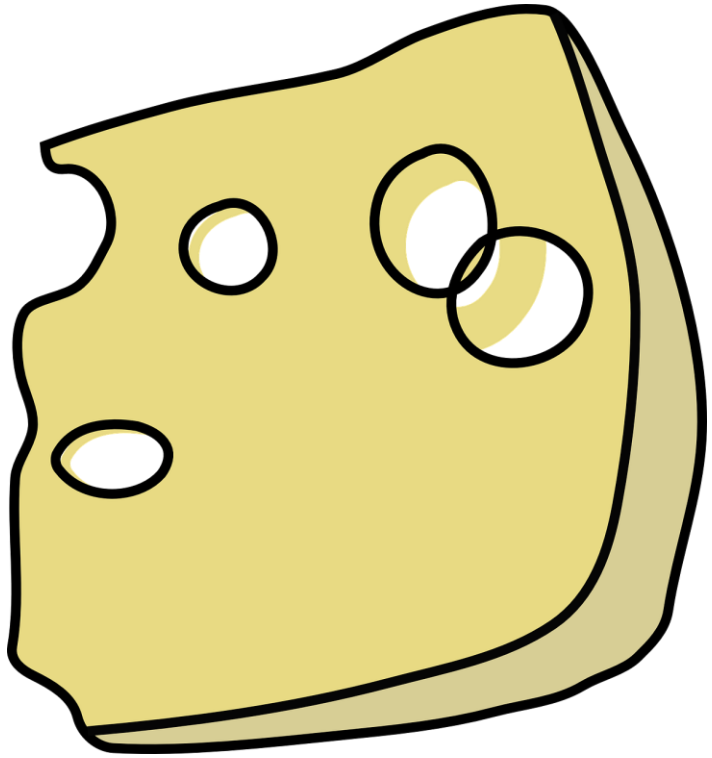
#1	#2	#3	#4
Blank fuel measurement	Attempted fix in Montreal	Pilot misunderstands fault	Metric conversion Kg to lb

- We cannot halt operations to fix every fault
- (Remember: min requirements list changed 55 times in 4 months)

How did it run out of fuel?

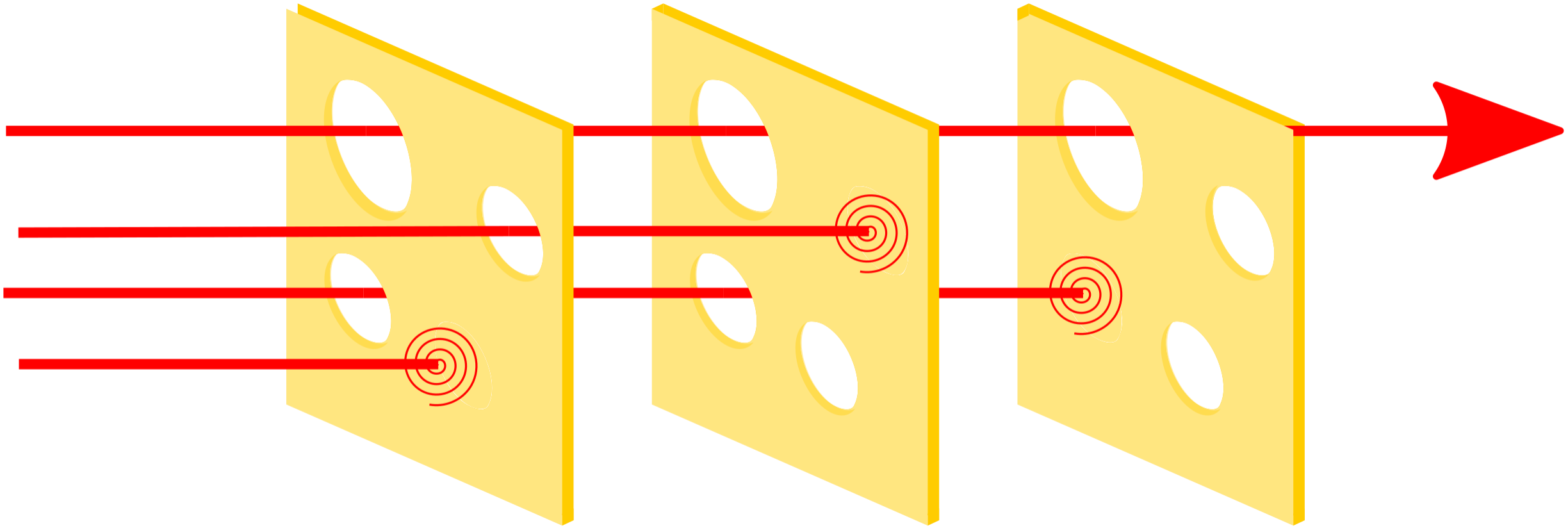
#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- We must rely upon others for information & guidance
- (List changed 55 times in 4 months)
- But we are often making judgement calls

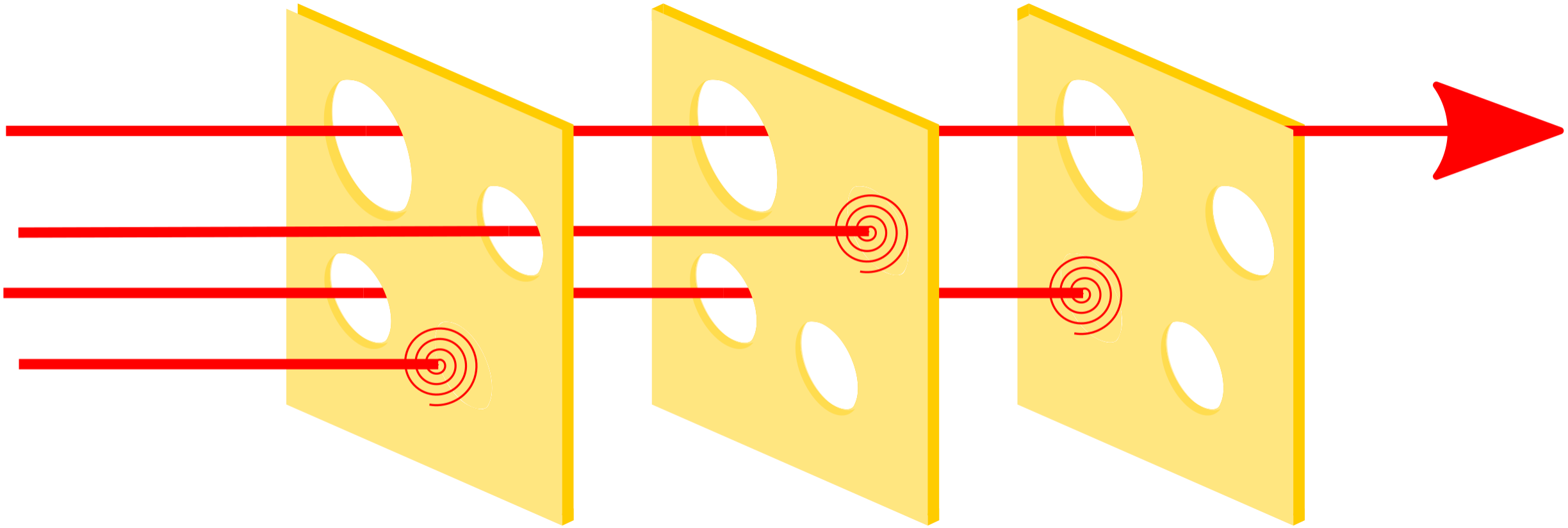


Swiss Cheese Model

– By James Reason

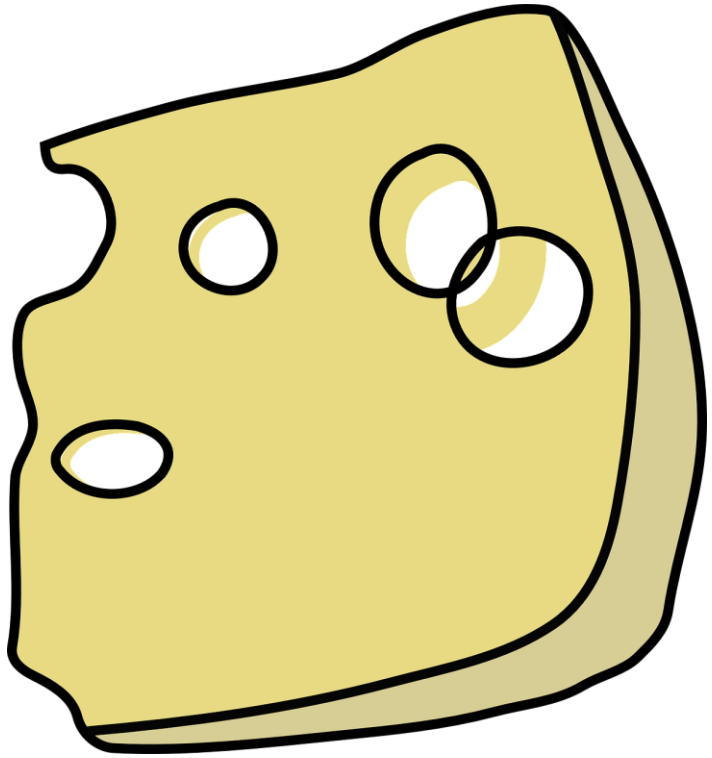


- Systems likened to multiple layers of Swiss cheese
- Holes represent weaknesses
- In live system, holes continually appear, move, disappear
- Failure in one defence does not allow a risk to materialise



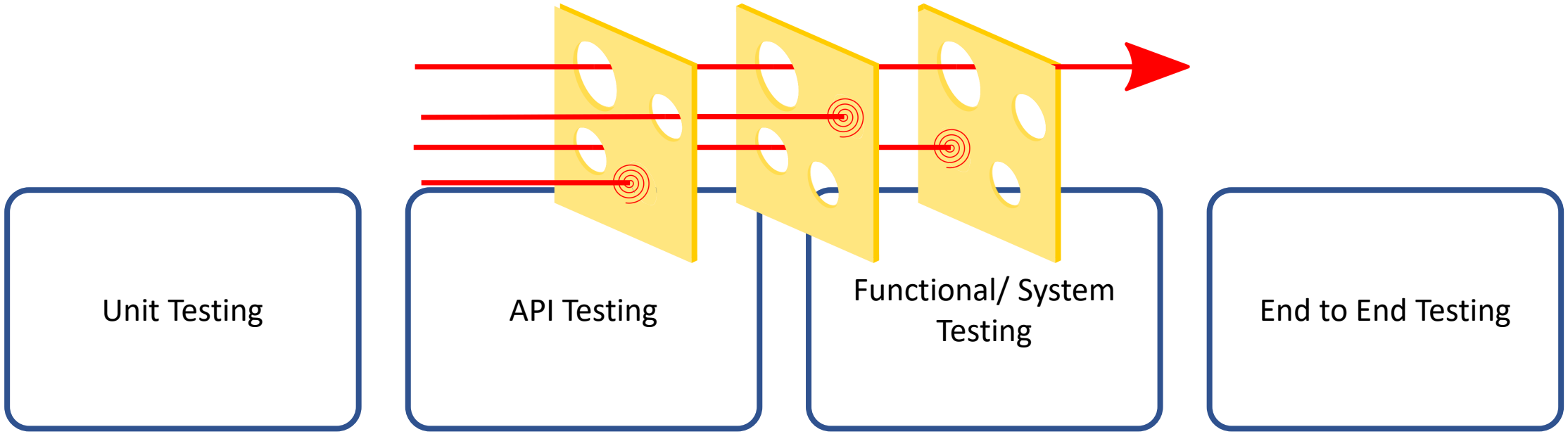
#1	#2	#3	#4
Blank fuel measurement	Attempted fix in Montreal	Pilot misunderstands fault	Metric conversion Kg to lb

- All factors needed to be present



Relevance to Software Testing

Relevance to Software Testing



- We can liken our test phases to slices of Swiss cheese
- We know exhaustive testing is impossible
- (We have holes in our cheese)
- Like Canada Air, our systems will run in degraded mode
- How can we prepare for problems in live?

What happened next?

What happened next?

- Issue partly caused by humans (decisions, misunderstandings)
- Humans avoided issue becoming a tragedy:

- Flying a jet without power is very difficult
  - Many instruments lost
  - Flaps non-functional, controls difficult to use
- No section in emergency checklist for this contingency
- Had not practised in simulator

What happened next?

- From descent rate, realised would not make Winnipeg
- * Co-pilot recalled disused Air Force base at Gimli
- At Gimli, their approach was too high and fast (Remember, no flaps)
- *Used experience as glider pilot to ‘forward slip’, and burn off height
- Landed without injuries, despite nose wheel collapsing


A good thing!

What happened next?

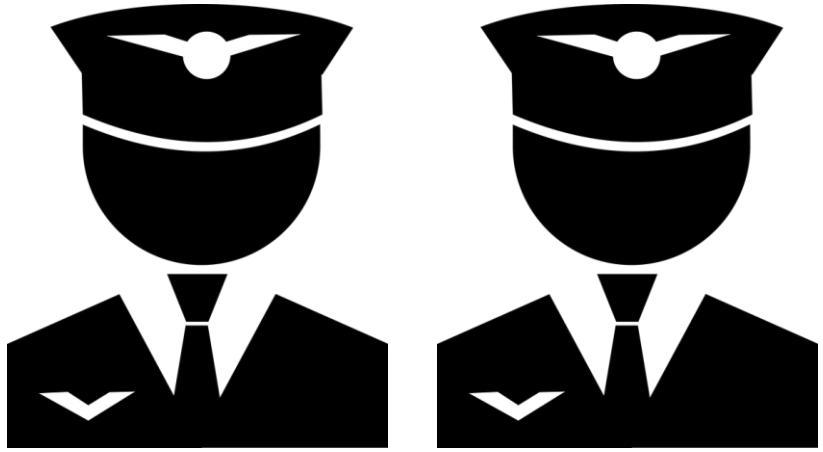
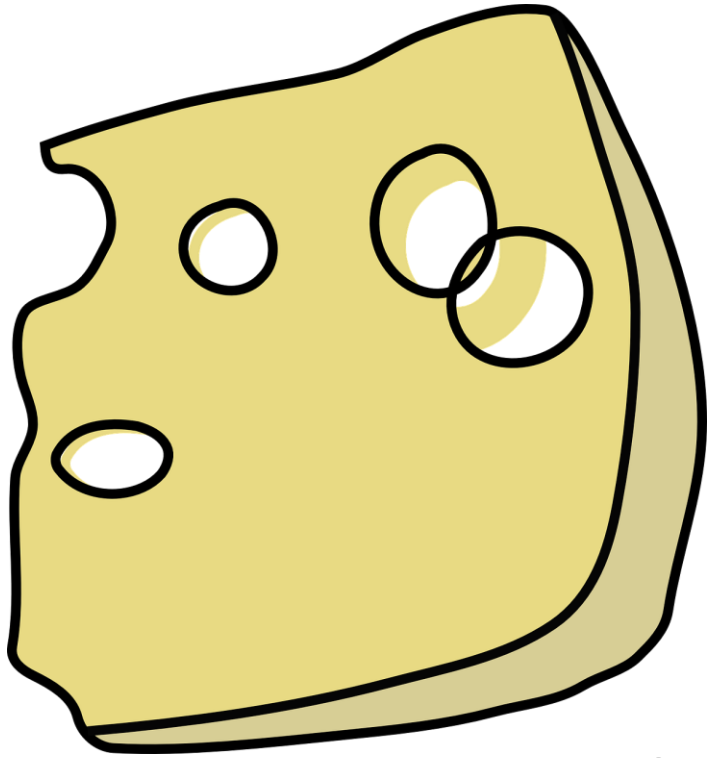


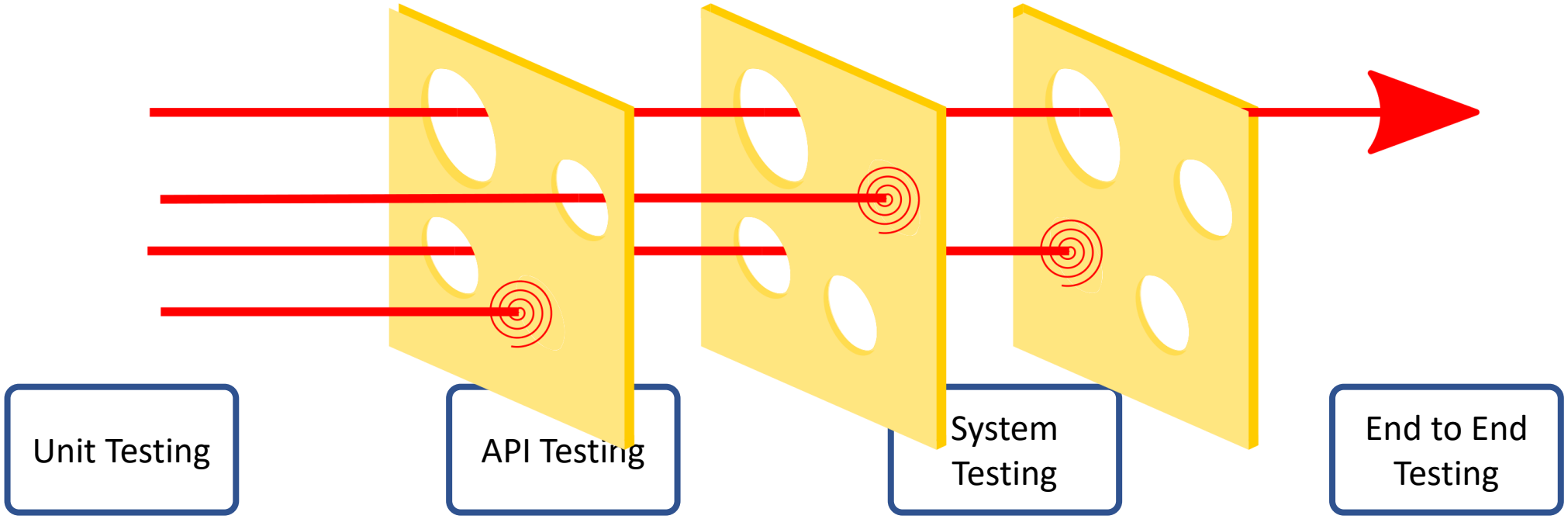
Image by OpenClipart-Vectors from pixabay.com

- The aircrew's experiences and skills averted a tragedy
- **Human intervention** both caused the issue, AND averted a tragedy



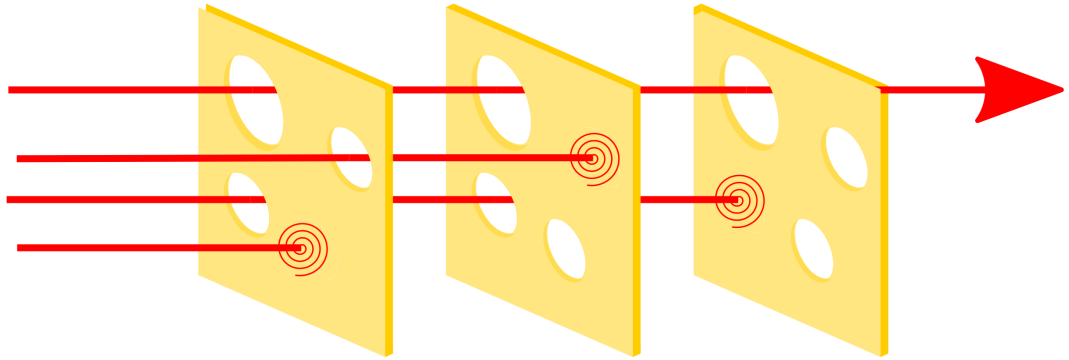
Lessons from complex systems failure for Software Testing

Lessons from complex systems



- Testing and QA cannot find every problem
- In any case, many bugs will not be fixed
- Need to communicate:
  - Our systems *always* run in degraded mode
  - Failure is *always* a possibility: We should prepare for it
  - Those unfixed bugs are more dangerous than you think

Lessons from complex systems



Production System

Unit Testing

API Testing

System Testing

End to End Testing

- How can we best respond to an issue in live?
- Training and preparing your humans
  - Simulations
  - Contingency planning
  - Checklists…

Read this paper:

How Complex Systems Fail

How Complex Systems Fail

(Being a Short Treatise on the Nature of Failure; How Failure is Evaluated; How Failure is Attributed to Proximate Cause; and the Resulting New Understanding of Patient Safety)

Richard I. Cook, MD[1]
Cognitive technologies Laboratory
University of Chicago

1) **Complex systems are intrinsically hazardous systems.**
All of the interesting systems (e.g. transportation, healthcare, power generation) are inherently and unavoidably hazardous by the own nature. The frequency of hazard exposure can sometimes be changed but the processes involved in the system are themselves intrinsically and irreducibly hazardous. It is the presence of these hazards that drives the creation of defenses against hazard that characterize these systems.

2) **Complex systems are heavily and successfully defended against failure.**
The high consequences of failure lead over time to the construction of multiple layers of defense against failure. These defenses include obvious technical components (e.g. backup systems

Principles of complex system failure

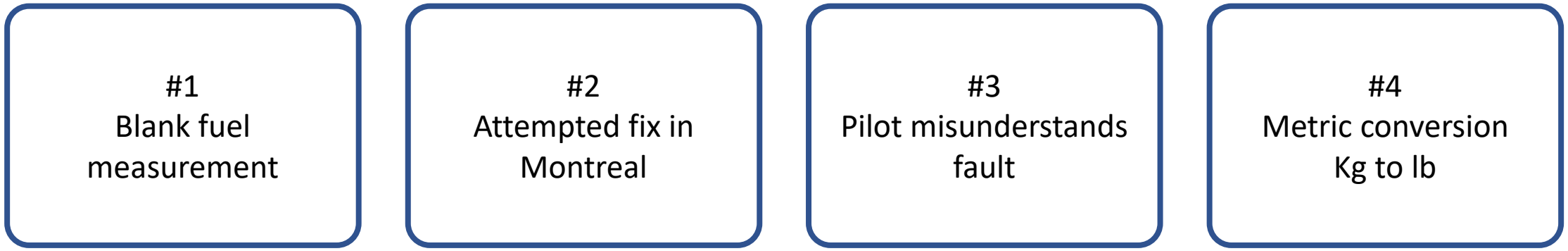
1. Complex systems are intrinsically hazardous systems


CANADA

Principles of complex system failure

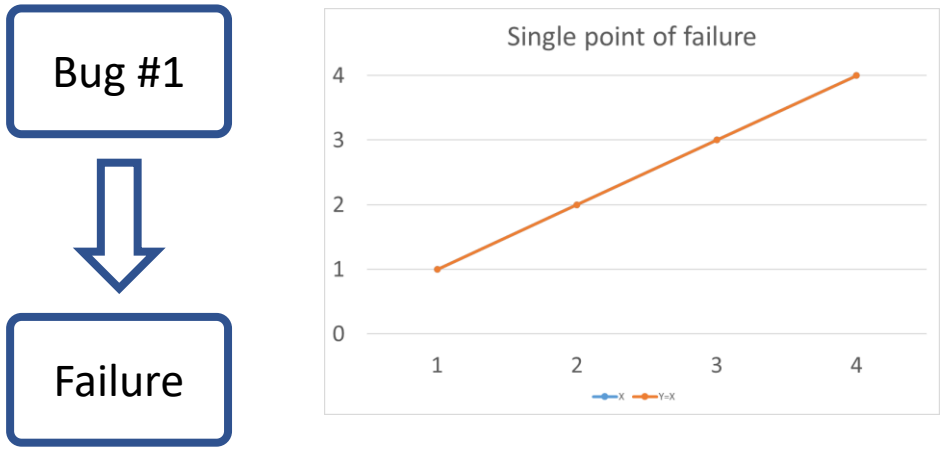
1. Complex systems are intrinsically hazardous systems
2. Complex systems are heavily and successfully defended against failure
3. Catastrophe requires multiple failures – single point failures are not enough

Catastrophe requires multiple failures – single point failures not enough



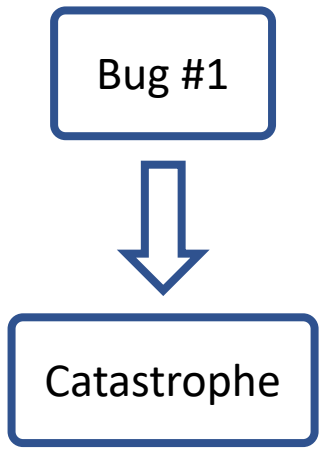
- 4 factors had to be present for accident to occur
- Important implications for bug fixing in safety-critical systems
  - All single point failures already fixed
  - Catastrophe requires 2 or more failure

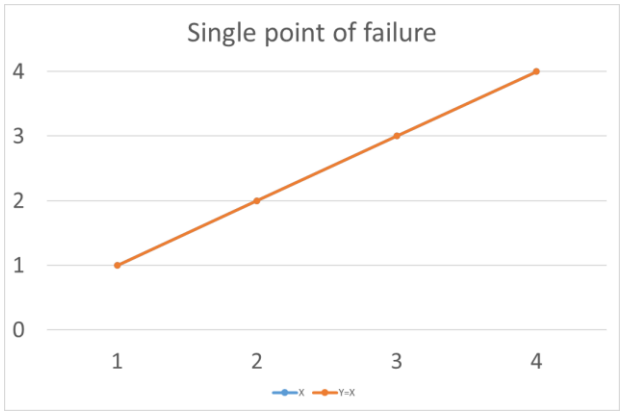
Catastrophe requires multiple failures – single point failures not enough

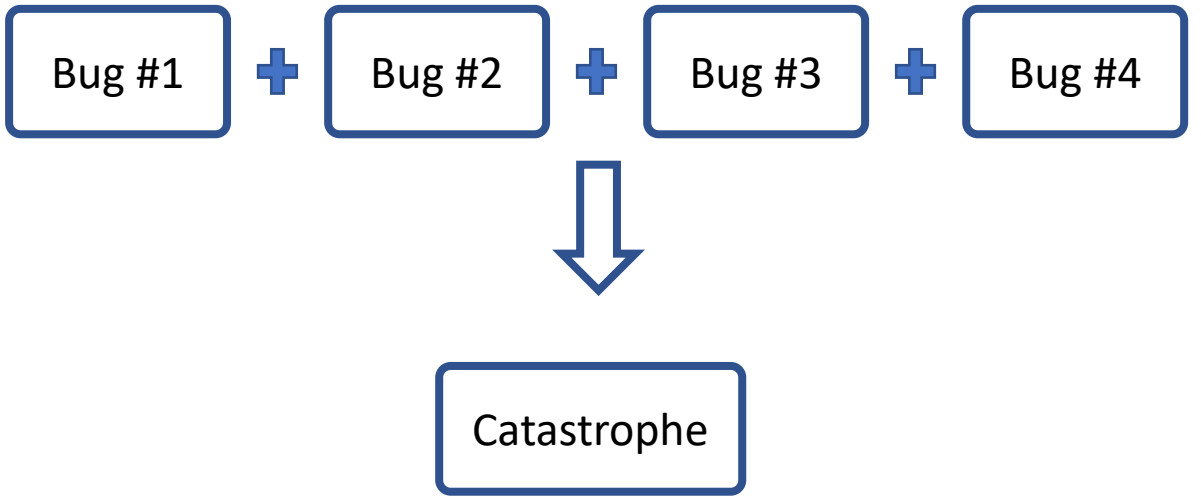


- If a single bug causes a failure, then failure rate is linearly proportional to number of bugs
- Double the bugs will double the failures

Catastrophe requires multiple failures – single point failures not enough







- If catastrophe only occurs from multiple bugs, then failure rate is proportional to the **Power** of number of bugs required
- 2 bugs needed: double the bugs will increase catastrophes by 4
- 3 bugs needed: double the bugs will increase catastrophes by 8
- 4 bugs needed: double the bugs will increase catastrophes by 16

Principles of complex system failure

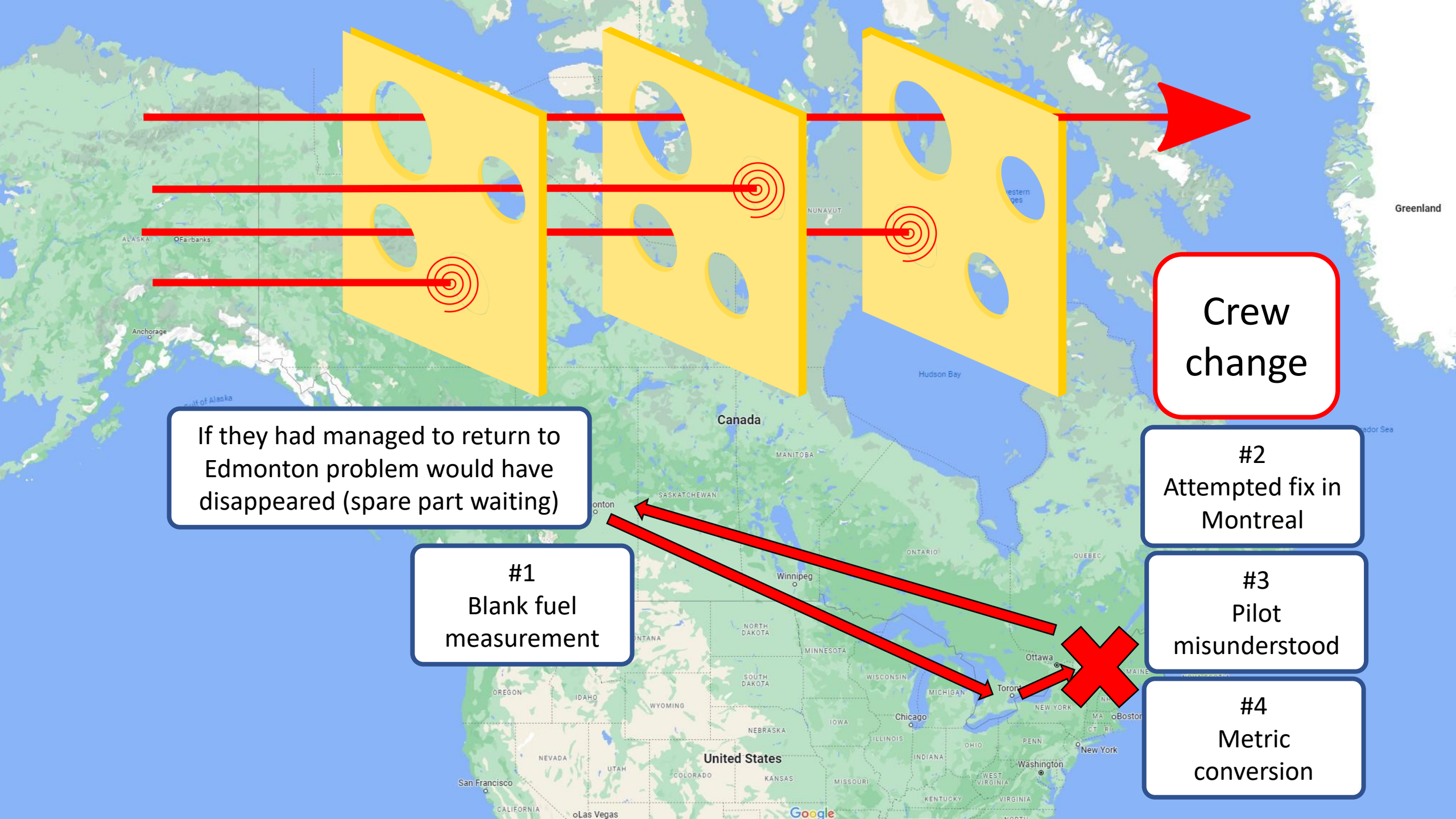
1. Complex systems are intrinsically hazardous systems
2. Complex systems are heavily and successfully defended against failure
3. Catastrophe requires multiple failures – single point failures are not enough..
4. Complex systems contain changing mixtures of failures latent within them


Crew change
#1
Blank fuel measurement
#2
Attempted fix in Montreal
#3
Pilot misunderstood
#4
Metric conversion
Edmonton
Calgary
Winnipeg
Seattle
Ottawa
Chicago
New York
Washington
San Francisco
Las Vegas
Anchorage
Fairbanks
Canada
United States
Greenland
Hudson Bay
Gulf of Alaska
Northwestern Passages
NUNAVUT
YUKON
NORTHWEST TERRITORIES
ALBERTA
SASKATCHEWAN
MANITOBA
ONTARIO
QUEBEC
Google


Crew change
#2
Attempted fix in Toronto
Would not have caused issue
#3
Pilot misunderstood
#4
Metric conversion
Edmonton
Calgary
Winnipeg
Vancouver
Seattle
Toronto
Ottawa
Chicago
New York
Washington
Boston
Canada
Greenland
Hudson Bay
Gulf of Alaska
Anchorage
Fairbanks
Las Vegas
San Francisco
Google


Crew change
Problem could not have occurred at start (no crew handover)
#3 Pilot misunderstood
#4 Metric conversion
Edmonton
Calgary
Winnipeg
Vancouver
Seattle
Ottawa
Chicago
New York
Washington
San Francisco
Las Vegas
Canada
United States
Greenland
Hudson Bay
Northwestern Passages
Labrador Sea
Anchorage
Fairbanks
Google


If they had managed to return to Edmonton problem would have disappeared (spare part waiting)
Edmonton
Calgary
Winnipeg
Vancouver
Seattle
Ottawa
Montreal
Toronto
Chicago
Boston
New York
Washington
San Francisco
Las Vegas
Anchorage
Fairbanks
Canada
United States
Greenland
Hudson Bay
Labrador Sea
Northwestern Passages
NUNAVUT
NORTHWEST TERRITORIES
YUKON
ALASKA
MANITOBA
SASKATCHEWAN
ONTARIO
QUEBEC
NEWFOUNDLAND AND LABRADOR
Gulf of St Lawrence
WASHINGTON
OREGON
CALIFORNIA
IDAHO
NEVADA
MONTANA
WYOMING
UTAH
COLORADO
NORTH DAKOTA
SOUTH DAKOTA
NEBRASKA
KANSAS
MINNESOTA
IOWA
MISSOURI
WISCONSIN
ILLINOIS
MICHIGAN
INDIANA
OHIO
KENTUCKY
WEST VIRGINIA
VIRGINIA
PENN
NEW YORK
MAINE
VT
NH
MA
CT
RI
NB
PE
NOVA SCOTIA
Google


Crew change
If they had managed to return to Edmonton problem would have disappeared (spare part waiting)
#1
Blank fuel measurement
#2
Attempted fix in Montreal
#3
Pilot misunderstood
#4
Metric conversion
Canada
United States
Greenland
Hudson Bay
Anchorage
Fairbanks
Winnipeg
Ottawa
Chicago
New York
Washington
San Francisco
Las Vegas


A good thing!

Principles of complex system failure

1. Complex systems are intrinsically hazardous systems
2. Complex systems are heavily and successfully defended against failure
3. Catastrophe requires multiple failures – single point failures are not enough..
4. Complex systems contain changing mixtures of failures latent within them
5. Complex systems run in degraded mode

How did it run out of fuel?

#1 Blank fuel measurement	#2 Attempted fix in Montreal	#3 Pilot misunderstands fault	#4 Metric conversion Kg to lb

- Pilot change at Montreal
- Sees blank fuel gauges
- **Minimum requirements list changed 55 times in 4 months**
- Consults maintenance list
- Sees fuel problem, but with approval to fly

Principles of complex system failure

1. Complex systems are intrinsically hazardous systems
2. Complex systems are heavily and successfully defended against failure
3. Catastrophe requires multiple failures – single point failures are not enough..
4. Complex systems contain changing mixtures of failures latent within them
5. Complex systems run in degraded mode
6. Catastrophe is always just around the corner


CANADA

Principles of complex system failure

7. Post-accident attribution accident to a ‘root cause’ is fundamentally wrong
8. Hindsight biases post-accident assessments of human performance
9. Views of ‘cause’ limit the effectiveness of defenses against future events
10. **Human operators have dual roles: as producers & as defenders against failure**

Principles of complex system failure

7. Post-accident attribution accident to a ‘root cause’ is fundamentally wrong
8. Hindsight biases post-accident assessments of human performance
9. Views of ‘cause’ limit the effectiveness of defenses against future events
10. **Human operators have dual roles: as producers & as defenders against failure**
11. All practitioner actions are gambles

Principles of complex system failure

7. Post-accident attribution accident to a ‘root cause’ is fundamentally wrong
8. Hindsight biases post-accident assessments of human performance
9. Views of ‘cause’ limit the effectiveness of defenses against future events
10. **Human operators have dual roles: as producers & as defenders against failure**
11. All practitioner actions are gambles
12. Actions at the sharp end resolve all ambiguity

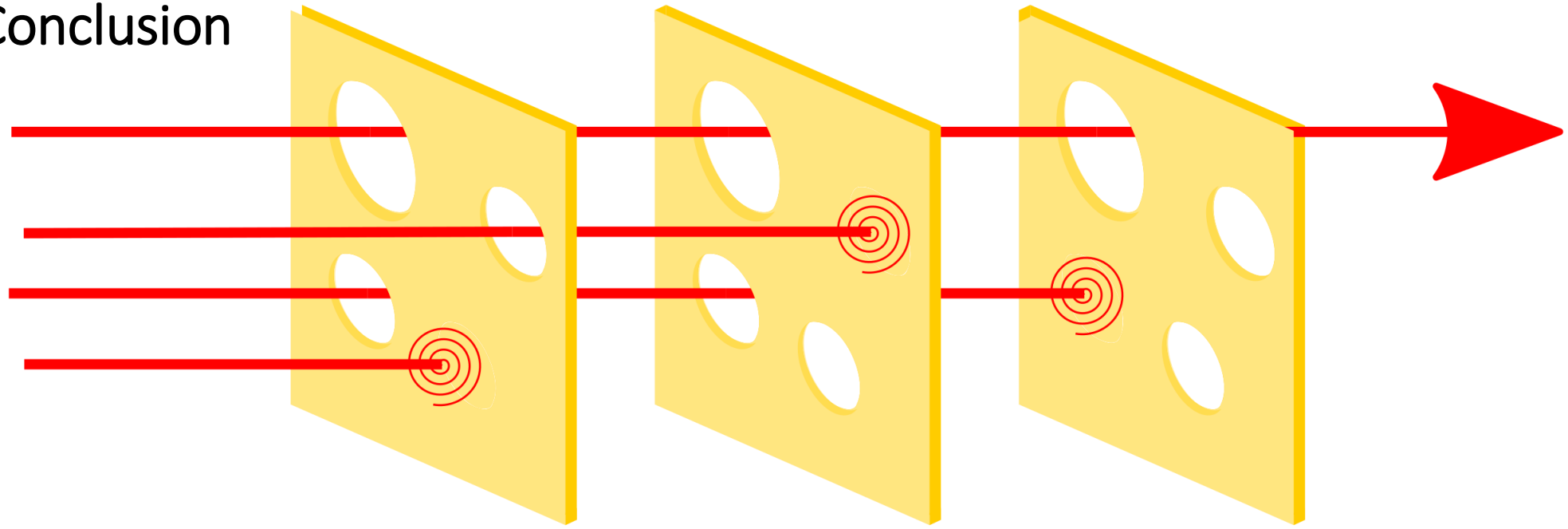
Principles of complex system failure

13. Human practitioners are the adaptable element of complex systems

Principles of complex system failure

13. Human practitioners are the adaptable element of complex systems
14. Human expertise in complex systems is constantly changing
15. Change introduces new forms of failure
16. Safety is a characteristic of systems and not of their components
17. People continuously create safety
18. Failure free operations require experience with failure

Conclusion



1. Complex systems fail in different ways from simple systems
2. The Swiss Cheese Model can help us think about failure & defences
3. Removing minor bugs may be important (3rd power effect)
4. We need to better prepare teams to respond to failure
5. Please read **How Complex Systems Fail** by Richard Cook

HUNGARIAN
TESTING BOARD

Andrew Brown

(expleo)

Think bold, act reliable

Thank you!
Questions?