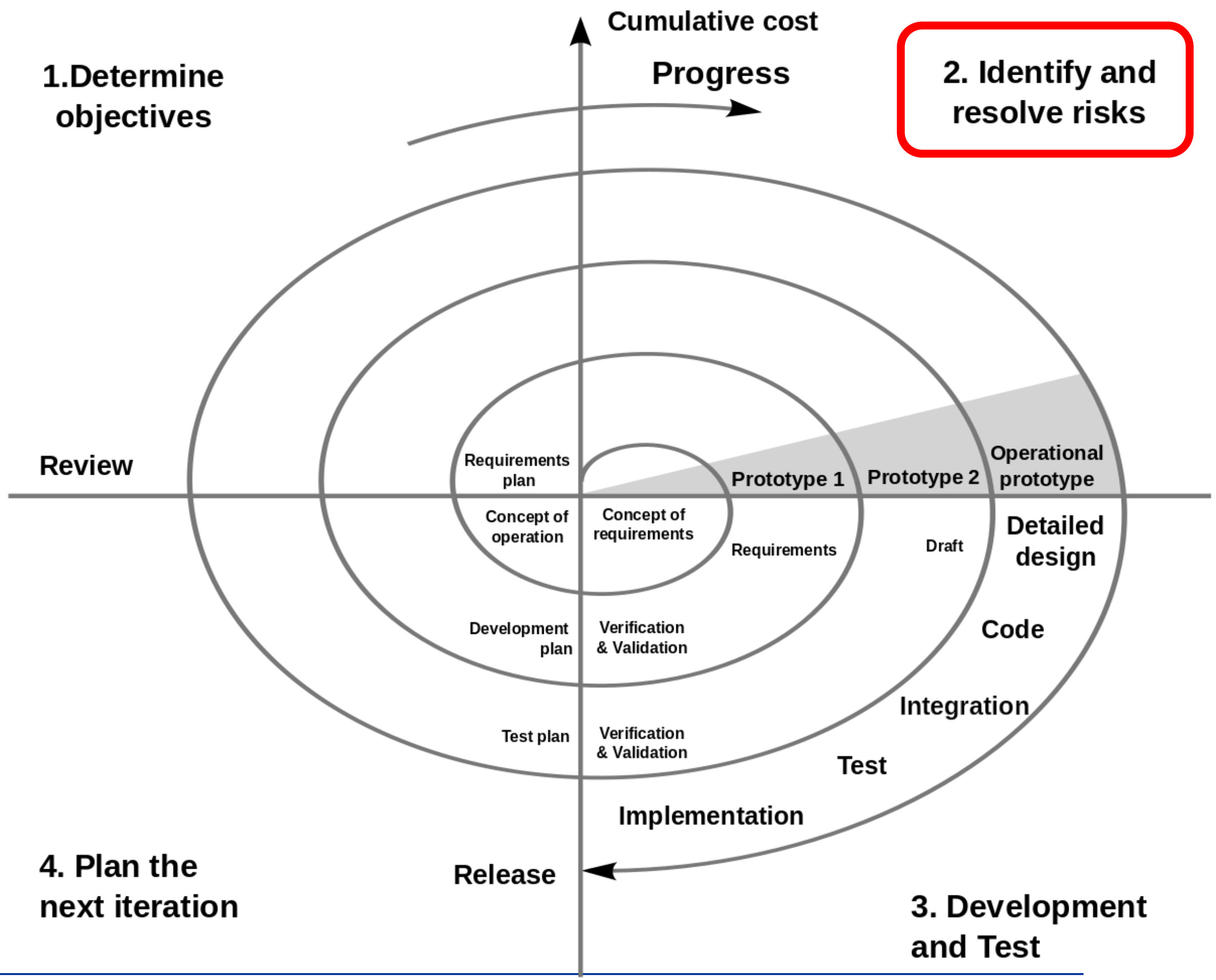
Lecture 8: Risk Management

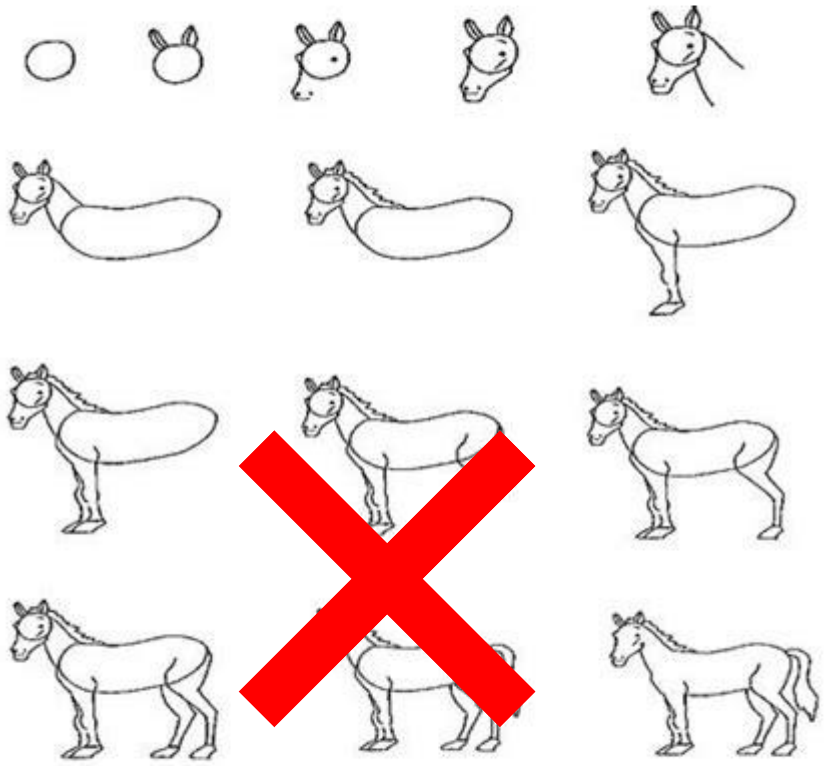
Previously…

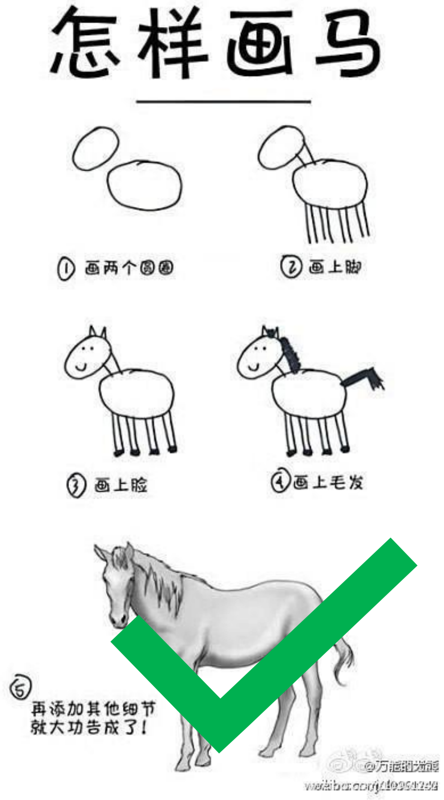
- The Spiral development model
- Use risk management to guide iterations



Iterative Software Development

- Develop “validatable” artifacts early



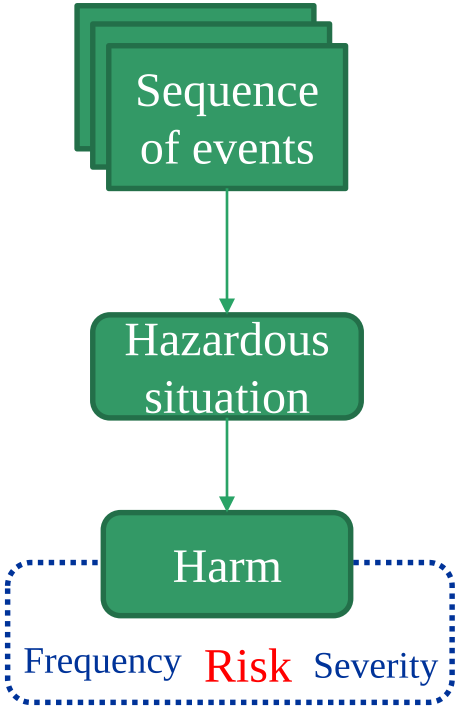


What is risk management?

- There are undesired situations that we don’t want to be in
  - i.e. an order was missed and the customer was not happy
- What can lead to those undesired situations?
- Can we avoid these undesired situations?
- If not, can we reduce potential damage?

Terminologies

- Harm/impact: Loss when running the system in certain situations
  - Financial/time loss
  - Life/health loss
- Hazard: A potential source of harm
- Hazardous situation: circumstance in which people or property are exposed to one or more hazard(s).
- Risk: Combination of the probability of occurrence of harm and the severity of that harm



Types of risks

- **Efficacy risk:** The system fails to do what it was intended to do

- **Safety risk:** People & properties may be harmed under normal use of the system

- **Security risk:** The system is prone to unintentional and malicious misuse which can cause harm

Example: Infusion pump

- Deliver drug with programmed dosage
- Hazard: Pump won’t stop
- Hazardous situation: over-delivery of drug
- Sequence of events:
  1. Unexpected user programming sequence
  2. Corrupted limit value
  3. Pump runs beyond programmed limit
- Harm:
  1. Discomfort
  2. Tissue/organ damage
  3. Death

Infusion
Pump

Risk Management process

1. Risk analysis
   – Analyze the frequency and severity of harms

2. Risk evaluation
   – Determine what is acceptable risk

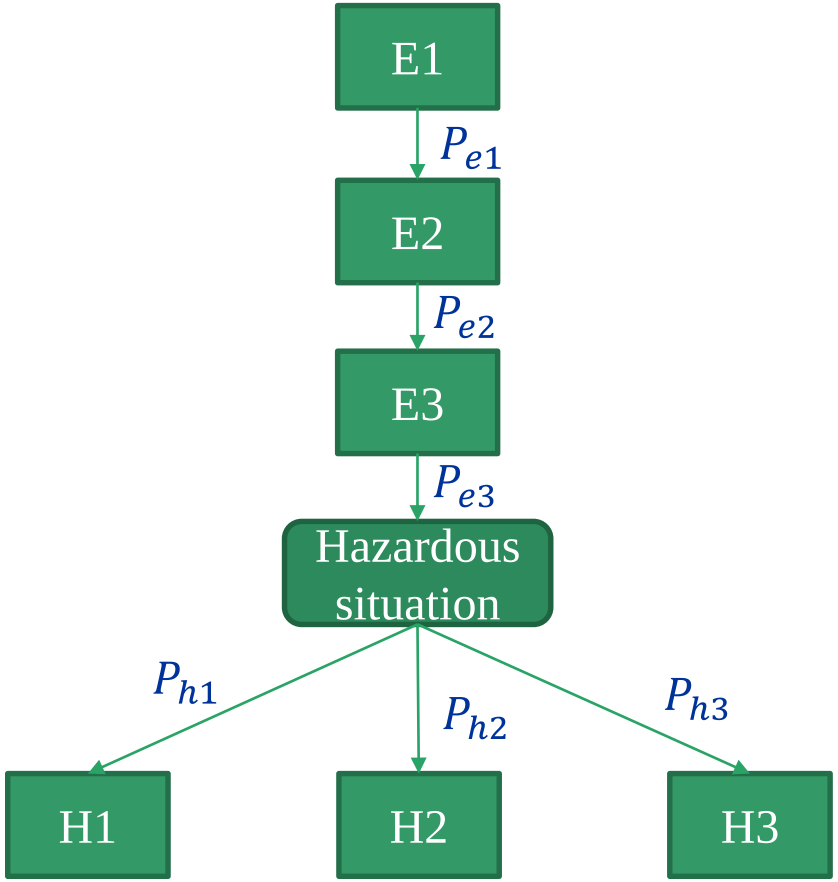
3. Risk control
   – How to prevent hazard and/or reduce harm?

4. Residual risk acceptability
   – Are there new risks introduced by control measures?

Risk analysis

- Hazard: Pump won't stop
- Hazardous situation: over delivery of drug
- Sequence of events:
  1. Unexpected user programming sequence
  2. Corrupted limit value
  3. Pump runs beyond programmed limit
- Harm:
  1. Discomfort **Minor**
  2. Tissue/organ damage **Major**
  3. Death **Catastrophic**

$$P_{death} = P_{e1} \times P_{e2} \times P_{e3} \times P_{h3}$$

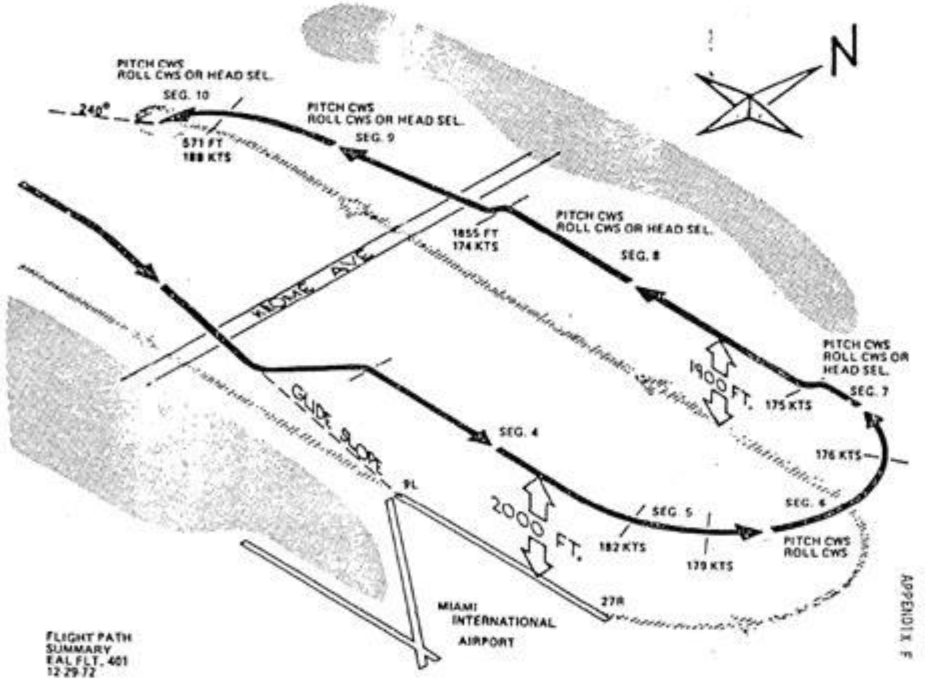


Risk assessment methods

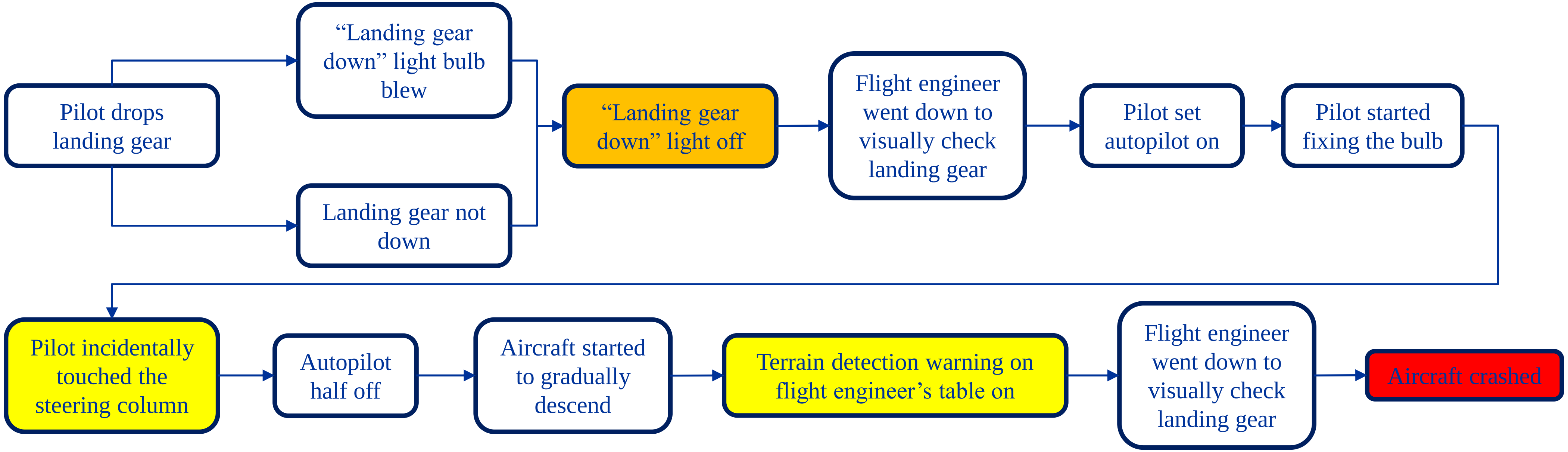
- Expert opinion
  - Solicitation of views from those deemed to be most knowledgeable
- Data diving
  - Use of data to assess impact and frequency over a specified time period as a proxy for likelihood
- Stochastic
  - Have some prior knowledge
  - Application of statistical models (e.g., Monte Carlo simulation) that capture the essentials of the underlying behavior
- Cultural
  - Reliance on the inherent subjective assessment of both the nature of events and their likelihood and impact
- Often used in combinations

Small & rare hazards can lead to fatal harm

- Eastern Airlines Flight 401, 1972

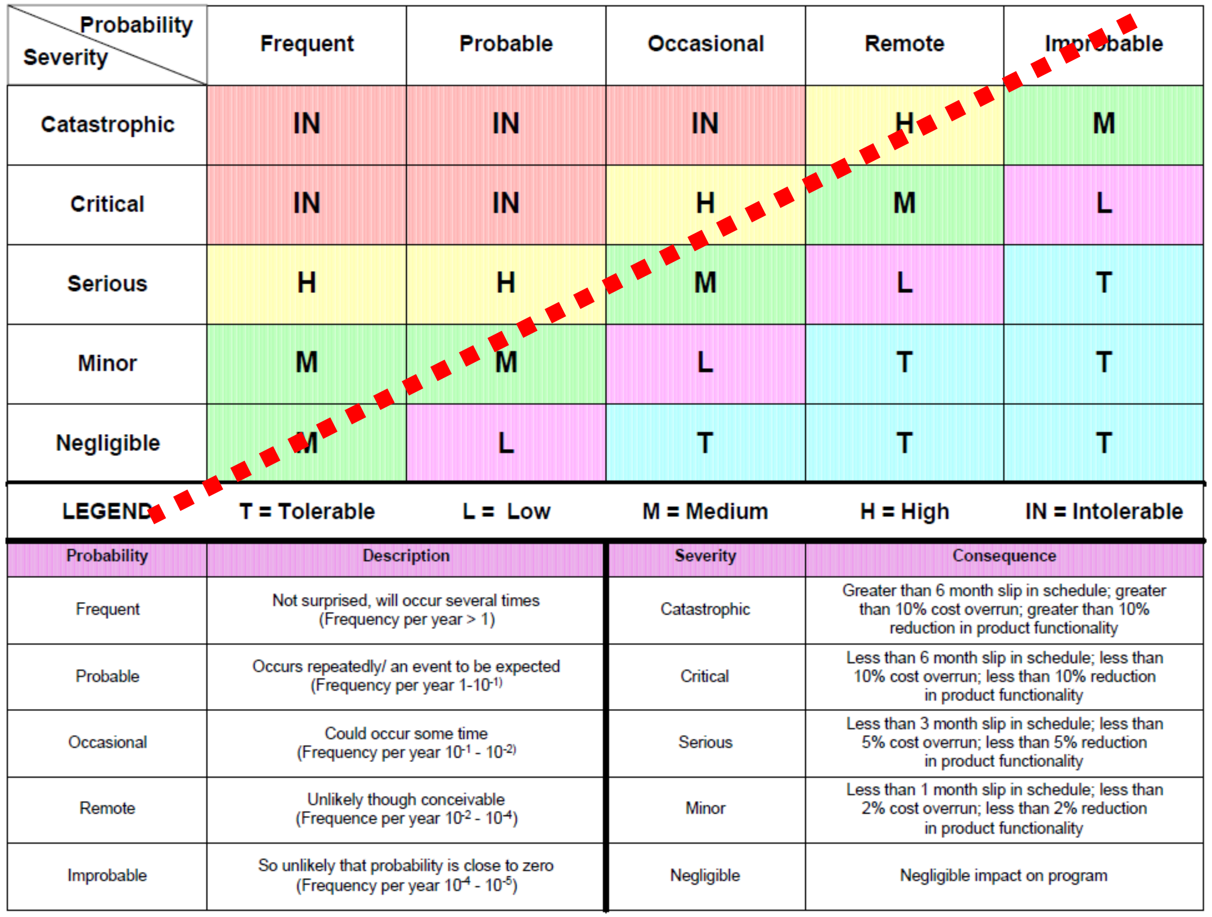


Sequence of events


Pilot drops landing gear
"Landing gear down" light bulb blew
Landing gear not down
"Landing gear down" light off
Flight engineer went down to visually check landing gear
Pilot set autopilot on
Pilot started fixing the bulb
Pilot incidentally touched the steering column
Autopilot half off
Aircraft started to gradually descend
Terrain detection warning on flight engineer's table on
Flight engineer went down to visually check landing gear
Aircraft crashed

Risk Evaluation

- Acceptable
- Unacceptable
- ALARP (As Low As Reasonably Practicable)



Probability / Severity	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic	IN	IN	IN	H	M
Critical	IN	IN	H	M	L
Serious	H	H	M	L	T
Minor	M	M	L	T	T
Negligible	M	L	T	T	T

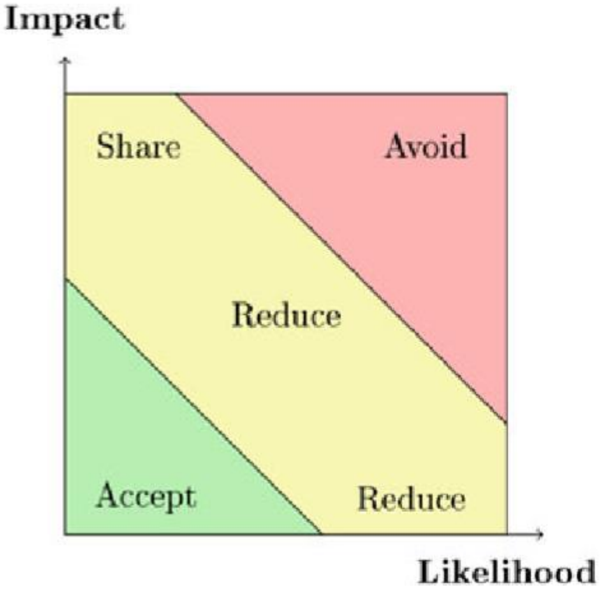
LEGEND T = Tolerable L = Low M = Medium H = High IN = Intolerable

Probability	Description	Severity	Consequence
Frequent	Not surprised, will occur several times (Frequency per year > 1)	Catastrophic	Greater than 6 month slip in schedule; greater than 10% cost overrun; greater than 10% reduction in product functionality
Probable	Occurs repeatedly/ an event to be expected (Frequency per year 1-10^{-1})	Critical	Less than 6 month slip in schedule; less than 10% cost overrun; less than 10% reduction in product functionality
Occasional	Could occur some time (Frequency per year 10^{-1} - 10^{-2})	Serious	Less than 3 month slip in schedule; less than 5% cost overrun; less than 5% reduction in product functionality
Remote	Unlikely though conceivable (Frequence per year 10^{-2} - 10^{-4})	Minor	Less than 1 month slip in schedule; less than 2% cost overrun; less than 2% reduction in product functionality
Improbable	So unlikely that probability is close to zero (Frequency per year 10^{-4} - 10^{-5})	Negligible	Negligible impact on program

Table 2-1 Sample Risk Matrix

Actions towards different risks

- Accept
  - Appropriate for low risk exposure. No specific action will be undertaken to mitigate or manage the risk. Instead a contingency plan will be developed to tackle the eventuality that the risk may be realized
- Reduce
  - Appropriate for medium negative risk. Actions will be undertaken to reduce either the impact or the likelihood of occurrence of the event
- Share/transfer
  - Appropriate for low frequency high impact positive risk where the efforts to manage the risk alone may not be warranted owing to the relative unlikelihood of it occurring. Measures will be undertaken (with others) to share the risks and rewards
- Avoid
  - Appropriate for high negative risk. The activities that give rise to the risk will not be undertaken



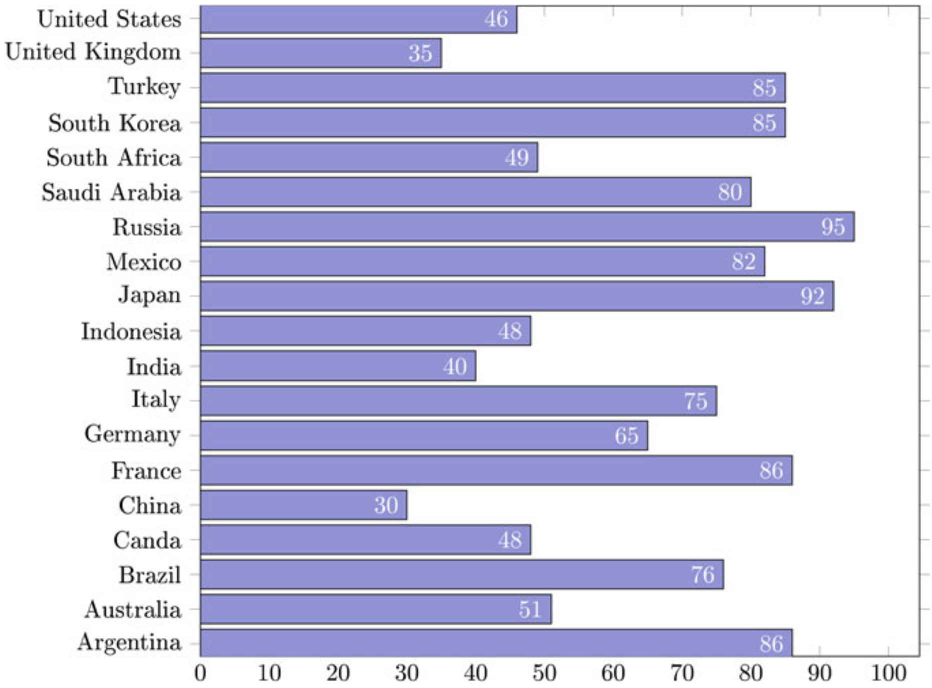
How to draw the line - Attitude towards risks

- *Risk-averse*:
  - Preference of secure payoffs, common sense and facts over theories. Propensity to over-react to threats and under-react to opportunities.
- *Risk-seeking*:
  - Preference towards speculation and unafraid to take action. Propensity to underestimate threats and overestimate opportunities.
- *Risk-tolerance*:
  - Indifference towards uncertainty that lends itself to reactive rather than proactive measures. Propensity to fail to appreciate importance of threats and opportunities alike.
- *Risk-neutral*:
  - Impartial attitude towards risk and act in the interests of significant benefits. Propensity to focus on the longer term.

*Murray-Webster and Hillson (2008)

Uncertainty Avoidance Index (UAI)

- Extent to which the members of a culture feel threatened by ambiguous or unknown situations and have created beliefs and institutions that try to avoid these” (Hofstede 2013)



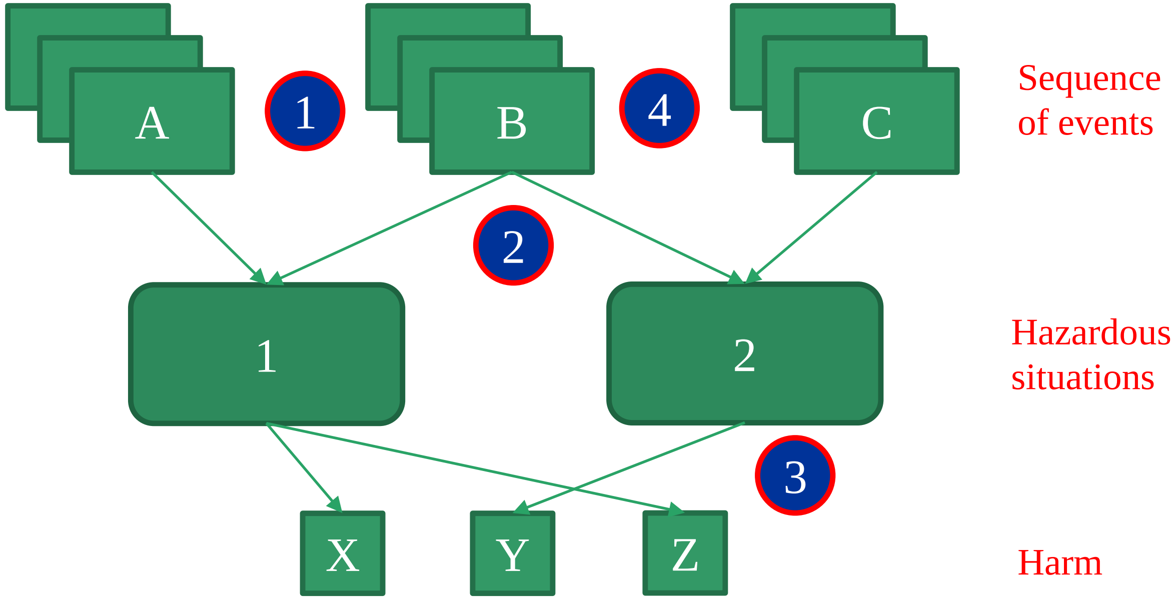
Risk Control

- The activity in which decisions are made and measures implemented in which risks are reduced to, or maintained within specified levels

- Risk Control Measures (RCM)

Risk Control Measures (RCM)

1. Preventive measures
   - i.e. a cover on emergency stop button
2. Corrective measures
   - i.e. watchdog
3. Mitigating measures
   - i.e. fuse
4. Informational control
   - i.e. warning, personnel training



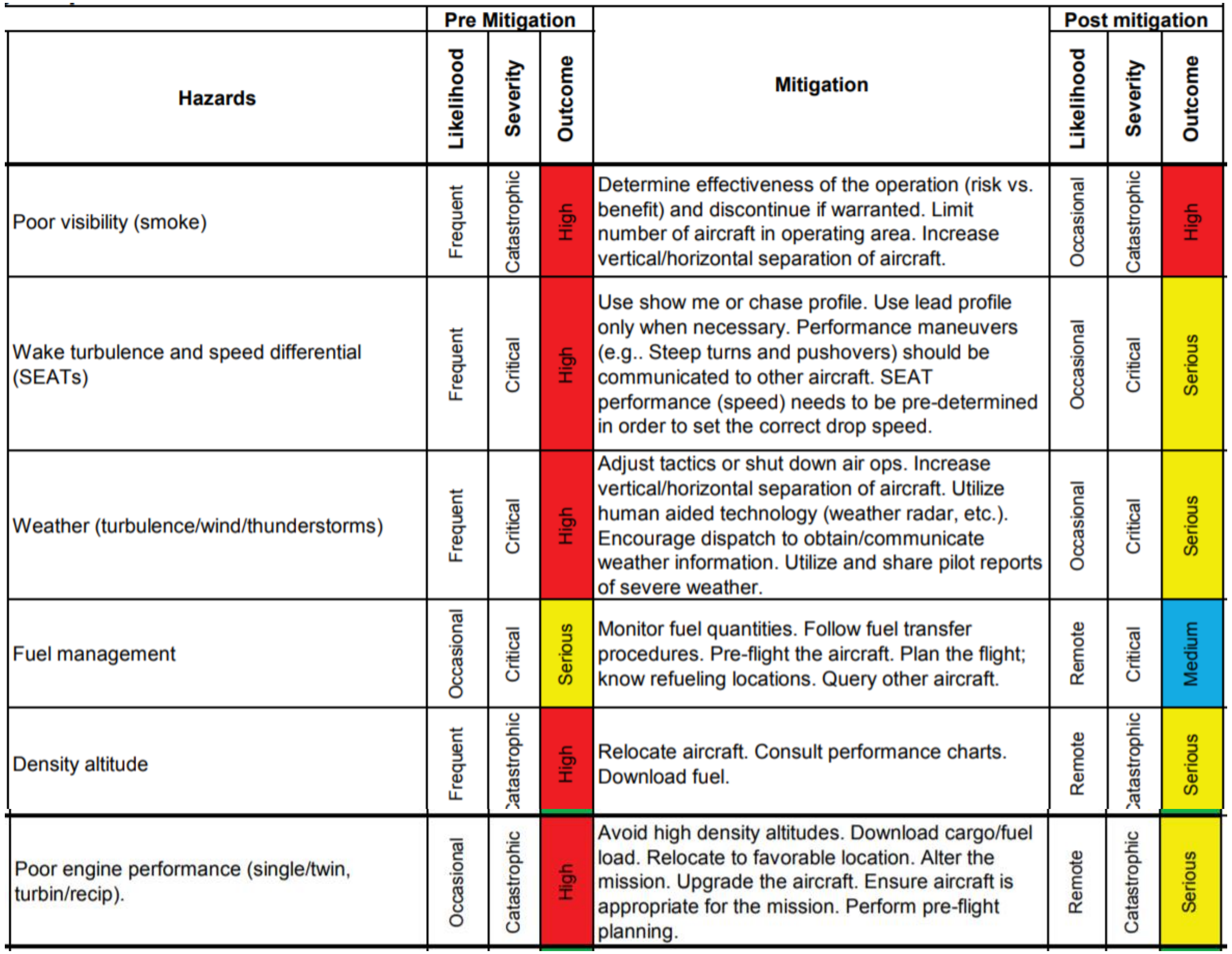
	Reduce probability	Reduce severity
Preventive	Yes	No
Corrective	Possibly	Possibly
Mitigating	No	Yes
Informational	Yes	No

Residual Risk Evaluation

- Whether the benefit of further measures outweigh the overall residual risk
- Treat remaining risk as new risk and see whether it’s acceptable
- Principle: ALARP (As Low As Reasonably Practicable)

RCM Example

- Mostly preventive



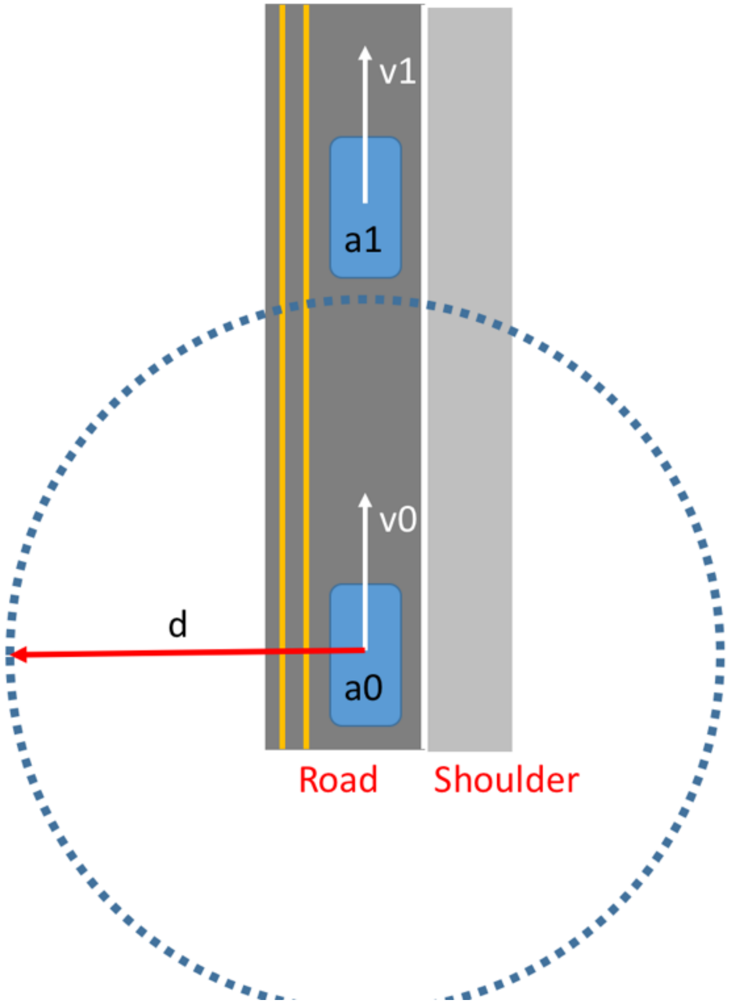
	Pre Mitigation				Post mitigation		
Hazards	**Likelihood**	**Severity**	**Outcome**	**Mitigation**	**Likelihood**	**Severity**	**Outcome**
Poor visibility (smoke)	Frequent	Catastrophic	High	Determine effectiveness of the operation (risk vs. benefit) and discontinue if warranted. Limit number of aircraft in operating area. Increase vertical/horizontal separation of aircraft.	Occasional	Catastrophic	High
Wake turbulence and speed differential (SEATs)	Frequent	Critical	High	Use show me or chase profile. Use lead profile only when necessary. Performance maneuvers (e.g.. Steep turns and pushovers) should be communicated to other aircraft. SEAT performance (speed) needs to be pre-determined in order to set the correct drop speed.	Occasional	Critical	Serious
Weather (turbulence/wind/thunderstorms)	Frequent	Critical	High	Adjust tactics or shut down air ops. Increase vertical/horizontal separation of aircraft. Utilize human aided technology (weather radar, etc.). Encourage dispatch to obtain/communicate weather information. Utilize and share pilot reports of severe weather.	Occasional	Critical	Serious
Fuel management	Occasional	Critical	Serious	Monitor fuel quantities. Follow fuel transfer procedures. Pre-flight the aircraft. Plan the flight; know refueling locations. Query other aircraft.	Remote	Critical	Medium
Density altitude	Frequent	Catastrophic	High	Relocate aircraft. Consult performance charts. Download fuel.	Remote	Catastrophic	Serious
Poor engine performance (single/twin, turbin/recip).	Occasional	Catastrophic	High	Avoid high density altitudes. Download cargo/fuel load. Relocate to favorable location. Alter the mission. Upgrade the aircraft. Ensure aircraft is appropriate for the mission. Perform pre-flight planning.	Remote	Catastrophic	Serious

Prioritize risks

1. Avoid Collision

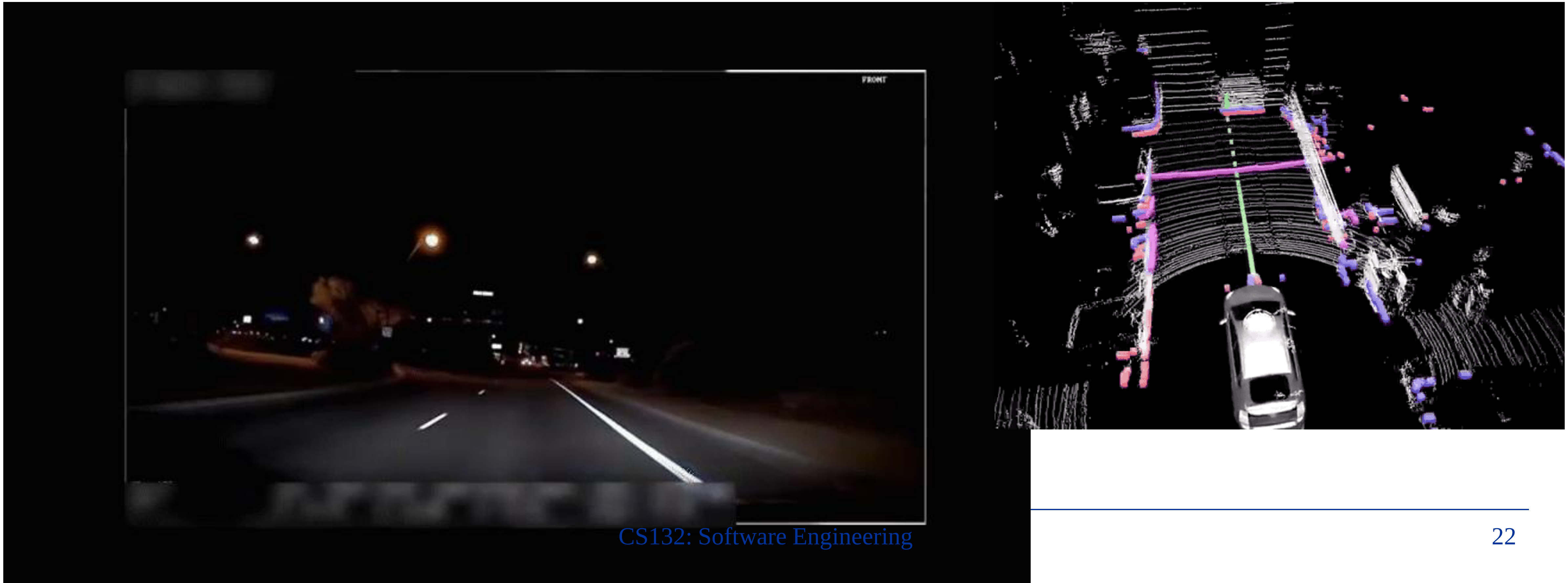
2. Driving on shoulder prohibited

3. Avoid hard brakes



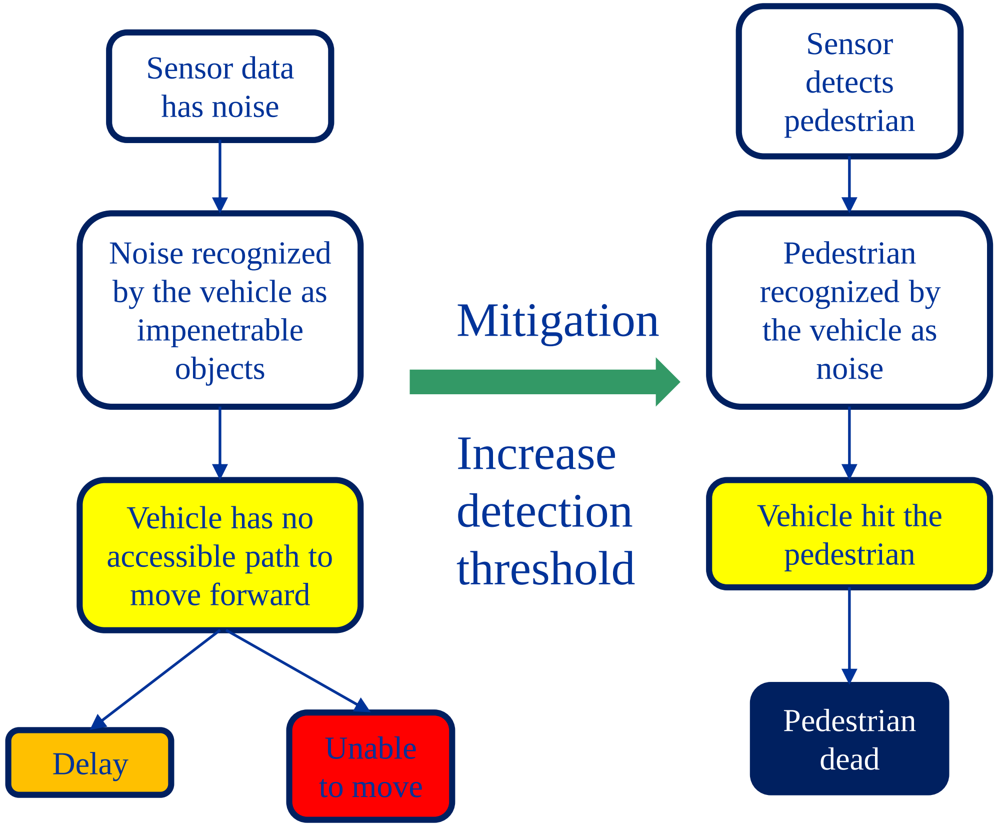
Balancing among risks

- Sometimes, mitigating Risk 1 will make Risk 2 more likely
- Uber Autonomous Vehicle Accident



Uber Autonomous Vehicle Accident

- High frequency * serious harm
- Low frequency * catastrophic harm
- False-positive vs. false-negative
  - Always balance between the two



Sensor data has noise

Noise recognized by the vehicle as impenetrable objects

Vehicle has no accessible path to move forward

Delay

Unable to move

Mitigation

Increase detection threshold

Sensor detects pedestrian

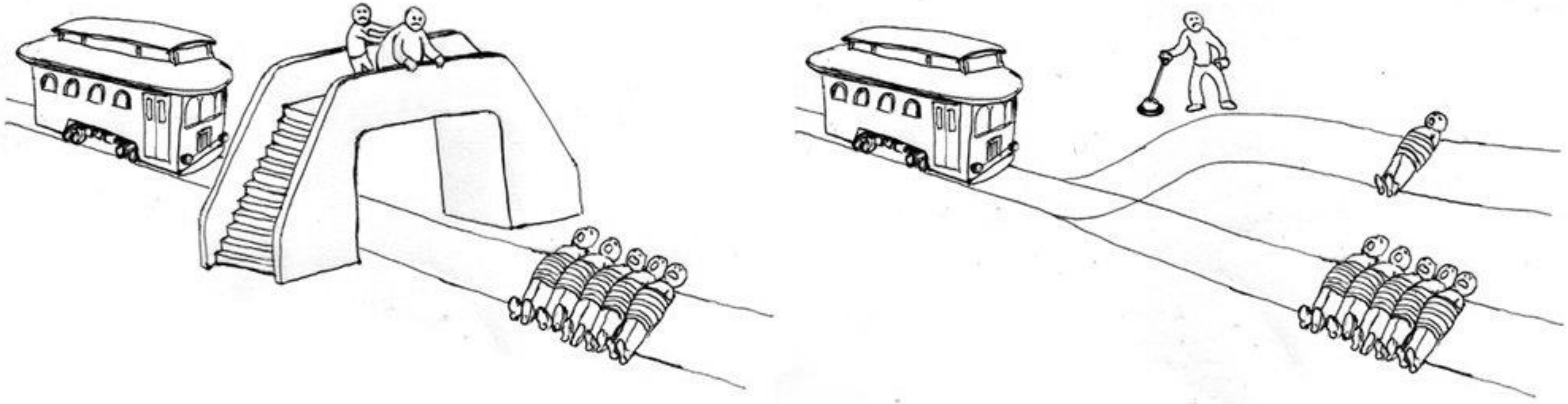
Pedestrian recognized by the vehicle as noise

Vehicle hit the pedestrian

Pedestrian dead

Ethnic considerations when balancing risks

- Choices have to be made
- Invaluable things have to be priced
- For medical applications: Institutional Review Board (IRB)



Risk management vs. Finding bugs vs. Validation

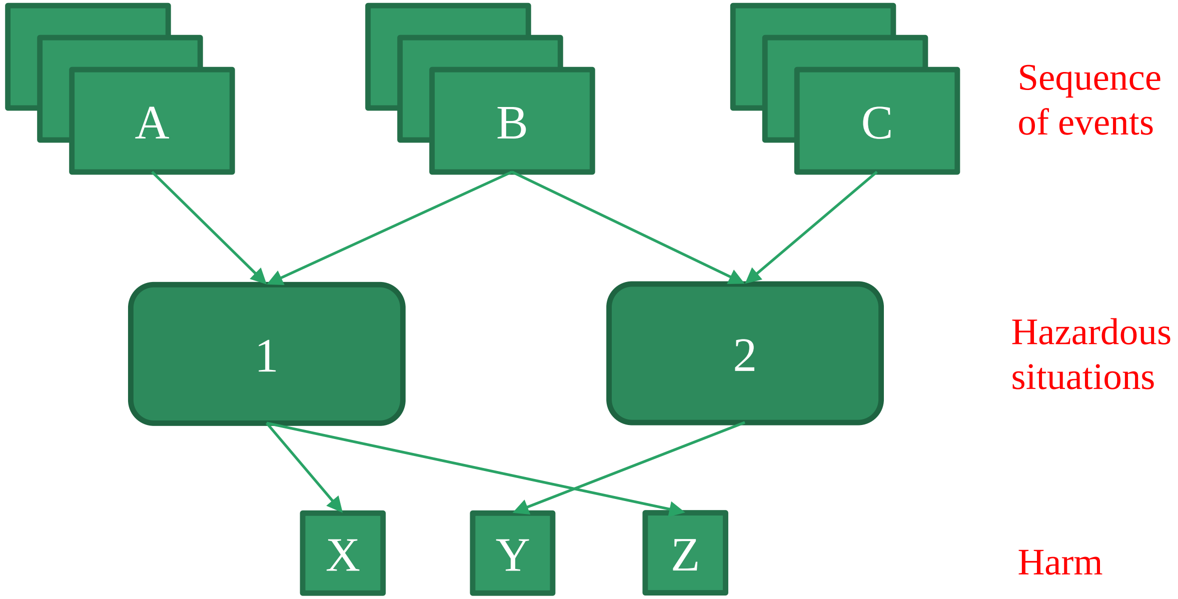
- Risk analysis
  - Finding flaws in design that may cause harm
- Finding bugs
  - Discrepancies when converting design into implementation
  - Verification
- Validation
  - Evaluate whether the design meets the requirements of customers

Identify sequences of events that can lead to hazardous situations

- Hazardous situations are relatively easy to identify

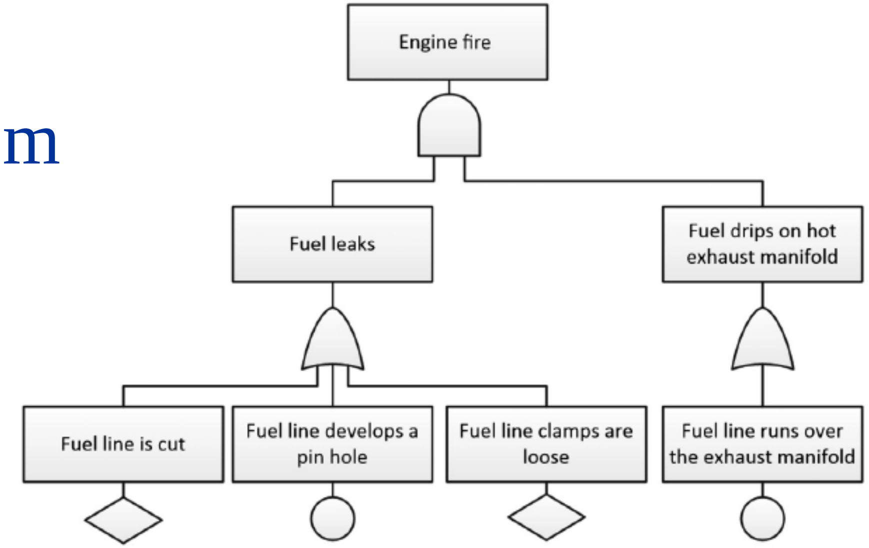
- What are the sequences of events that can lead to the hazardous situation?

- What's the frequency of hazardous situations?



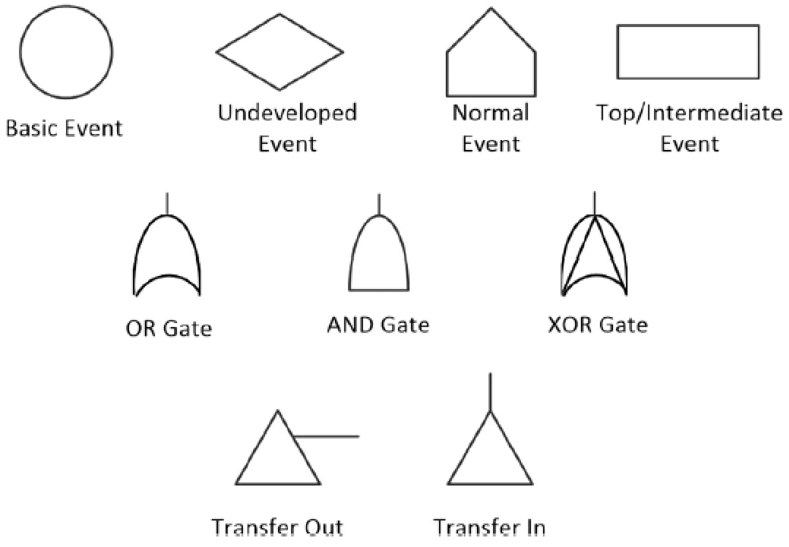
Fault Tree Analysis (FTA)

- Developed by Bell Labs in 1962 during development of the Minuteman missile system
- Later been used in Nuclear Regulation and also NASA
- A deductive top-down reasoning process
  - Starts from the undesired system outcomes
  - Attempts to find out all the credible sequences of events that could result in the undesired system outcomes


Engine fire
Fuel leaks
Fuel drips on hot exhaust manifold
Fuel line is cut
Fuel line develops a pin hole
Fuel line clamps are loose
Fuel line runs over the exhaust manifold

Fault Tree Analysis Symbols

- Basic Event:
  - Requiring no further development
- Undeveloped Event
  - An event that is not further developed due to lack of information, or when the consequences are not important
- Normal Event
  - An event that is normally expected to occur, e.g., the device gets used
- Top/Intermediate Event
  - An event that is further analyzed
- OR Gate
  - Output occurs when one or more of the inputs occur
- AND Gate
  - Output occurs when all of the inputs occur
- XOR Gate
  - Output occurs when only one of the inputs occurs
- Transfer
  - Used to manage the size of the tree on a page, and to avoid duplications

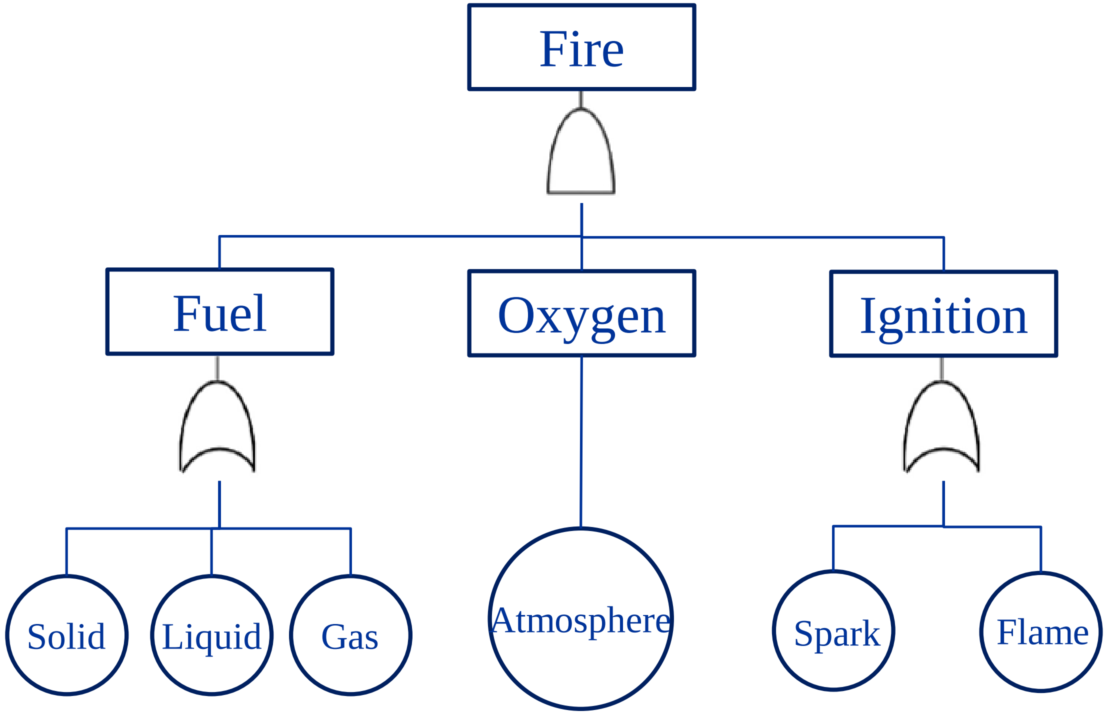


Principles When Identifying the Next Level

- Immediate
  - Is the next event on the lower level, immediately preceding the event in question?
  - Think small/myopically
- Necessary
  - Is the next event on the lower level necessary to cause the fault in question?
  - Avoid entering unnecessary events
- Sufficient
  - Do you have all the necessary events to cause the fault in question?
  - Ensures the higher event can actually happen, given the lower-level events.

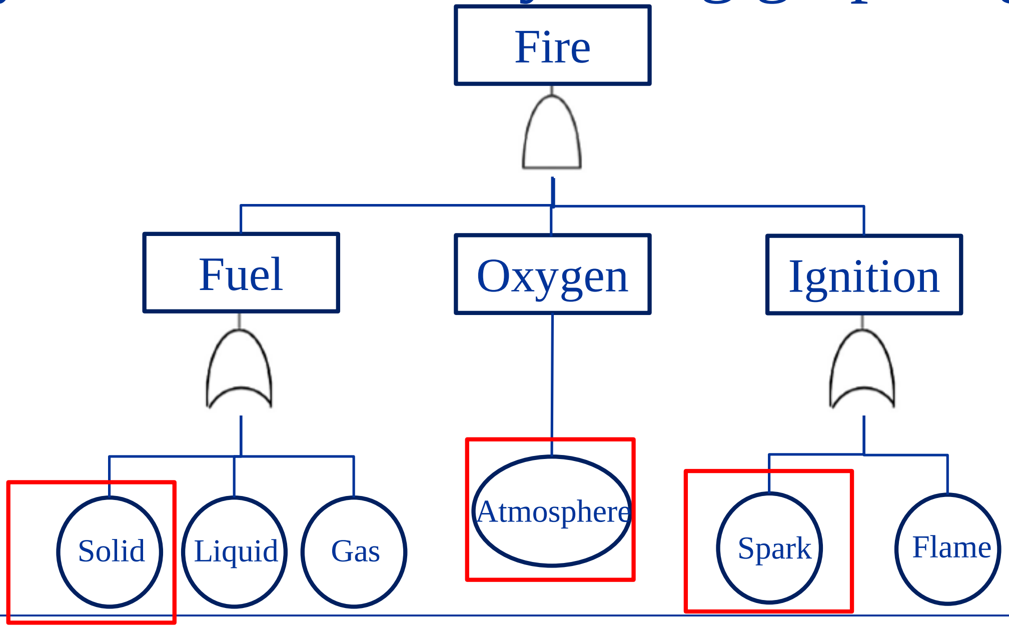
Example

- The hazardous situation “Fire”
  - Requires “Fuel”, “Oxygen” and “Ignition”
  - “Fuel” can be either “Solid”, “Liquid” or “Gas”
  - “Ignition” can be done with either “Spark” or “Other flames”



Qualitative Analysis

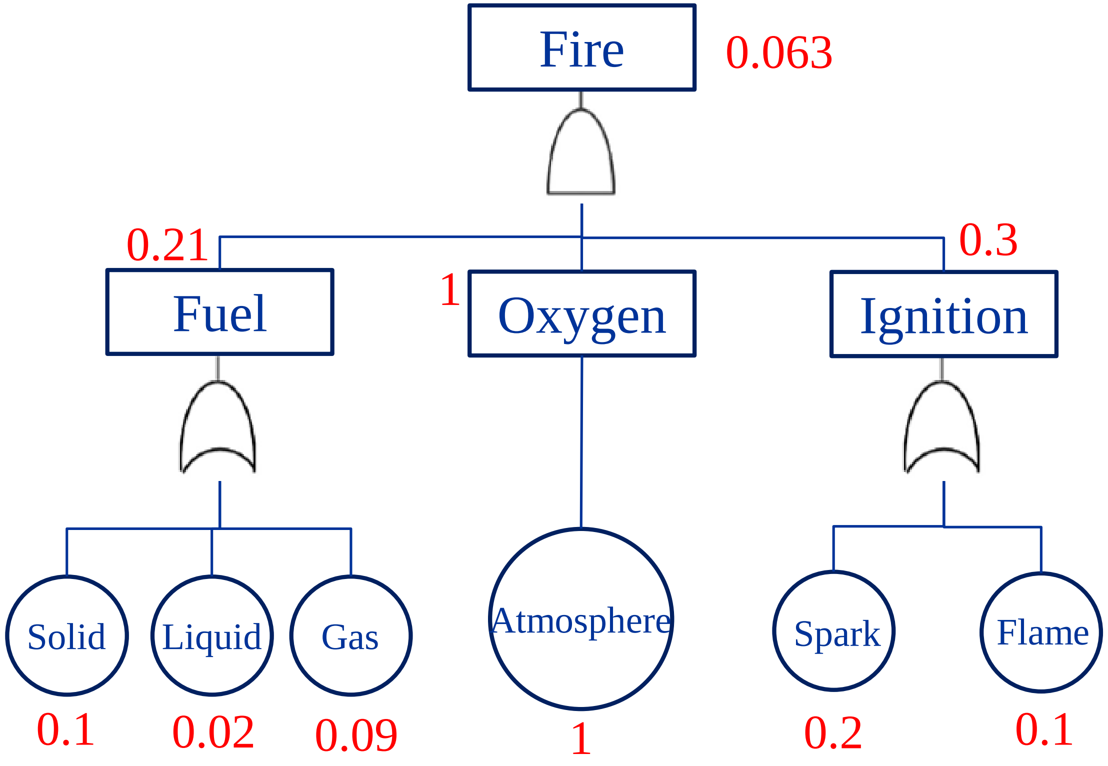
- Minimum Cut Set:
  - The smallest set of basic events, which if they all occur will result in the occurrence of the top event (Not unique)
- Can be analyzed automatically using graph algorithms



Quantitative Analysis

- Probabilities of basic events are measured per certain period
- Add probabilities under the “or” gate
- Multiply probabilities under the “and” gate

- Focus on the “and” gate
  - Only need to bring one down
- Focus on the branches with higher probabilities

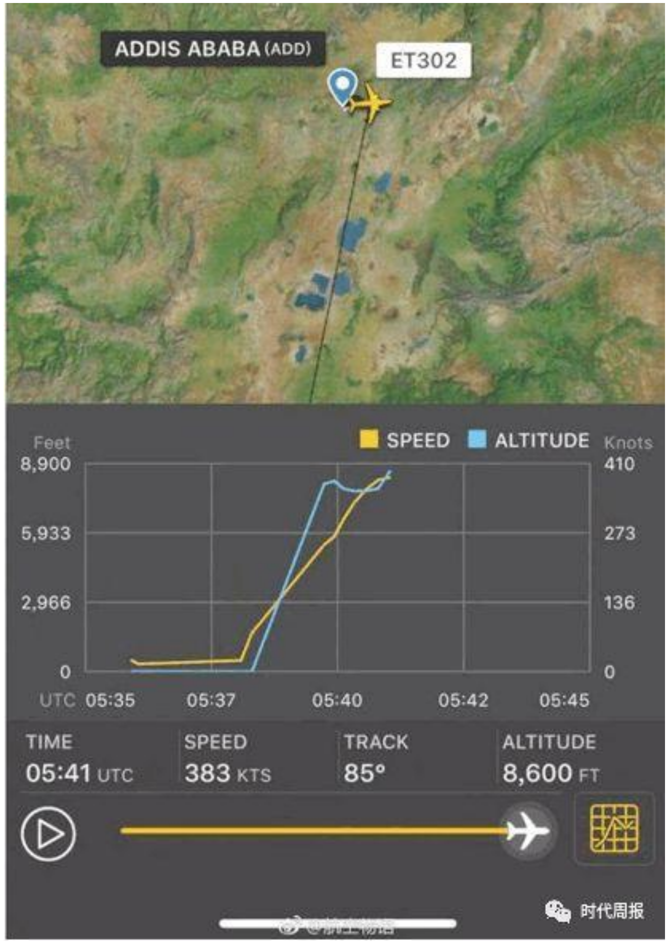


Limitations for FTA

- Can be only used to reason hazardous situations
  - What about other non-safety related qualities i.e. reliability?
- The analysis may not be exhaustive
  - There can be sequences of events that were not identified

Ethiopian airline crash

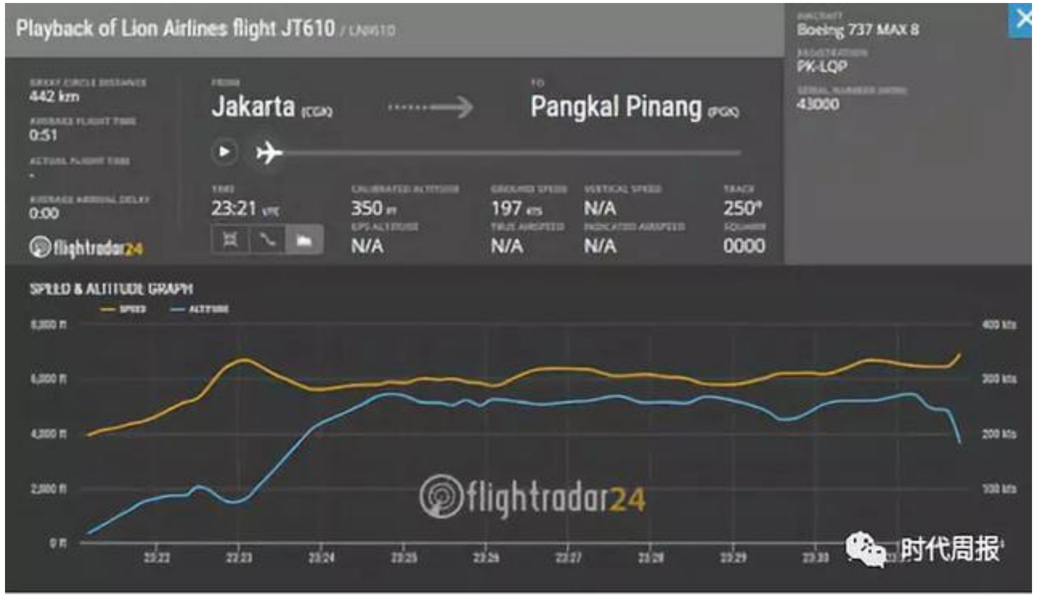
- Flight ET302 from Addis Ababa for Nairobi
- Crashed on March 10, 2019
- Crashed 6 mins after takeoff
- All 157 people on board died
- Boeing 737-Max 8



TIME 05:41 UTC
SPEED 383 KTS
TRACK 85°
ALTITUDE 8,600 FT

Similar Crash

- Lion Airline JT610 Oct 29, 2018
- Crashed 12 mins after takeoff
- All 189 people on board died



Playback of Lion Airlines flight JT610 / LNI610

GREAT CIRCLE DISTANCE
442 km
AVERAGE FLIGHT TIME
0:51
ACTUAL FLIGHT TIME
-
AVERAGE ARRIVAL DELAY
0:00

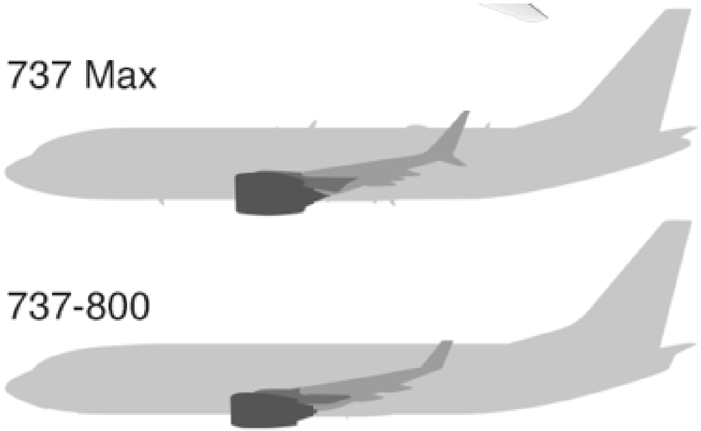
FROM
Jakarta (CGK)
TO
Pangkal Pinang (PGK)

TIME
23:21 UTC
CALIBRATED ALTITUDE
350 FT
GPS ALTITUDE
N/A
GROUND SPEED
197 KTS
TRUE AIRSPEED
N/A
VERTICAL SPEED
N/A
INDICATED AIRSPEED
N/A
TRACK
250°
SQUAWK
0000

AIRCRAFT
Boeing 737 MAX 8
REGISTRATION
PK-LQP
SERIAL NUMBER (MSN)
43000

Boeing 737 Max 8/9

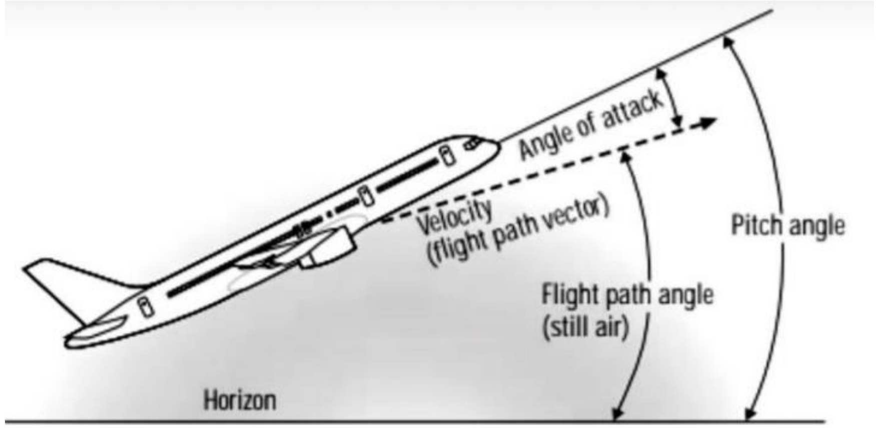
- The Max’s engines were bigger and mounted farther upward on its wings

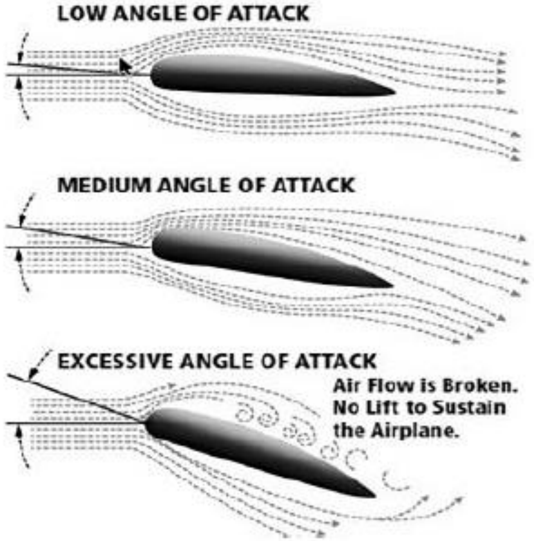


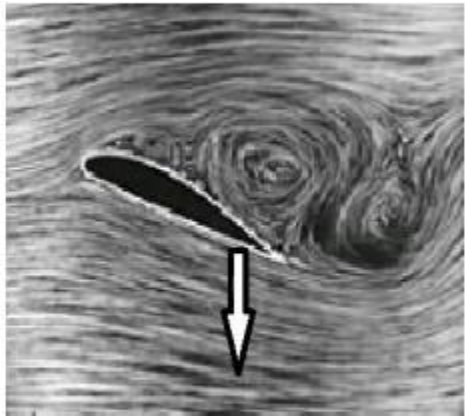
The Boeing 737 Max has larger engines than earlier models

Stall

- Angle of attack (AOA): the angle between velocity vector and a line along the fuselage
- High AOA results in stall, which leads to crash
- The new engine configuration of 737 max makes it more likely to have high AOA

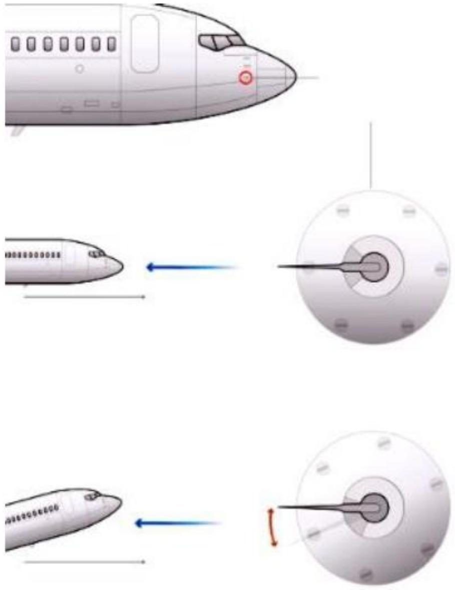




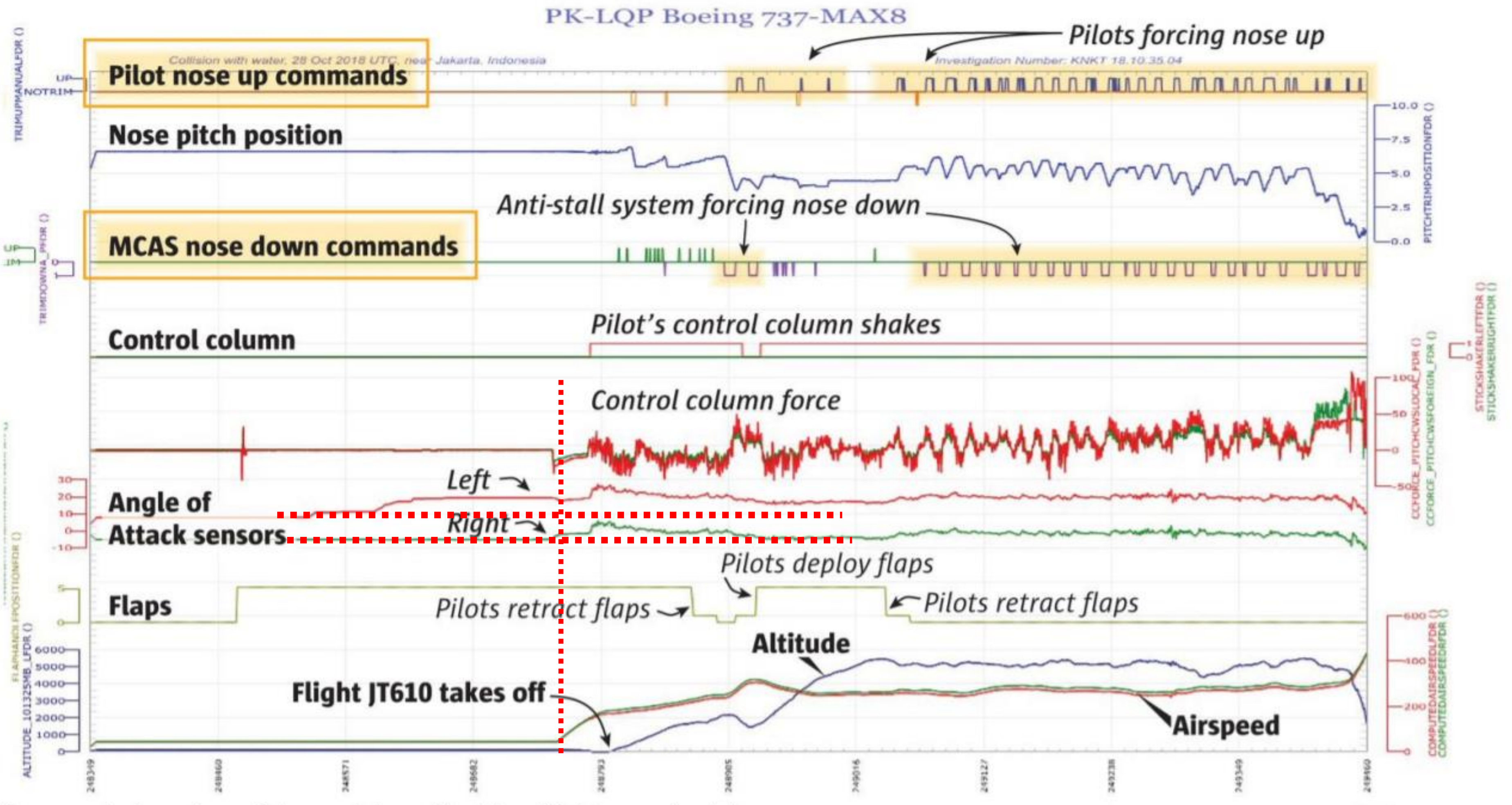


Maneuvering Characteristics Augmentation System (MCAS)

- MCAS to automatically push the nose down after detecting high AOA
- Two AOA sensors mounted at the head of the aircraft
- MCAS activates if one of the two AOA sensors says the AOA is too high.

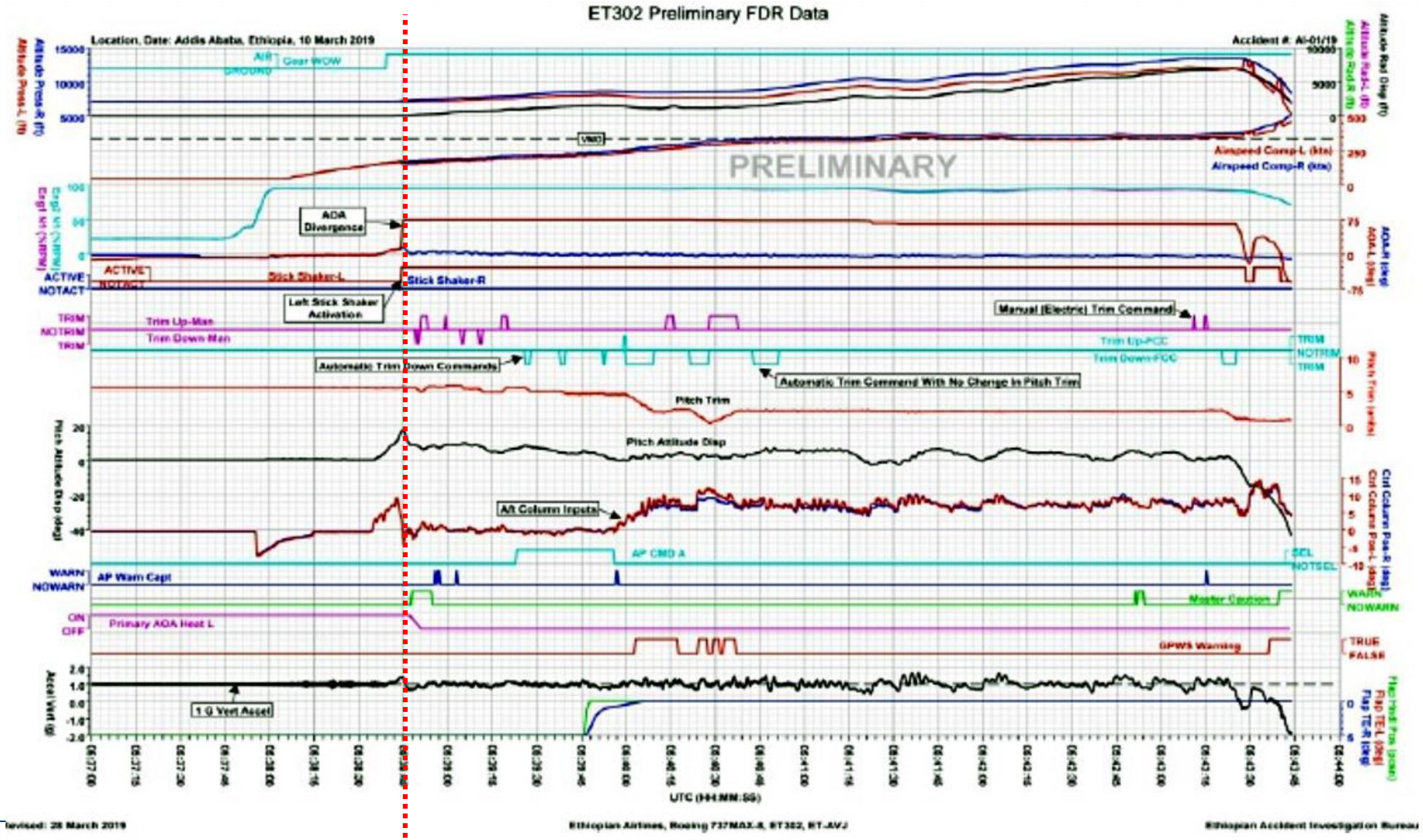


Lion JT610 Flight Data Recording



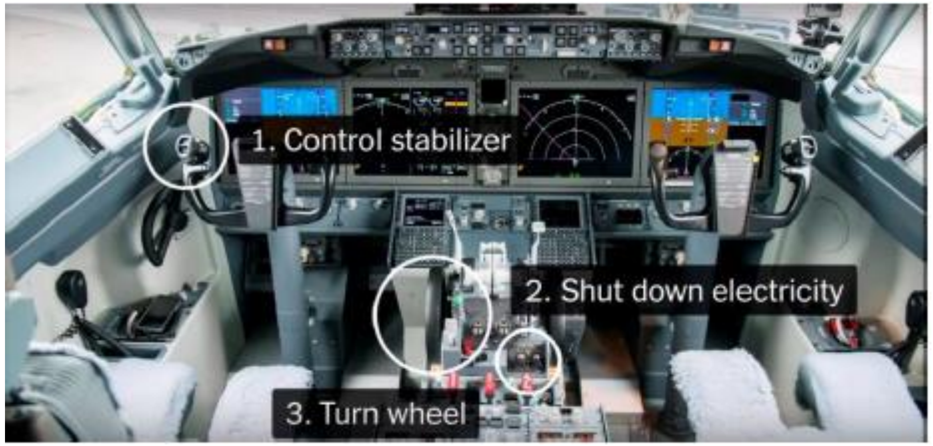
Sources: Indonesian safety regulators, black box flight recorder data

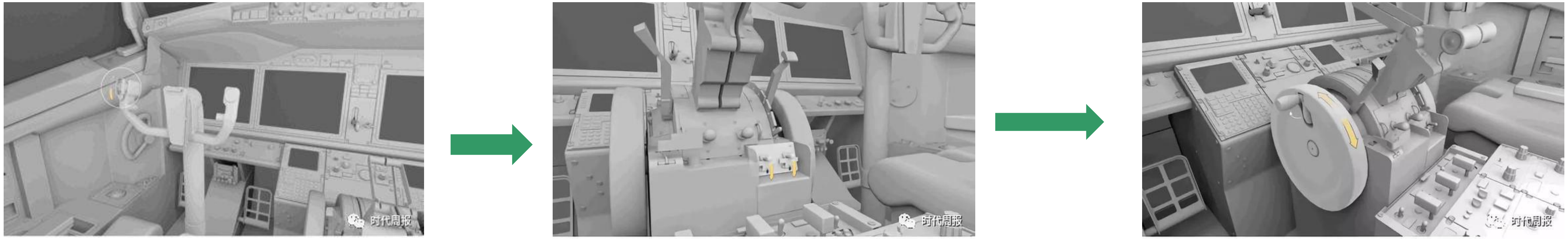
ET302 Flight Data Recording



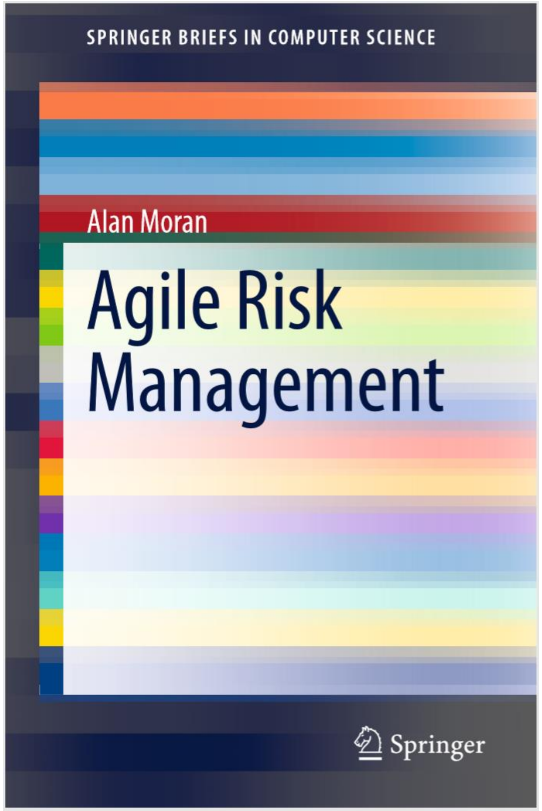
How to override MCAS?

- It’s not easy…
- Provided instructions to the pilots on how to turn off MCAS





- Available from library website

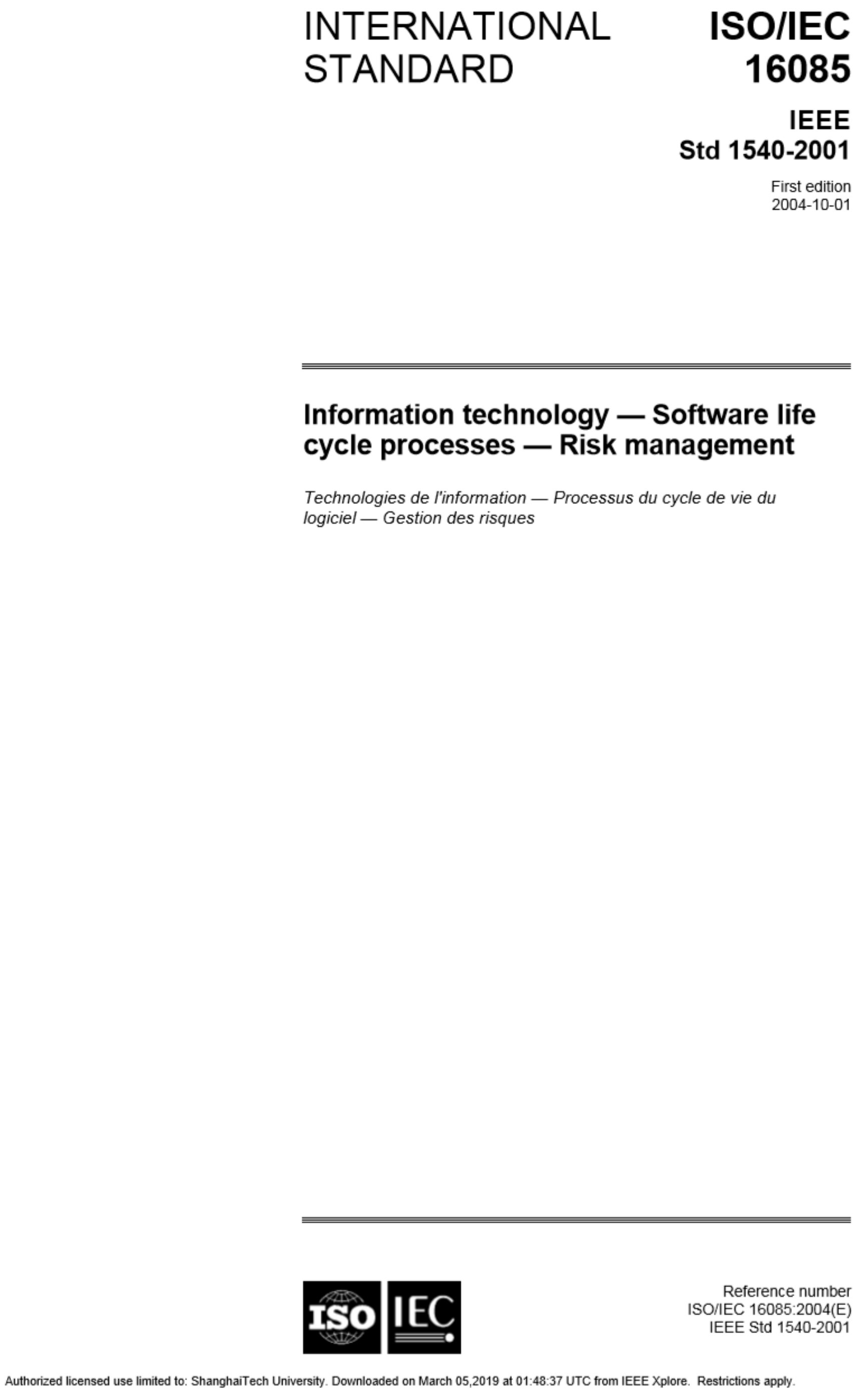


SPRINGER BRIEFS IN COMPUTER SCIENCE

Alan Moran

Agile Risk Management

Springer



INTERNATIONAL STANDARD

ISO/IEC 16085

IEEE Std 1540-2001

First edition
2004-10-01

Information technology — Software life cycle processes — Risk management

Technologies de l'information — Processus du cycle de vie du logiciel — Gestion des risques

Reference number
ISO/IEC 16085:2004(E)
IEEE Std 1540-2001