Leading Indicators Based on STAMP

Nancy Leveson

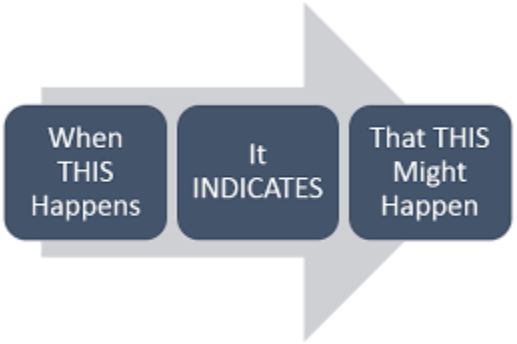
Topics

- What is a leading indicator? Why do we need them?
- What do people do now for leading indicators?
- A new approach that starts from a new definition
- How to create effective leading indicators and integrate them into your risk management program
- Is this new approach feasible?

Why do accidents occur?

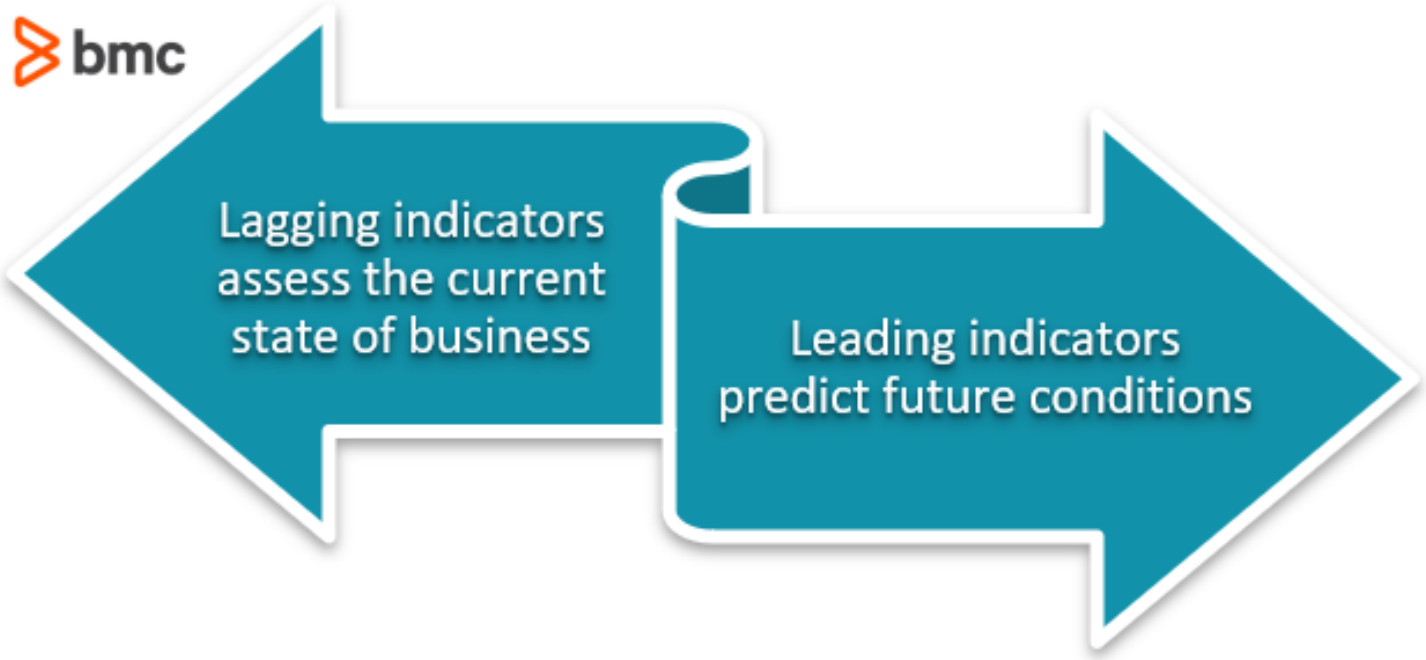
What is a Leading Indicator?

- Identifies potential for an accident before it occurs
- Underlying assumption:
  - Major accidents not due to a unique set of random, proximal events
  - Instead result from
    - Migration of system/organization to state of increasing risk over time
    - As safeguards and controls relaxed
    - Due to
      - conflicting goals and tradeoffs and
      - reduced perceptions of risk
    - Leading to more risky behavior



- Def: A signal that intervention is necessary

Lagging vs. Leading Indicators



Current State of the Art: Industry

- Much effort, particularly in petrochemicals
  - Trying to find generally applicable indicators

    e.g., maintenance backlogs, minor incidents, equipment failure rates, surveys on employee culture (assumes that all or most accidents caused by operator/worker misbehavior)

  - Tend to focus on workplace safety
  - May try to identify leading indicators from hazard analysis
    - Use standard techniques so limited types of causes (mostly failures)
    - Use likelihood to reduce scope of search
      - May result in overlooking low likelihood events

Heuristic Biases (Tversky, Slovic, and Kahneman)

- Confirmation bias (look for data that supports our beliefs)
- Construct simple causal scenarios
  - If none comes to mind, assume impossible
- Tend to identify simple, dramatic events rather than events that are chronic or cumulative
- Incomplete search for causes
  - Once one cause identified and not compelling, then stop search
- Defensive avoidance
  - Downgrade accuracy or don't take seriously
  - Avoid topic that is stressful or conflicts with other goals

Controlling Heuristic Biases

- Cannot eliminate completely but can reduce
- Use structured method for identifying, detecting, and managing leading indicators
  - Following a structured process and rules to follow can diminish power of biases and encourage more thorough search
  - Concentrate on causal mechanisms vs. likelihood
- Use worst case analysis (vs. most likely or “design basis accident”)

Why Do Accidents Occur?

Why do Accidents Occur?
Why are Dangerous Products Produced?

Design and Manufacturing

- Inadequate hazard analysis
  - Not performed or not completed
  - Some hazards not identified due to inadequacies in hazard analysis process
  - Hazards identified but not handled because assumed to be "sufficiently unlikely" (and even ignore data to show it happened)
- Inadequate design of control and mitigation measures
  - Inadequate engineering knowledge
  - Inappropriate assumptions about operations
- Inadequate construction of control and mitigation measures

Why do Accidents Occur? (2)

Operations

- Controls assumed will exist do not, are not used, or turn out to be ineffective
- Controls exist and are used and originally were effective, but changes over time violate the assumptions underlying their design
  - New hazards arise with changing conditions, were not anticipated during development, or were dismissed as unlikely to occur
  - Physical controls degrade over time in unanticipated ways
  - System components (including humans) behave differently over time (which violate assumptions made during design, analysis, and test)
  - System environment changes over time (violates assumptions made during analysis and design)

Why do Accidents Occur? (3)

Management

- Safety management system is flawed
  - E.g, focus on measurement rather than control
  - The goal of an SMS is to prevent accidents, not to predict them
- SMS could be effective, but does not operate the way it was designed and assumed to operate
  - Safety culture (goals and values of organization with respect to safety)
    - Ineffective from beginning
    - Degrades over time
  - Assumptions were flawed
  - Behavior of those making safety-related decisions influenced by competitive, financial, or other pressures

World is Continually Changing

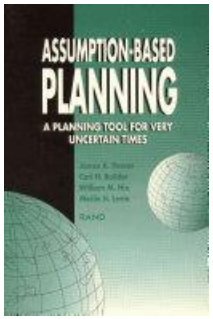
- Accidents usually happen after changes
- Planned vs. unplanned changes
- Changes within system and in environment

CHANGE IS INEVITABLE, EXCEPT FROM A VENDING MACHINE.

Assumption-Based Planning

- James Dewar, Rand
  - A Tool for Preventing Avoidable Surprises

  - A Planning Tool for Uncertain Times



- Used to help the U.S. Army in mid-term and long-term defense planning
- To reduce uncertainty and manage risk in Army missions

Assumption-Based Leading Indicators

Argument:

Useful leading indicators of increasing risk can be identified based on the assumptions underlying the safety design process for the specific organization, product, or operations.

- All engineering involves assumptions about behavior of the operational system and its environment (including organizational or management structure)
- Our accident avoidance is based on those assumptions.
- When the assumed behavior changes, then more likely to have an accident.

Common Assumptions in System Safety

- Failure rates for a hardware component over time
- What software needs to do
- How product will be used, environment in which used or services are provided
- Basic training for people on tools they are tasked to use
- Information needs for decision making and how effectively information channels operate
- Beliefs about what customers want and need, which can change over time as marketplace changes
- Etc.

Three General Types of Assumptions

1. Models and assumptions used in design are correct.
2. System will be constructed and operated in manner assumed by designers
3. Original models and assumptions are not violated
   a. By changes to system over time, perhaps to improve or optimize the processes,
   b. By changes in the environment

Assumption-Based Leading Indicators

- Accidents occur when these assumptions are wrong
  - Originally incorrect
  - Become incorrect over time
- So detect when assumptions are starting to fail
- Base leading indicators on the assumptions made when designing system to be safe.

Goals

- Identify appropriate and effective assumption-based leading indicators
- Create a leading indicators monitoring program
- Embed monitoring program within a well-designed risk management program.
  - Detection not enough
  - Must be a management process in place to act when leading indicators show action is necessary.

Identification

Monitoring

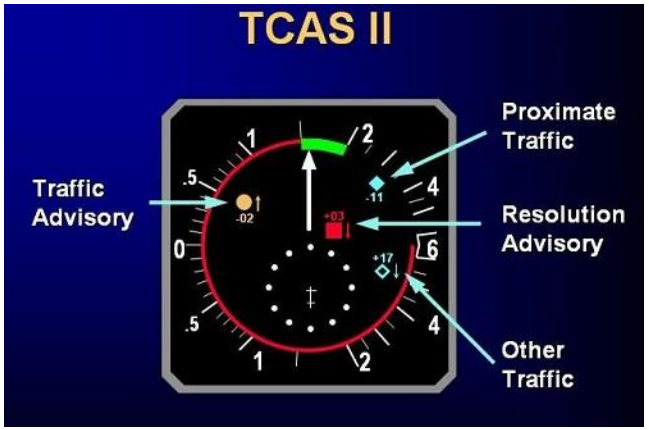
Reacting Appropriately

Identifying Leading Indicators

Documenting Assumptions During System Engineering

Example: Intent Specification for TCAS

- Critical part of intent specs is to document assumptions under which system is built and on which safety is based.
- Example done by myself with a student (who built a formal model)
- Causal scenarios were generated by a qualitative hazard analysis



System Goals and High-Level Requirements

G1: Provide affordable and compatible collision avoidance system options for a broad spectrum of National Airspace System (NAS) users.

G2: Detect potential midair collisions with other aircraft in all meteorological conditions; throughout navigable airspace, including airspace not covered by ATC primary or secondary radar systems, and in the absence of ground equipment.

1.18: TCAS shall provide collision avoidance protection for any two aircraft closing horizontally at any rate up to 1200 knots and vertically up to 10,000 feet per minute [G1].

> *Assumption: This requirement is derived from the assumption that commercial aircraft can operate up to 600 knots and 5000 feet per minute during vertical climb or controlled descent and therefore two planes can close horizontally up to 1200 knots and vertically up to 10,000 fpm.*

Another High-Level Requirement

1.19.1: TCAS shall operate in enroute and terminal areas with traffic densities up to 0.3 aircraft per square nautical miles (i.e., 24 aircraft within 5 nmi) [G2].

> *<u>Assumption</u>: Traffic density may increase to this level by 1990, and this will be the maximum density over the next 20 years.*

Environmental Assumptions

EA1: High-integrity communications exist among aircraft

EA2: The TCAS-equipped aircraft carries a Mode-S air traffic control transponder.

EA3: All aircraft have operating transponders

EA4: All aircraft have legal identification numbers

EA5: Altitude information is available from intruding targets with a minimum precision of 100 feet.

EA6: The altimetry system that provides the aircraft's pressure altitude to the TCAS equipment will satisfy the requirements in RTCA Standard …

EA7: Threat aircraft will not make an abrupt maneuver that thwarts the TCAS escape maneuver.

Using Assumptions to Create an Assumption-Based Leading Indicator Program

Ways to Enforce Assumption-Based Leading Indicators

- Shaping actions: prevent violation of assumptions
- Hedging actions: prepare for failure of an assumption
- Assumption checking during operations
  - *Planned changes*: Signposts, MoC procedures
  - *Unplanned changes* (checks can be periodic or continual)
    - Performance audits
    - Surveys
    - Automatically collected data (e.g., FOQA)

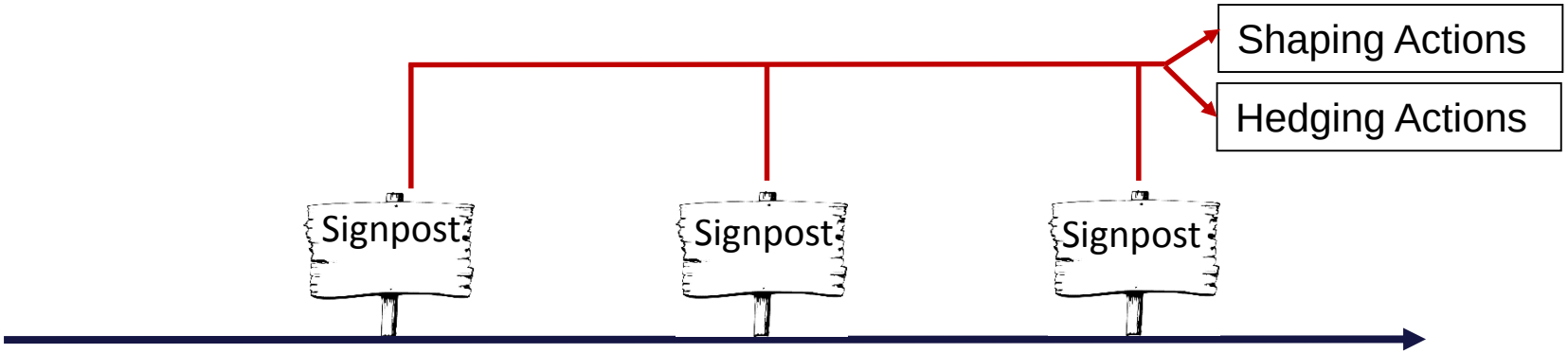
Handling Assumption-Based Leading Indicators

- **Shaping Actions**
  - Used to maintain assumptions, prevent hazards, and control migration to states of higher risk, e.g.,
    - Interlocks
    - Dessicant to prevent corrosion
    - Design human operation to be easy and hard to omit
  - Feedforward control

- **Hedging (Contingency) Actions**
  - Prepare for possibility an assumption will fail
  - Generate scenarios from broken assumptions (worst case analysis) to identify actions that might be taken
  - Feedback control
  - Examples:
    - Performance audits
    - Fail-safe design (e.g., protection and shutdown systems)
- **Signposts**
  - Points in future where changes in safety controls (shaping and hedging actions) may be necessary or advisable
  - Examples: New construction or known future changes may trigger a planned response or MoC action

- **Assumption Checking**
  - Checking whether assumptions underlying safety design are still valid
  - Monitor operations to determine if assumptions still valid
  - Might focus on signposts or on assumptions that have not been adequately handled by shaping and hedging actions
  - Accidents most often occur after a change
    - MOC procedures can be used for planned changes
    - Signposts can be used for expected but unplanned changes
    - Assumption checking used for detecting unexpected, unplanned, and potentially unsafe changes
  - Predicated on observation that always lots of incidents before a major accident.

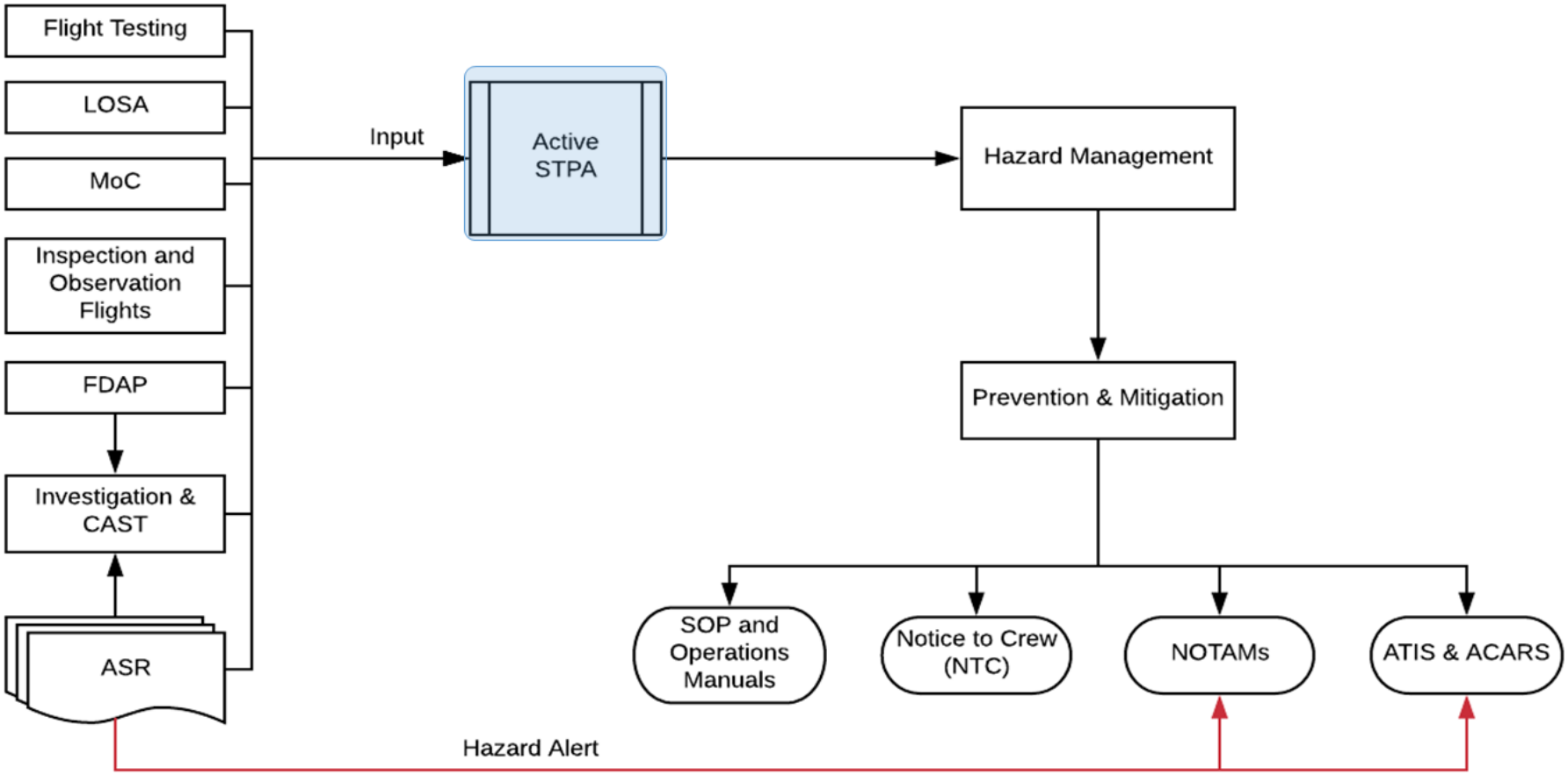
Combining Actions



Assumption checking

Using STPA to Analyze Operational Events

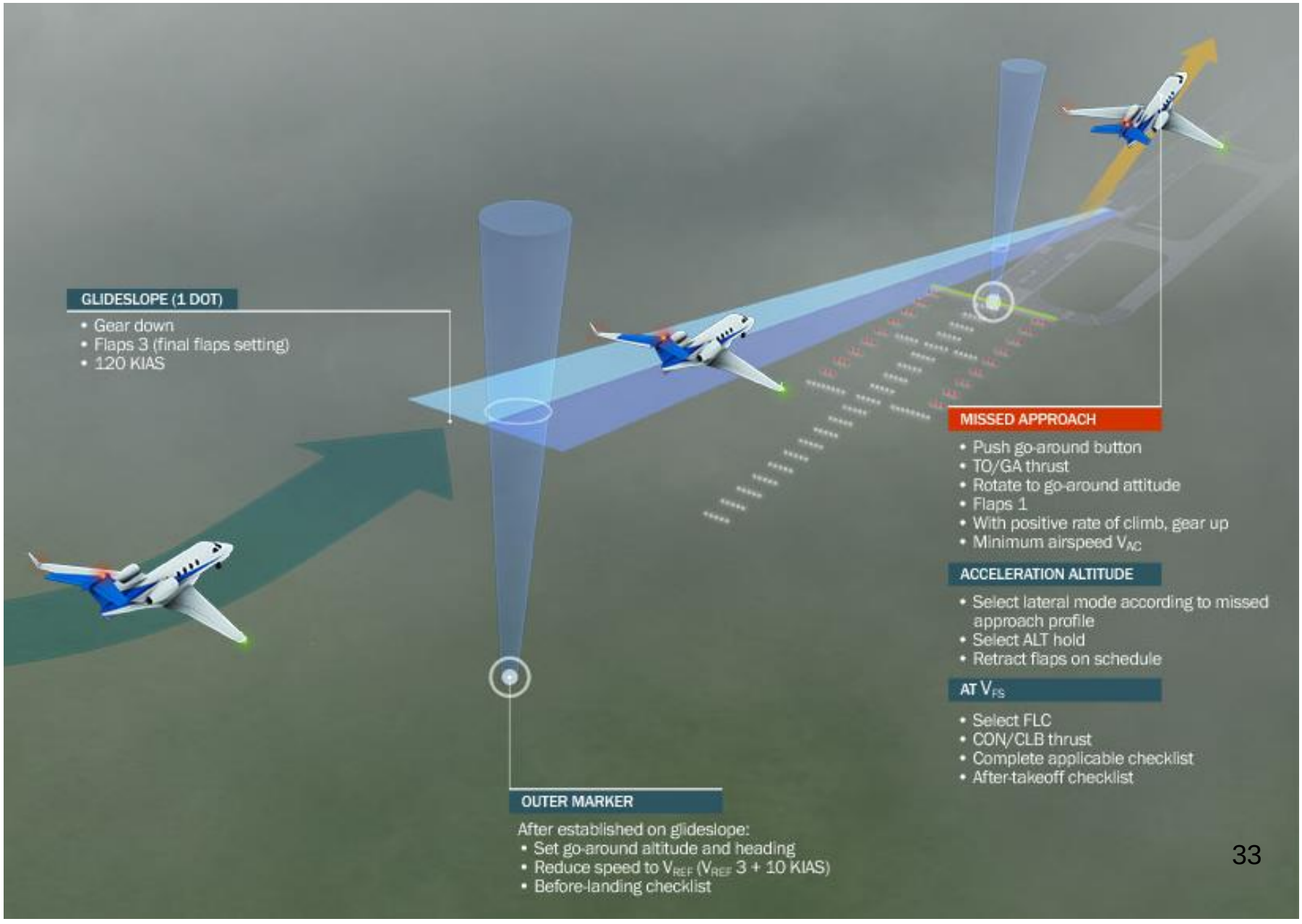
- Dissertation by Dr. Diogo Silva Castilo (MIT, 2019)
- Active STPA
  - Uses operational data and development activities to identify why events (leading indicators) occurred
  - Step-by-Step process to examine STPA analysis to determine why not identified or prevented during development
  - Output is a set of new defenses



Four Processes:

- P1 - Communication protocol for sensitive data
- P2 - Active Hazard Analysis update
- P3 – Hazard Management
- P4 – Prevention & Mitigation

Missed Approach Example



STPA

1. Define the Purpose of the Analysis

a. Identify Losses

b. Identify System-level Hazards

c. Identify System-level Safety Constraints

d. Refine Hazards (optional)

2. Model the Control Structure

3. Identify Unsafe Control Structure

a. Not providing causes hazard

b. Providing causes hazards

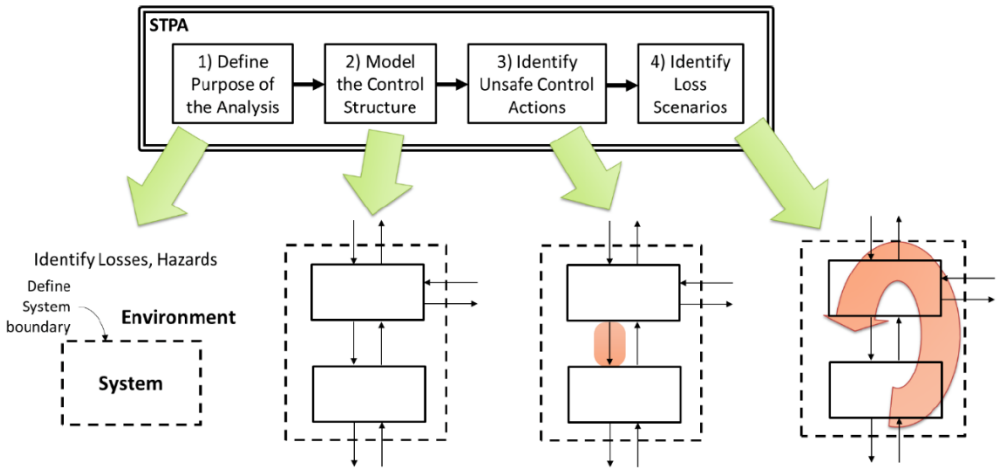
c. Too early, too soon, out of order

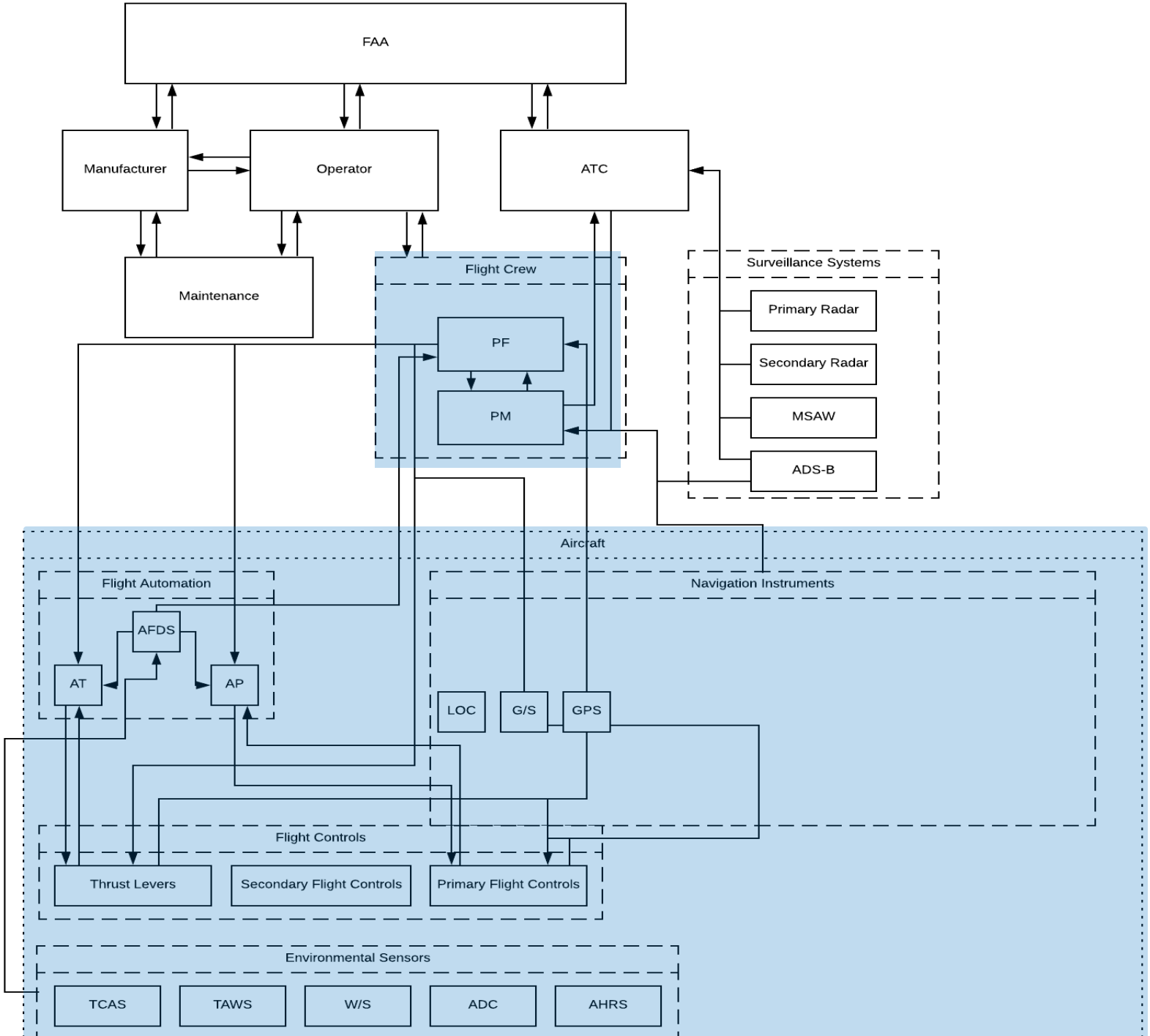
d. Stopped too soon, applied too long

4. Identify Loss Scenarios

a. Unsafe controller behavior

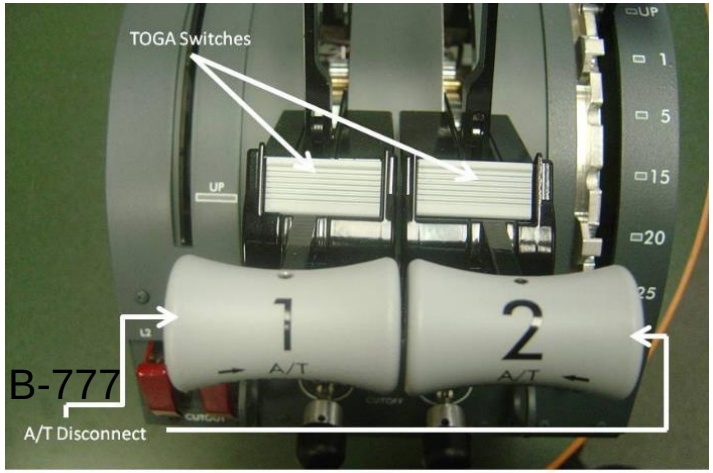
b. Causes of inadequate feedback and information




FAA
Manufacturer
Operator
ATC
Maintenance
Flight Crew
PF
PM
Surveillance Systems
Primary Radar
Secondary Radar
MSAW
ADS-B
Aircraft
Flight Automation
AFDS
AT
AP
Navigation Instruments
LOC
G/S
GPS
Flight Controls
Thrust Levers
Secondary Flight Controls
Primary Flight Controls
Environmental Sensors
TCAS
TAWS
W/S
ADC
AHRS

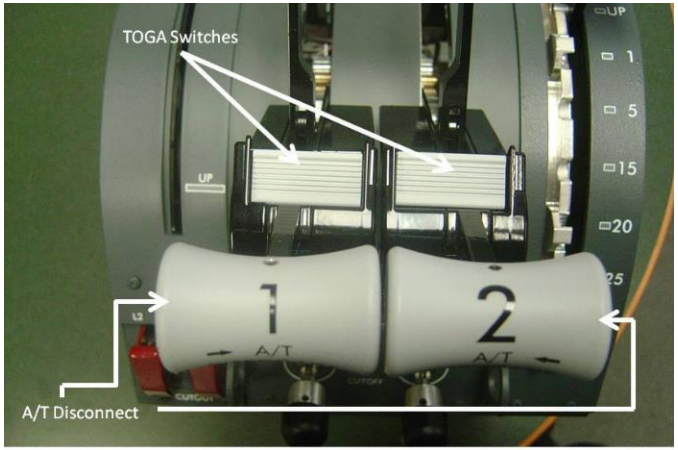
Original STPA Analysis

Controller	Process	Switch / Selector	Control Actions	Unsafe Control Actions											
				Provided causes Hazard			Not Provided causes Hazard			Applied for too long or too short			Wrong timing or order		
				UCA	Hazards	Description	UCA	Hazards	Description	UCA	Hazards	Description	UCA	Hazards	Description
Crew	AP	TO/GA	Press TO/GA	27	H2	Pressing TO/GA button after touchdown (it is inhibited)	28	H1.1 H3	Not pressing TO/GA when approach is unstable		-	N/A	29	H2	Pressing TO/GA after raising the nose



Scenario	Constraint
After a long flight, the approach becomes unstable and the PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TOGA switches because pilots are fatigued	Crew must press TO/GA when approach is unstable

Assumption-based Leading Indicator Example

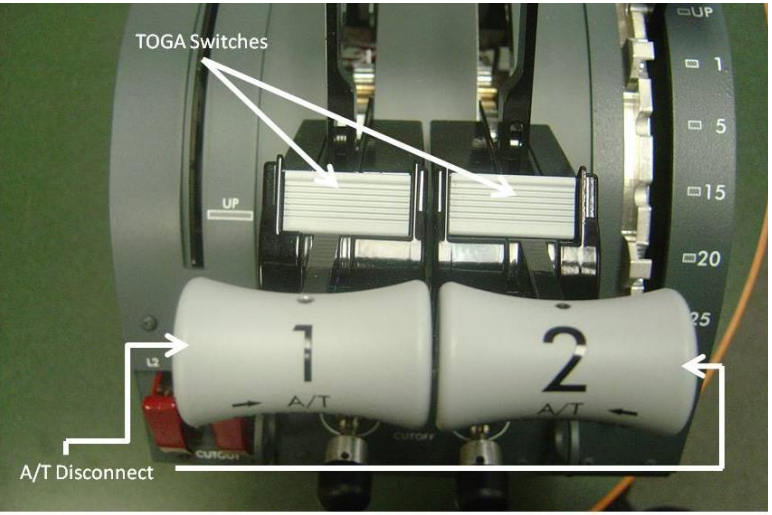


B-777

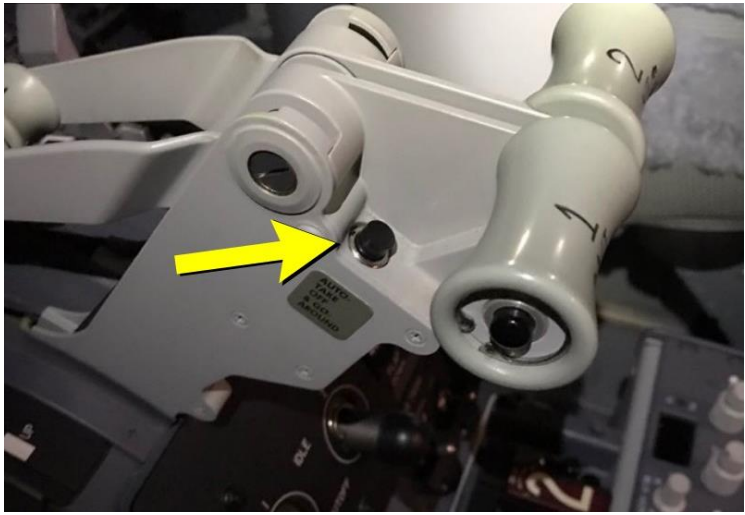
Scenario	Constraint
After a long flight, the approach becomes unstable and the PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TOGA switches because pilots are fatigued	Crew must press TO/GA when approach is unstable

Assumption	Mitigating Measure	Lagging Indicator	Monitor	Frequency
This mistake is unlikely to happen because the format of A/T disconnect button is very different from the TOGA switches and they are far from each other	Five Missed Approach trainings on Simulators per year	Collect statistics of how many pilots had this kind of confusion	Survey	Once a year

Go Around Button



B-777



B-737

B-767

Basic Aircraft

When a Leading Indicator shows a Broken Assumption

Old

Scenario	Constraint
PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TOGA switches because pilots are fatigued	Crew must press TO/GA when approach is unstable

Assumption	Mitigating Measure	Leading Indicator	Monitor	Frequency
This mistake is unlikely to happen because the format of A/T disconnect button is very different from the TOGA switches and they are far from each other	Five Missed Approach trainings on Simulators per year	Run statistics of how many pilots had this kind of confusion	Survey	Once a year

New

Scenario	Constraint
PF (Pilot Flying) decides to Go Around and, by mistake, presses the A/T disengagement button instead of the TOGA switches **because this button in B777 is at the same position as the GA button in the PF previous operational aircraft**	Crew must press TO/GA when approach is instable

Assumption	Mitigating Measure	Leading Indicator	Monitor	Frequency
This is a common mistake in pilots transitioning to the B777 with large experience in commuter aircraft, but it can be mitigated with training and it is safe to operate if another pilot is monitoring	Eight Missed Approach trainings on Simulators per year A Note on manual alerting to this mistake Alert flight instructors about verifying if pilots are pressing TO/GA switches correctly	Observe in Simulator trainings signs of confusion Include item on observation flights	Instructor Sim and flight Reports	Every training

Examples of Assumptions in Other Types of Systems

- Shell Moerdijk: catalyst will not change over time and will remain inert. [Explosions happened twice before big one at Moerdijk]
- Healthcare Adverse Event: Heart transplant patient not given immunosuppressant before surgery and rejected it
  - Had not done heart transplants at this hospital for some time (a change)
  - Assumptions (and confusion) about who would give the immunosuppressant
  - EHR design did not provide surgeons with information they needed in a form that could be used. Assumed medication had been given but no easy way to check

Examples of Assumptions in Other Types of Systems (2)

- Assumptions about what happened during handoffs from CCU to surgical team
- Assumption that nursing staff would be familiar with procedure
- Assumption that nursing staff in CCU would be well trained (changes in budgets and staff resources)
- Responsibilities will be documented and communicated
- We found similar incorrect assumptions in other adverse events related to cardiac surgery at this hospital

Integrating Leading Indicators into your Risk Management Program

Managing a Leading Indicators Program

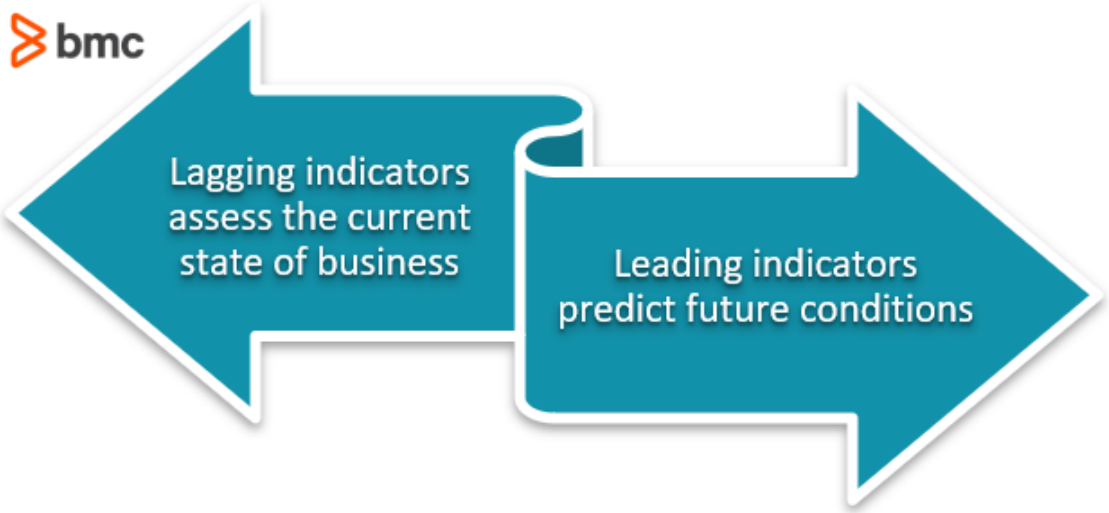
- Integrate into risk management program
- Communicate to decision makers when assumption fails
- Develop detailed action plans and triggers for implementing them before assumptions found to be invalid
  - To lessen denial and avoidance behavior
  - To overcome organizational and cultural blinders
- May need to assign responsibility to independent organization and not project managers or those with conflicting pressures
- Periodically revisit list of leading indicators. Establish a continuous improvement process

Feasibility Considerations

- Most assumptions identified and considered during development so just need to document them.
- I've done it for TCAS II (technical) and NASA ITA program (management)
- Hazard analysis is expensive itself
  - People use PRA to reduce analysis and design costs. But impossible to know the probability except for simple hardware failures.
  - STPA turning out to be much cheaper than older methods. Accidents/incidents are also expensive
  - Many assumptions will be handled in design or do not need to be checked continually. Signposts may trigger checks.
- Documenting assumptions is important for creation, maintenance, and evolution of systems, not just safety

SUMMARY

- Lagging vs. Leading indicators



- New definition: Assumption-Based Leading Indicators
- Create risk management system that supports

Identification
Monitoring
Reacting Appropriately

Thank you!

Questions?