# Leading Indicators Based on STAMP

Nancy Leveson

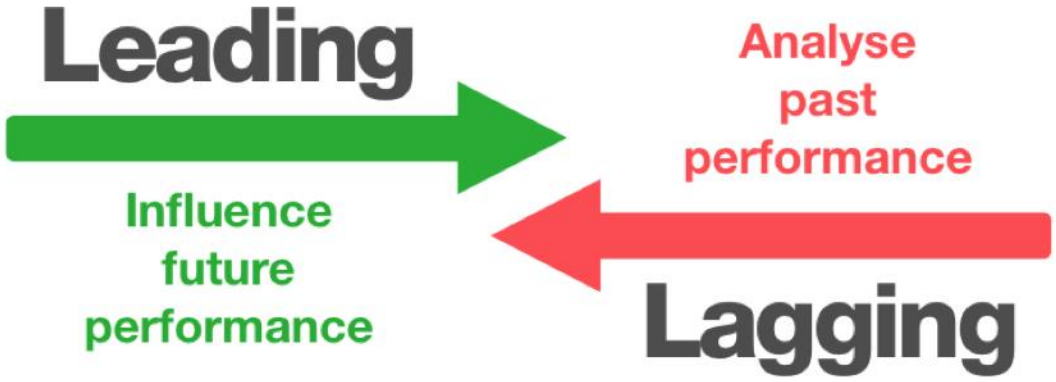

# Topics:

- What is a leading indicator?
- What do people do now for leading indicators?
- What are assumption-based leading indicators?
- How to:
  - Identify appropriate and effective leading indicators using STAMP and STPA
  - Generate assumptions on which to base leading indicators
  - Use the assumptions to create an “assumption-based leading indicator program”
  - Integrate the leading indicators program into your risk management program
- Feasibility

# 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
- 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 occupational safety
  - May try to identify of leading indicators from hazard analysis
    - Use standard techniques so limited types of causes
    - Use likelihood to reduce scope of search
      - May result in overlooking low likelihood events

# Heuristic Biases (Tversky 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?

## 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
- 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)
    - Degrades over time
    - Ineffective from beginning
  - 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

# Assumption-Based Planning

- James Dewar, Rand
- Used to help the U.S. Army in mid-term and long-term planning 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

# Common Assumptions

- 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 were 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, or
   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 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.

# Identifying Leading Indicators

# Where Assumptions Come From

- High-level system goals generated during concept development
- System-level requirements generated from system goals
- Assumptions about external environment in which system will operate
- System behavioral requirements imposed by safety-related environmental requirements and constraints (including constraints on the use of the system)
- STPA-generated hazards, the hierarchical control structure, unsafe control actions, and causal scenarios
- Design features devised to manage the causal scenarios
- Operational requirements created to manage causal scenarios
- Limitations in design of safety-related controls, including operational controls

# Intent Specification for TCAS

- Done by myself with a student who built a formal model
- Scenarios generated by a qualitative hazard analysis
- Critical part of intent specs is to document assumptions under which system is built and safety based.

# 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].*

> *Assumption: 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.*

# Assumptions Imposed by or on Environment

*E1: The behavior or interaction of non-TCAS equipment with TCAS must not degrade the performance of the TCAS equipment or the performance of the equipment with which TCAS interacts.*

*E2: Among the aircraft environmental alerts, the hierarchy shall be: Windshear has first priority, then the Ground Proximity Warning System (GPWS), then TCAS.*

*E3: The TCAS alerts and advisories must be independent of those using the master caution and warning system.*

# Hazards

*H1: TCAS causes or contributes to a near midair collision (NMAC), defined as a pair of controlled aircraft violating minimum separation standards.*

*H2: TCAS causes or contributes to an aircraft coming too close to a fixed structure or natural terrain.*

*H3: TCAS causes or contributes to the pilot losing control over the aircraft.*

*H4: TCAS interferes with other safety-related aircraft systems (for example, ground proximity warning)*

*H5: TCAS interferes with the ground-based air traffic control system (e.g., transponder transmissions to the ground or radar or radio services).*

*H6: TCAS interferes with an ATC advisory that is safety-related (e.g., avoiding a restricted area or adverse weather conditions).*

# A Factor in Uberlingen

- A year prior there was a near miss due to conflicting TCAS and ATC commands
  - Two Japanese airliners
  - One pilot made evasive maneuvers based on visual judgment.
    - Aircraft came within 300 ft
    - Evasive maneuvers caused ~100 injuries
  - Japan called for changes, but ICAO did not take action until after Uberlingen
- Four other near misses in Europe before Uberlingen collision (involving one flight crew obeying TCAS and one following the air traffic controller)

# Safety Constraints

*SC.2: TCAS must not interfere with the ground ATC system or other aircraft transmissions to the ground ATC system (H5).*

STPA can be used to identify causes for the violation of SC.2. This information can then be refined into a more detailed safety constraint SC2.1:

*SC2.1 The system design must not interfere with ground-based secondary surveillance radar, distance-measuring equipment channels, and with other radio services that operate in the 1030/1090 MHz frequency band (2.5.1).*

# Operator-Related Assumptions

*SC.6: TCAS must not disrupt the pilot and ATC operations during critical phases of flight nor disrupt aircraft operation (H3, 2.2.3, 2.19, 2.24.2).*

*SC6.1 The pilot of a TCAS-equipped aircraft must have the option to switch to the Traffic-Advisory-Mode-Only where traffic advisories are displayed but display of resolution advisories is inhibited (2.2.3).*

*Assumption: This feature will be used only during takeoff or in final approach to parallel runways, when two aircraft are projected to come close to each other and TCAS would call for an evasive maneuver.*

# Other Operational Requirements

- *OP4: After the threat is resolved, the pilot shall return promptly and smoothly to his/her previously assigned flight path.*
- *OP9: The pilot must not maneuver on the basis of a Traffic advisory only*

# System Design Limitations

*L4: TCAS does not currently indicate horizontal escape maneuvers and therefore does not (and is not intended to) increase horizontal separation.*

Other limitations are related to the environmental assumptions, for example:

*L1. TCAS provides no protection against aircraft without transponders or with nonoperational transponders (EA3).*

*L6: Aircraft performance limitations constrain the magnitude of the escape maneuver that the flight crew can safely execute in response to a resolution advisory. It is possible for these limitations to preclude a successful resolution of the conflict (H3, 2.38, 2.39)*

*L4: TCAS is dependent on the accuracy of the threat aircraft's reported altitude. Separation assurance may be degraded by errors in intruder pressure altitude as reported by the transponder of the intruder aircraft (EA5)*

*<u>Assumption</u>: Will go away or be reduced as more aircraft install GPS*

Limitations are accepted risks

# More Limitation Examples

- *L3: TCAS will not issue an advisory if it is turned on or enabled to issue resolution advisories in the middle of a conflict.*

An implied assumption here is that pilots will, except under unusual circumstances, turn TCAS on before taking off, which can be checked in performance audits.

Finally, limitations may be related to problems encountered or tradeoffs made during system design.

For example, TCAS has a high-level, performance-monitoring requirement that led to the inclusion of a self-test function in the system design to determine whether TCAS is functioning correctly. The following system limitation relates to this self-test facility:

- *L9: Use by the pilot of the self-test function in flight will inhibit TCAS operation for up to 20 seconds depending upon the number of targets being tracked. The ATC transponder will not function during some portion of the self-test sequence.*

# 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 L.I.

- **<u>Shaping Actions</u>**
  - 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 often occur after a change
    - Signposts used for planned or expected changes
    - Assumption checking used for detecting unplanned and potentially unsafe change

# 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 PHA 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