# Human Factors Discovered: Stories from the Front Lines


**Randy Mumaw**

San Jose State University Research Foundation
[NASA Ames Research Center]


May 8, 2018

# The Path to Here

**Ph.D. cognitive psychology**
University of Pittsburgh / Learning Research & Development Center

**Human Resources Research Organization**

**ATC Training**

**Westinghouse Electric / R&D Center**

**Nuclear Power Plant Control Room Operators**

**Boeing Commercial Airplane**

**Commercial Transport Pilots**

**San Jose State University /**
**NASA Ames Research Center**

# Central Ideas

- Humans operating complex, socio-technical systems strive to develop a system understanding deeper than the interface and procedures support.
- System indications may not support a clear understanding of system state; indications can be fragmented, and the operator is responsible for integrating data.
- System designers make inappropriately generous assumptions about the average operator’s ability to make sense of the system.

# Understanding System State:  Monitoring and Procedure Use

Illustration:  Monitoring as Problem-Solving

AECB (Canada):  How do NPP operators monitor the plant?

Method:  Ethnographic; 288 hrs of observation

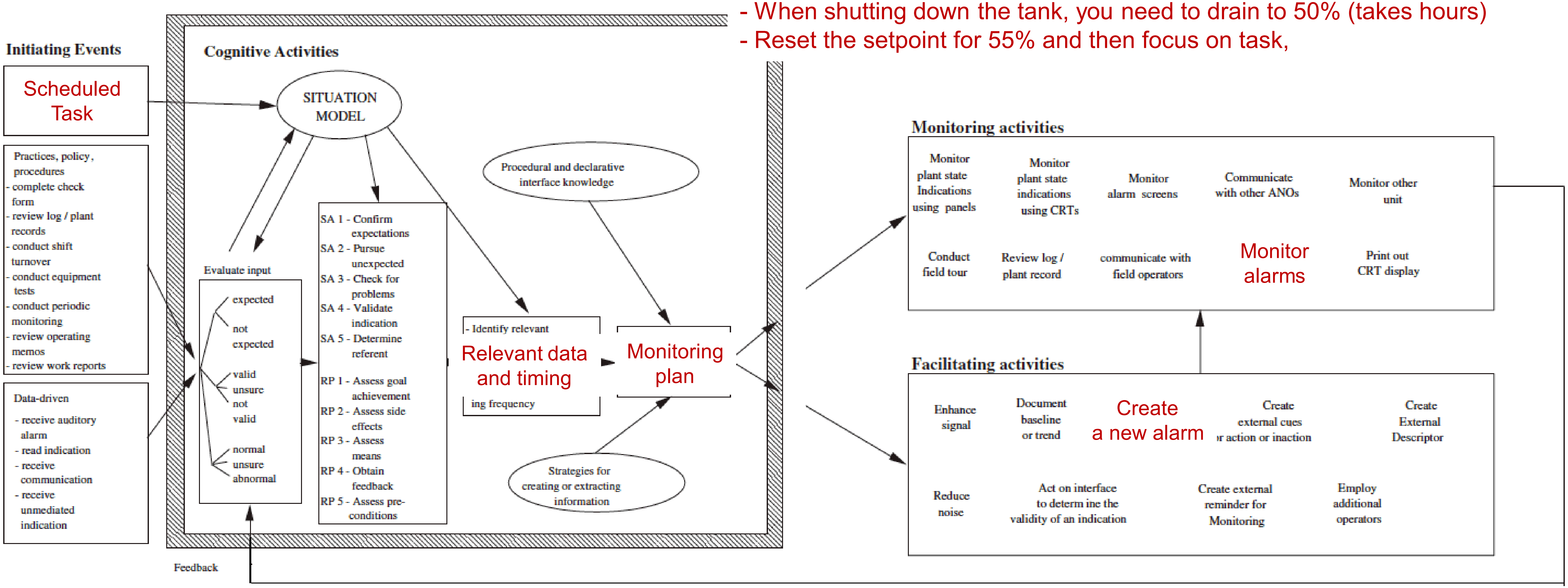
Single-sensor; single-indicator architecture

There is a burden on the operator to
- allocate attention appropriately
- add context
- understand system state
- identify developing problems

**What does monitoring look like?**

# Model of Monitoring

Create a new alarm:
- There is an existing alarm on a tank level to ensure level is sufficient (> 75%)
- When shutting down the tank, you need to drain to 50% (takes hours)
- Reset the setpoint for 55% and then focus on task,

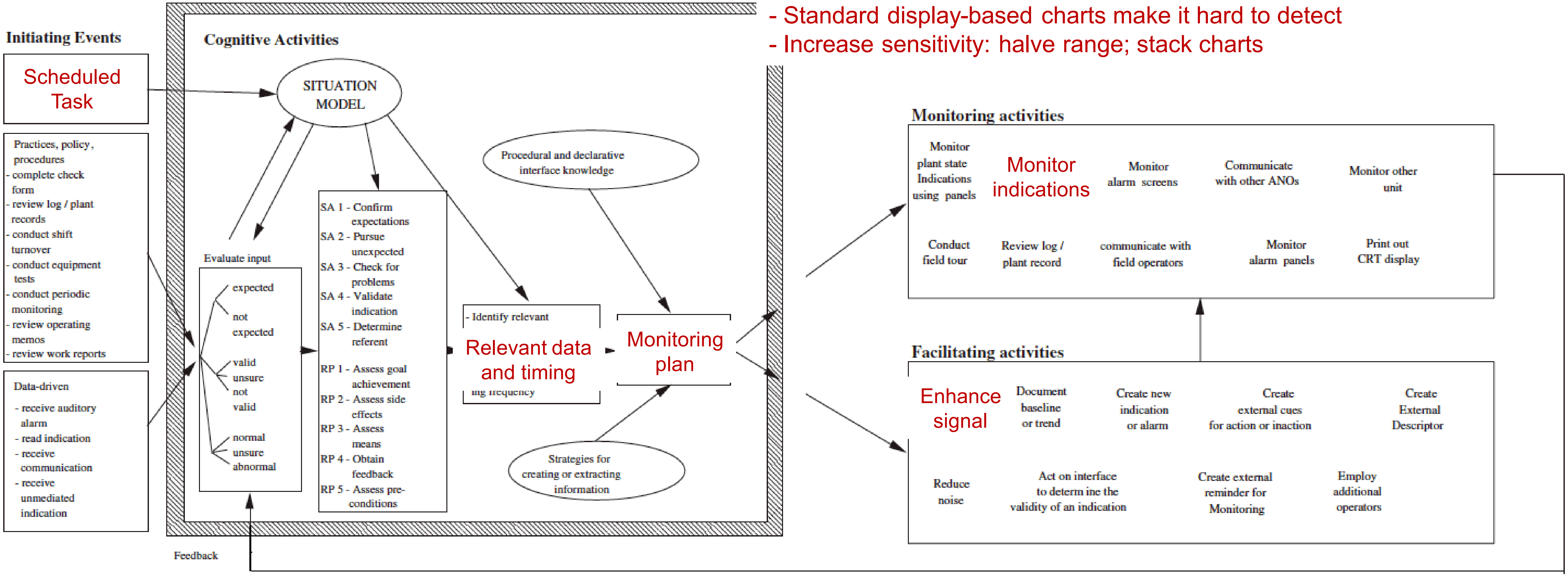



Vicente, K.J., Mumaw, R.J., & Roth, E.M. (2004). Operator monitoring in a complex dynamic work environment: A qualitative cognitive model based on field observations. Theoretical Issues in Ergonomic Science, 5(5), 359-384.

# Model of Monitoring

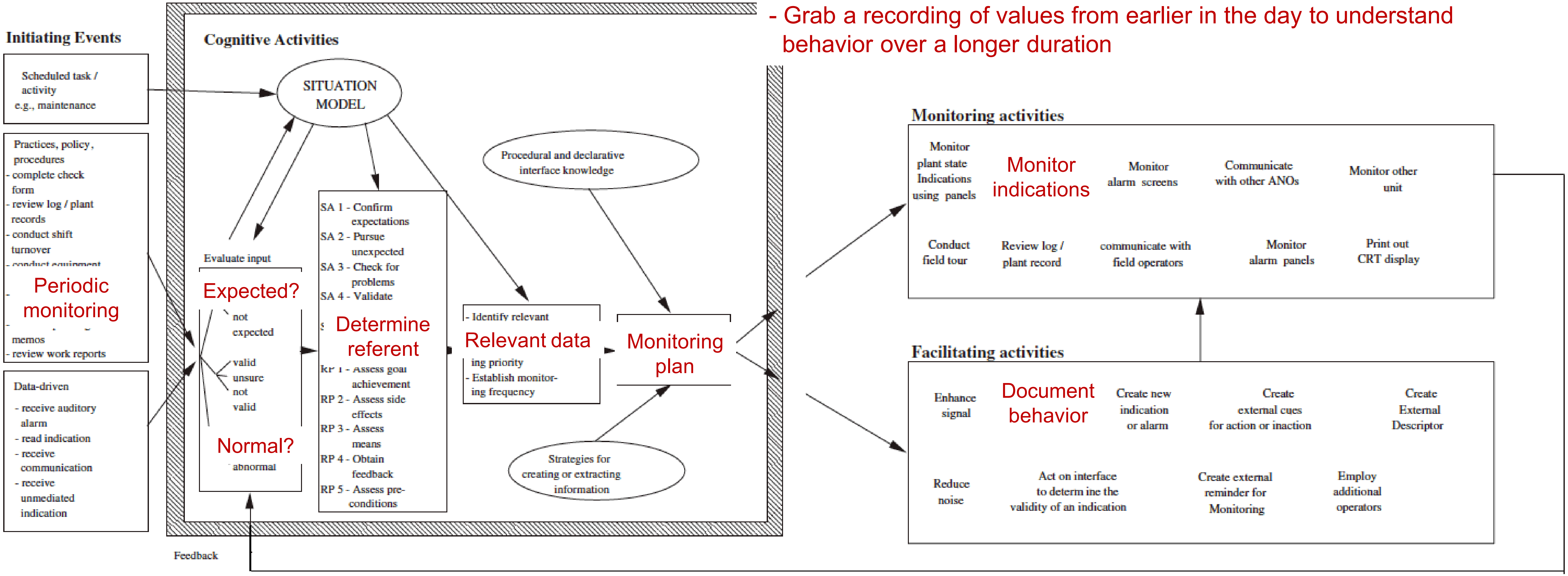
<u>Increase sensitivity:</u>

- When refueling occurs, there is a need to monitor temperature changes, which can be small
- Standard display-based charts make it hard to detect
- Increase sensitivity: halve range; stack charts



# Model of Monitoring

Establish baseline or trend:
- Some parameters are more variable and there is value in knowing their behavior over a longer period of time
- Grab a recording of values from earlier in the day to understand behavior over a longer duration



# Take-Aways

- The older technology makes visible these active monitoring strategies
  - changing saliency
  - managing tasks / workload
  - reducing uncertainty
- Operators are “finishing the design”; creating information that the interface designer failed to provide
- Cognition is distributed to the interface
  - reminders and alerts
  - [spatial dedication]
- How do we create opportunities for finishing the design with new technologies?

# Understanding System State:  Monitoring and Procedure Use

Illustration:  Procedure Use

Nuclear Reg Comm:  Cognitive inputs to procedure use

Method:  Human in the loop simulation

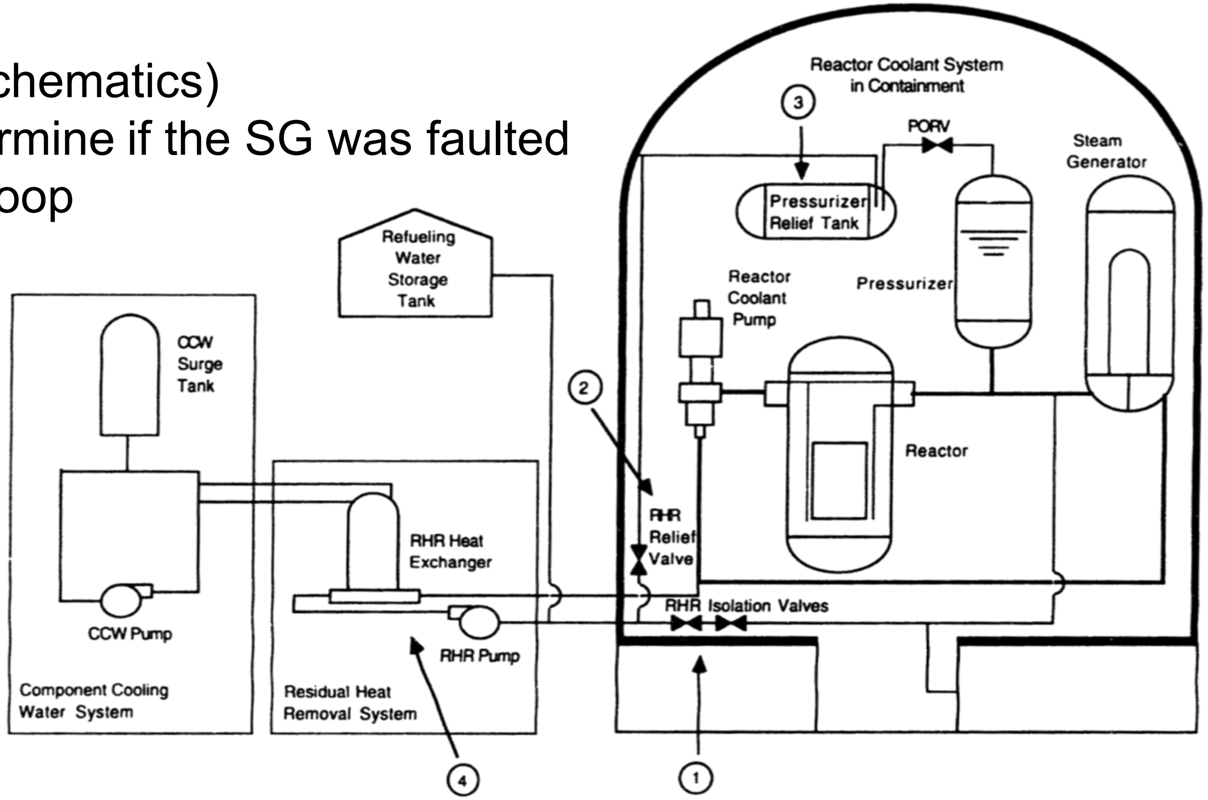
Malicious Procedural Compliance

# Procedure Use for a Cognitively Demanding Fault

Problem: Reactor coolant leak in an unusual place (distributed symptoms);
Solution requires a transition between separate Emergency Operating Procedures (EOPs)

Key EOP step: if Steam Generator (SG) pressure NOT stable or increasing return to step 1 [and, SG pressure is decreasing]

Key to solving:
- a focus on other inputs to SG pressure (use of schematics)
- understood that the point of the step was to determine if the SG was faulted
- awareness that they were stuck in a procedural loop




Roth, E.M., Mumaw, R.J., & Lewis, P.M. (1994). An empirical investigation of operator performance in cognitively demanding simulated emergencies. (NUREG/CR-6208). Washington, DC: Nuclear Regulatory Commission.

# Take-Aways

- For both situation assessment and response planning, operators supported their procedure use through extra-procedural actions, such as developing a coherent account of symptoms.
- Some crews appropriately chose not to take safety actions that were recommended by the EOPs.
- Successful crews had knowledge of the structure of the EOPs and the objectives of different procedures.

# Incoherence of System Indications

- Airplanes have a more compact, more modern interface;
- Airplanes are (generally) less about diagnosing system faults and more about continuing safe flight and landing;
- However, they can present a pretty incoherent or fragmented picture of airplane state.

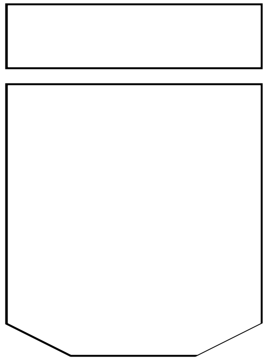
Let's look at how the following are presented:
- Unreliable airspeed
- Engine indications
- Cabin altitude (Helios)

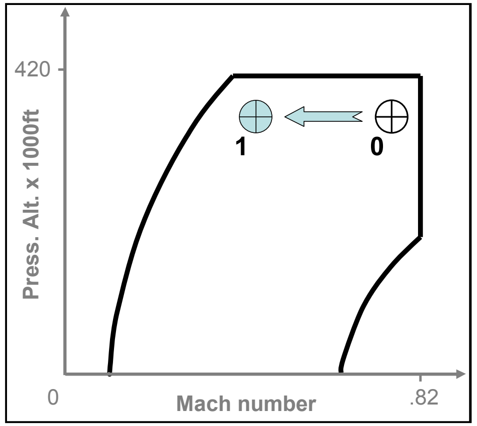
High-Altitude Pitot Icing
Scen 1: Fail L+C+R pitots

# FDE: Event 1
(first 30 seconds)

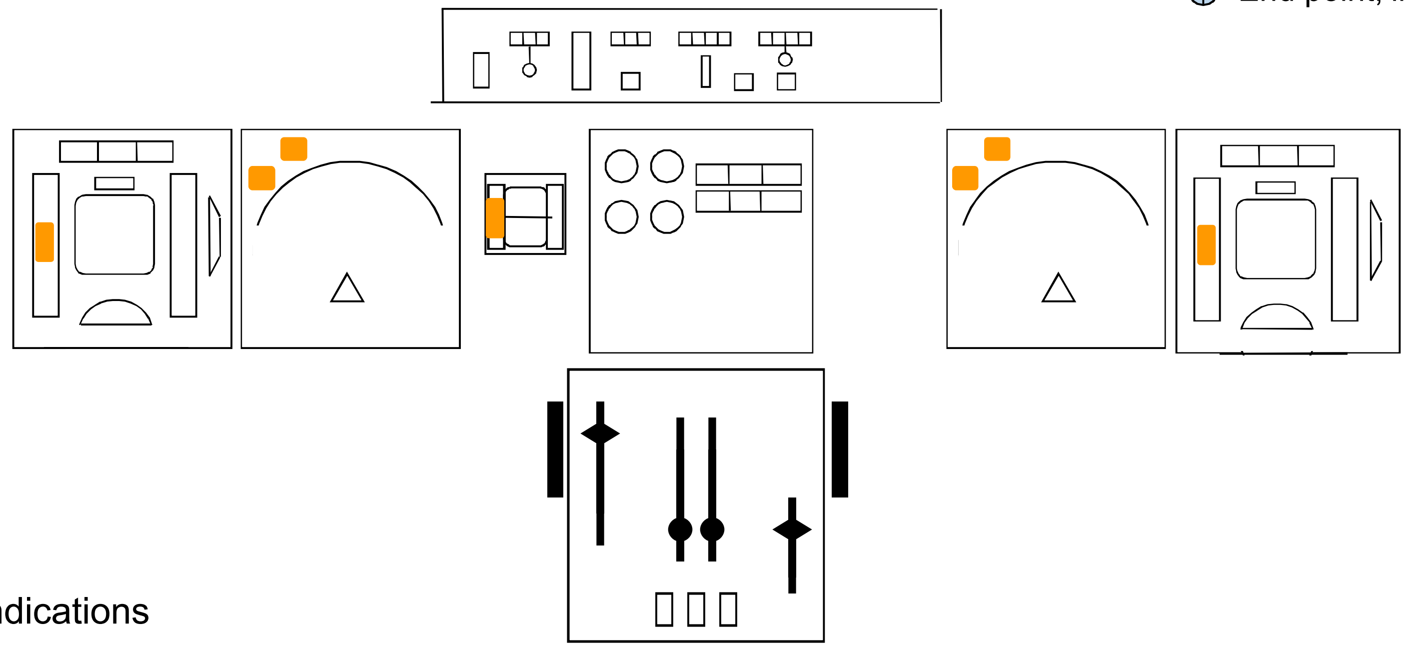
<u>PFD:</u>
Capt IAS ↓ 125
Stdby IAS ↓ 125
FO IAS ↓ 125

<u>ND:</u>
Capt TAS ↓ 231
FO TAS ↓ 231
Capt wind ↑ 250 kts
FO wind ↑ 250 kts






Starting point
End point, indicated



accurate indications
erroneous indications

High-Altitude Pitot Icing
Scen 1: Fail L+C+R

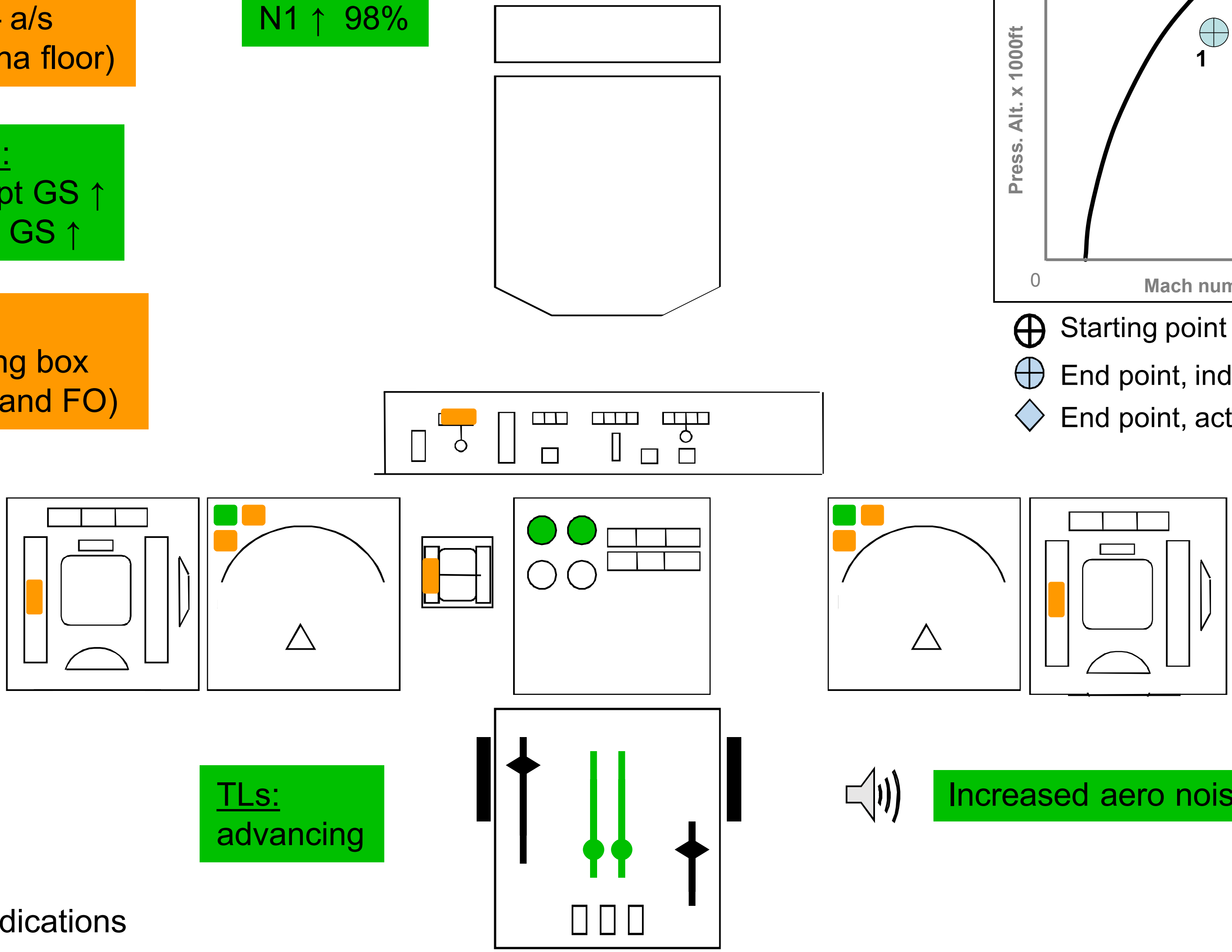
# FDE: Event 1
(after 30 seconds)

**MCP:**
Flashing A – a/s window (alpha floor)

**Eng Ind:**
N1 ↑ 98%

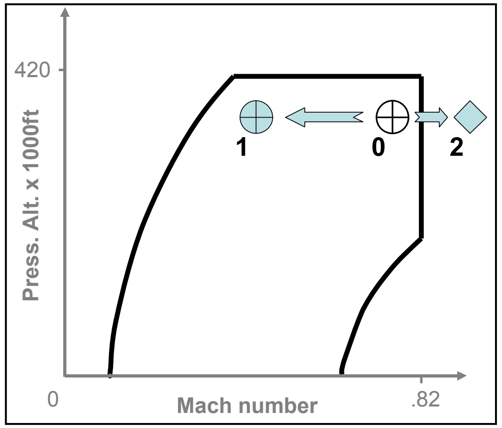
**ND:**
Capt GS ↑
FO GS ↑

**PFD:**
Amber flashing box on IAS (CA and FO)



**TLs:**
advancing

Increased aero noise




Starting point
End point, indicated
End point, actual

accurate indications
erroneous indications

High-Altitude Pitot Icing
Scen 1: Fail L+C+R

# FDE: Event 1
(first 50 seconds)

**ND:**

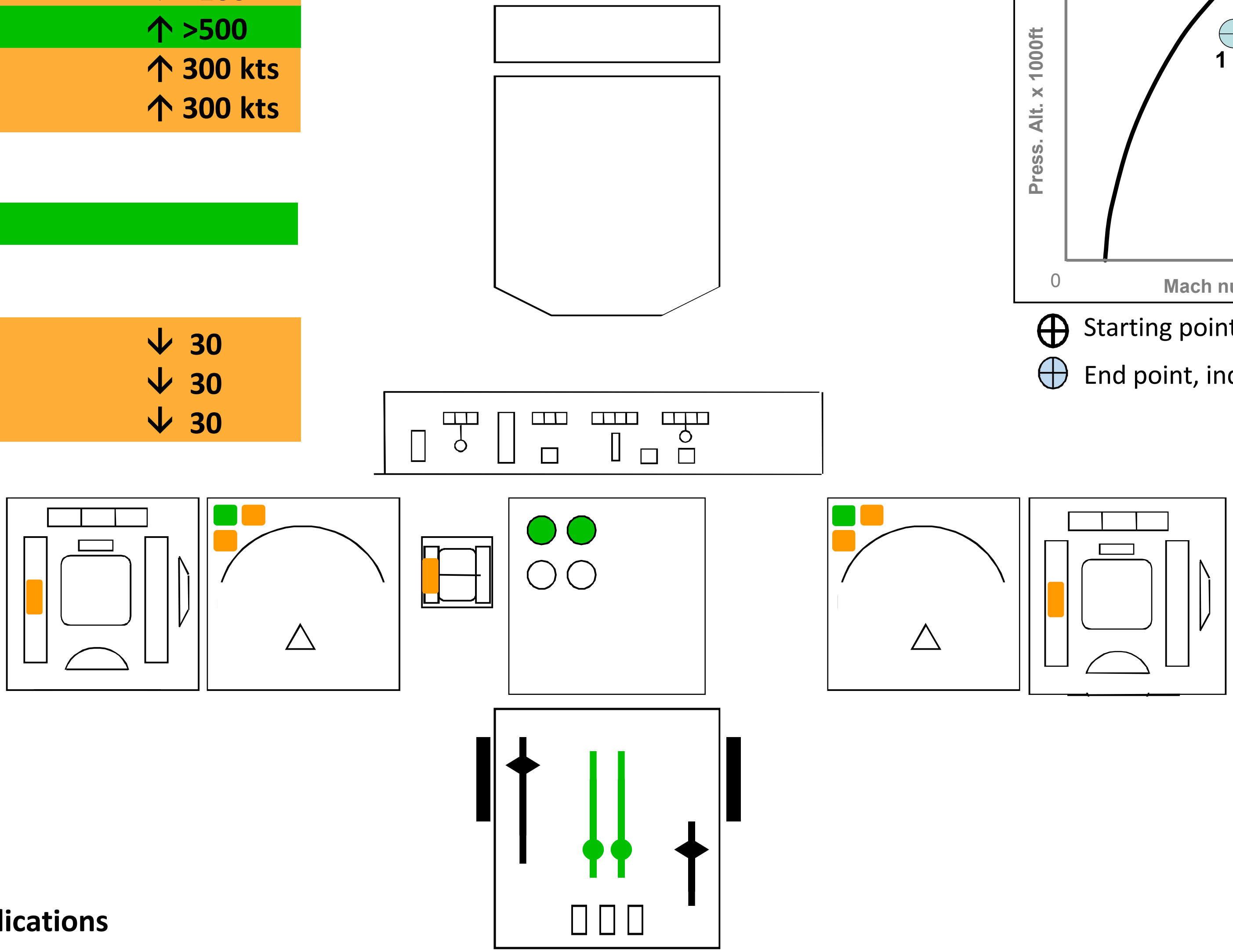
| | |
|---|---|
| CAPT + FO TAS | ↓ <100 |
| CAPT + FO GS | ↑ >500 |
| Capt wind | ↑ 300 kts |
| FO wind | ↑ 300 kts |

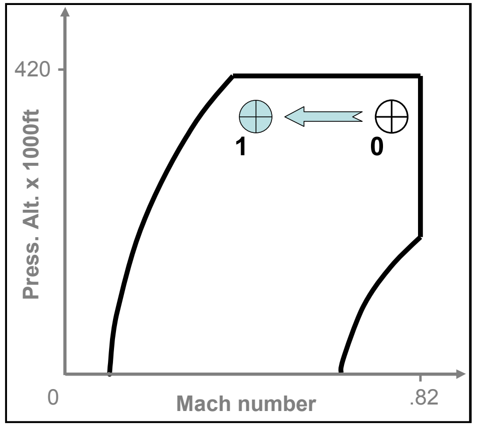
**TLs:**

Advancing

**PFD:**

| | |
|---|---|
| Capt IAS | ↓ 30 |
| Stdby IAS | ↓ 30 |
| FO IAS | ↓ 30 |






⊕ Starting point

⊕ End point, indicated

accurate indications

erroneous indications

# FDE: Event 2

(after 50 seconds, @ approx. 55kts)

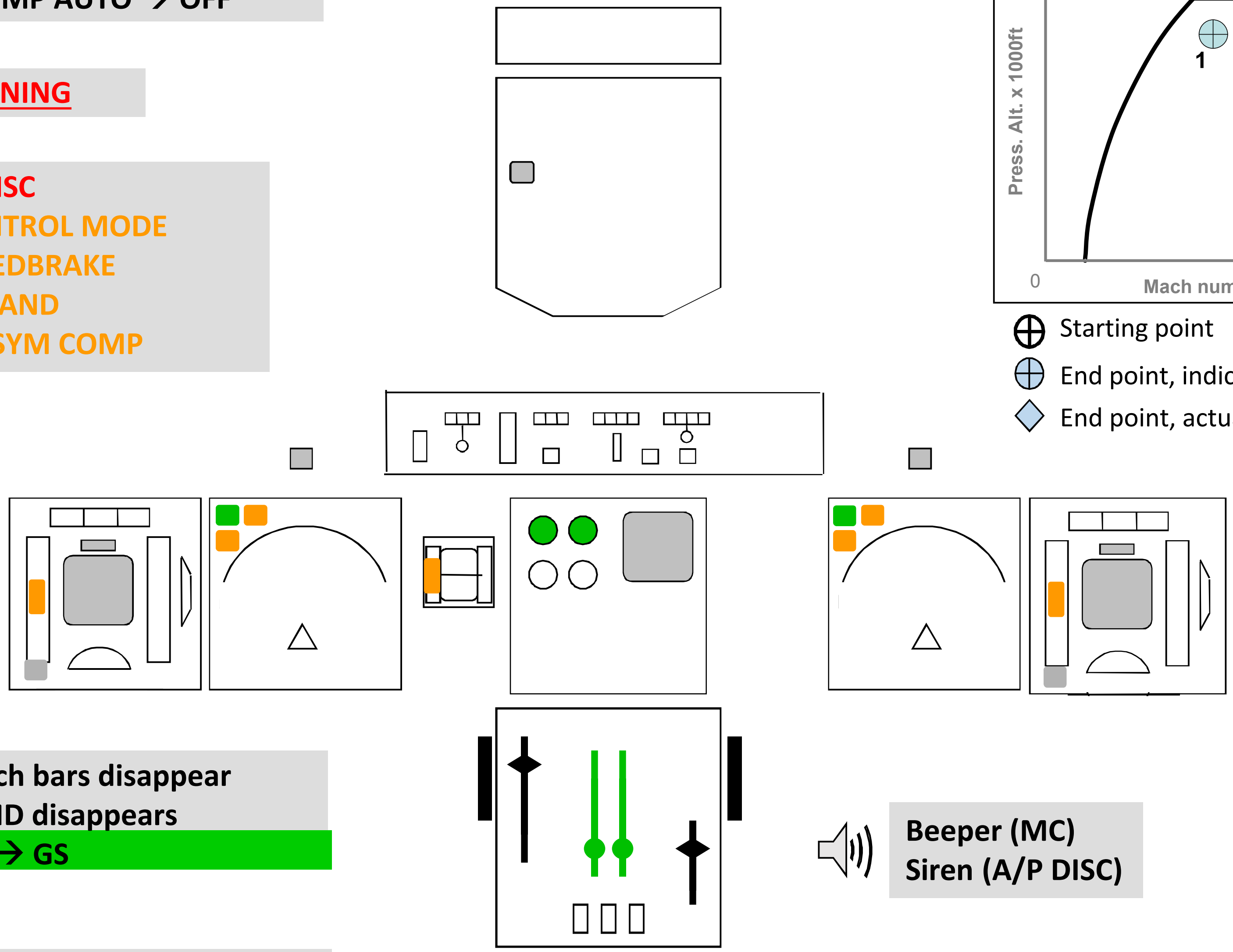
**OVHD PANEL:**

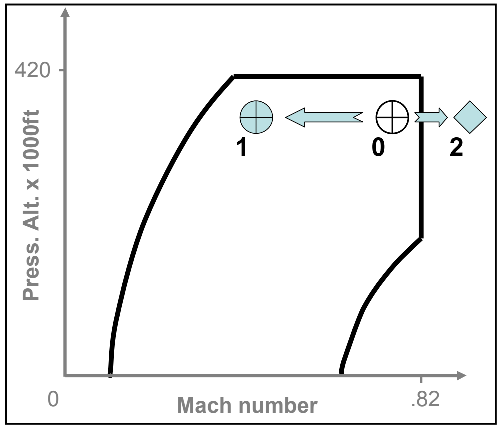
THR ASYM COMP AUTO → OFF

**MASTER WARNING**

**EICAS:**

AUTOPILOT DISC
[] FLIGHT CONTROL MODE
AUTO SPEEDBRAKE
NO AUTOLAND
THRUST ASYM COMP






Starting point
End point, indicated
End point, actual

**PFD:**

CAPT + FO pitch bars disappear
CAPT + FO CMD disappears
CAPT + FO M → GS

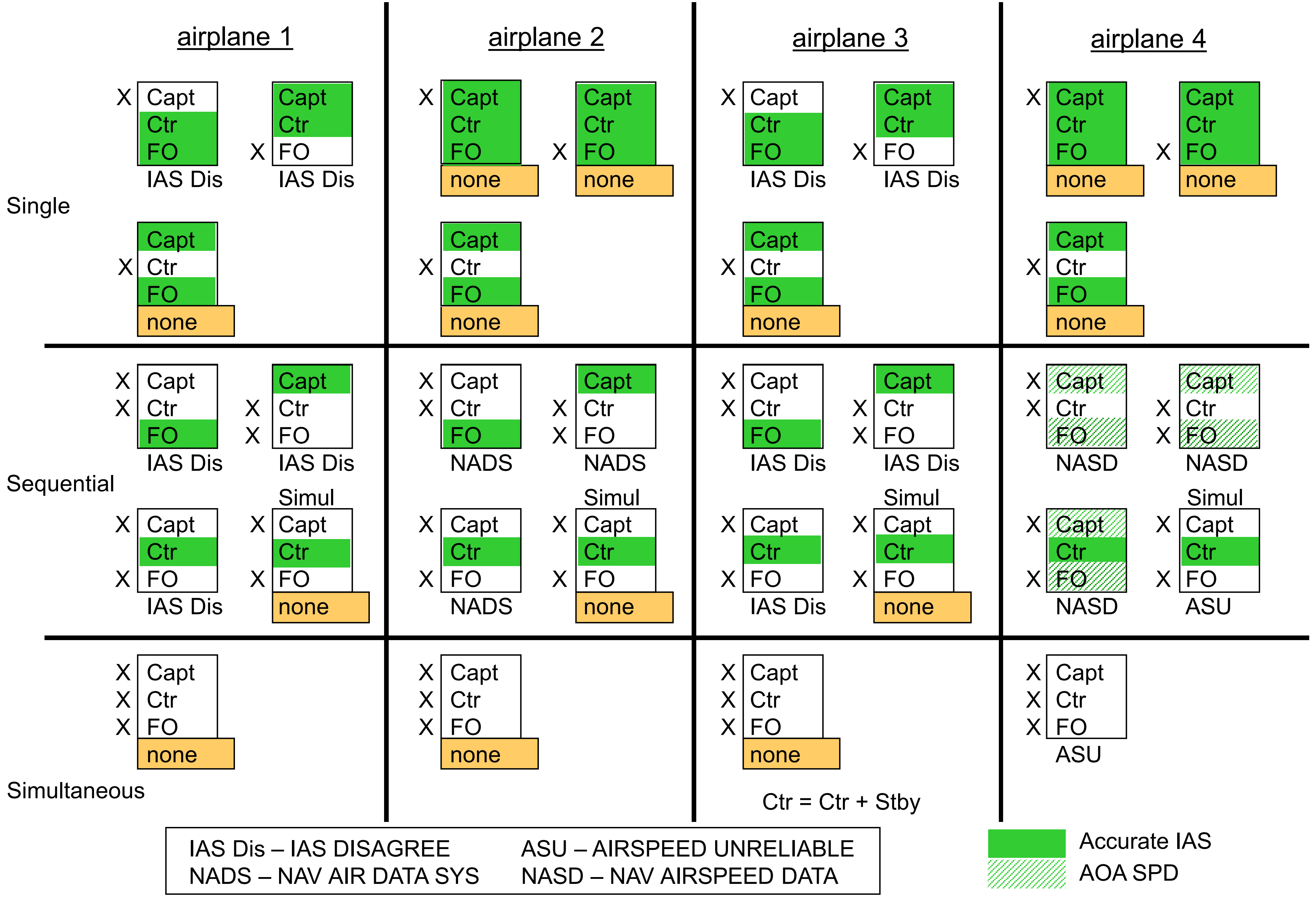
**ND:**

TAS + wind disappears

Beeper (MC)
Siren (A/P DISC)

accurate indications
erroneous indications

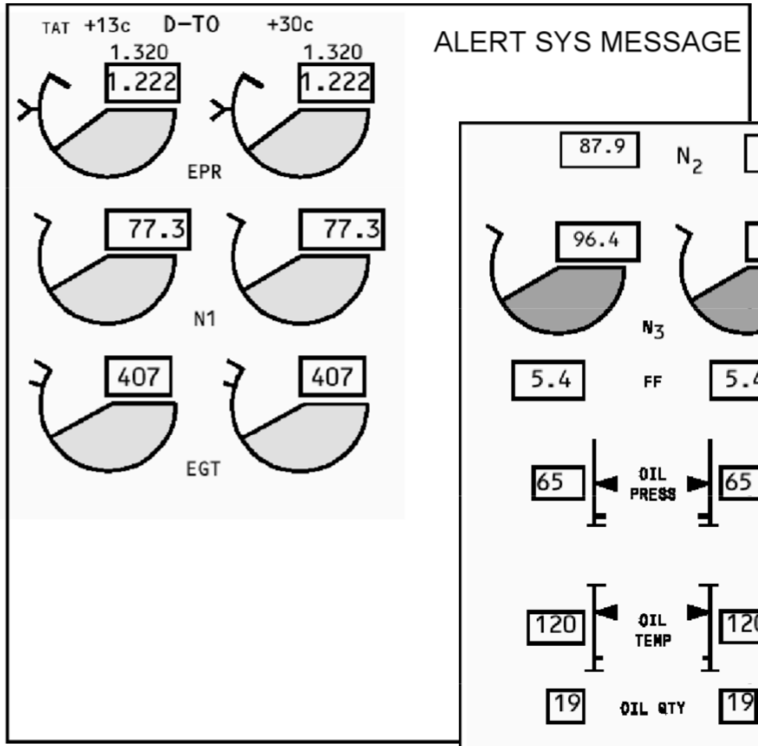
# IAS Behavior and Relevant Alerts



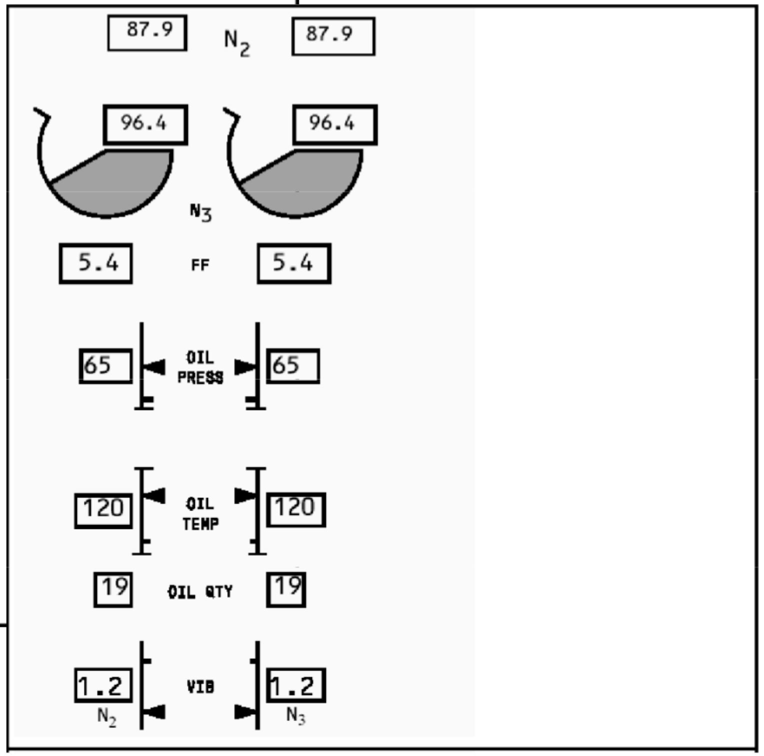
# Take-Aways

- The burden is on the pilot to integrate across seemingly contradictory indications; no clear, direct indication of fault
- There is no indication of data validity; airspeed indications look “normal”
- Some progress has been made in this area: AoA-based speed

# Engine Indications




**Primary Indications**




**Secondary Indications**

Single-sensor; single-indicator . . . again

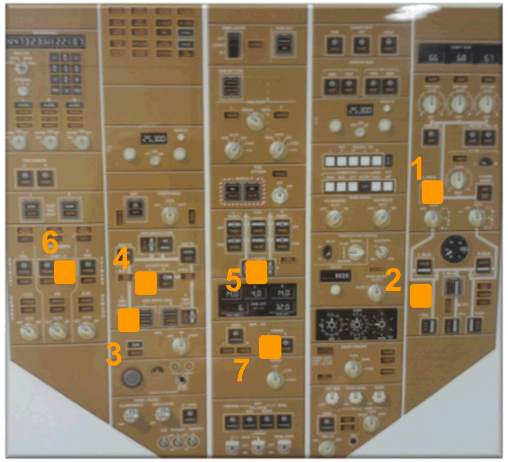
Important engine states must be inferred
- engine surge
- engine damage / severe engine damage
- significant degradation or vibration

Confusion about which engine is affected

The Regs <u>require</u> all of these parameters

# Flight Deck Effects: Engine Icing

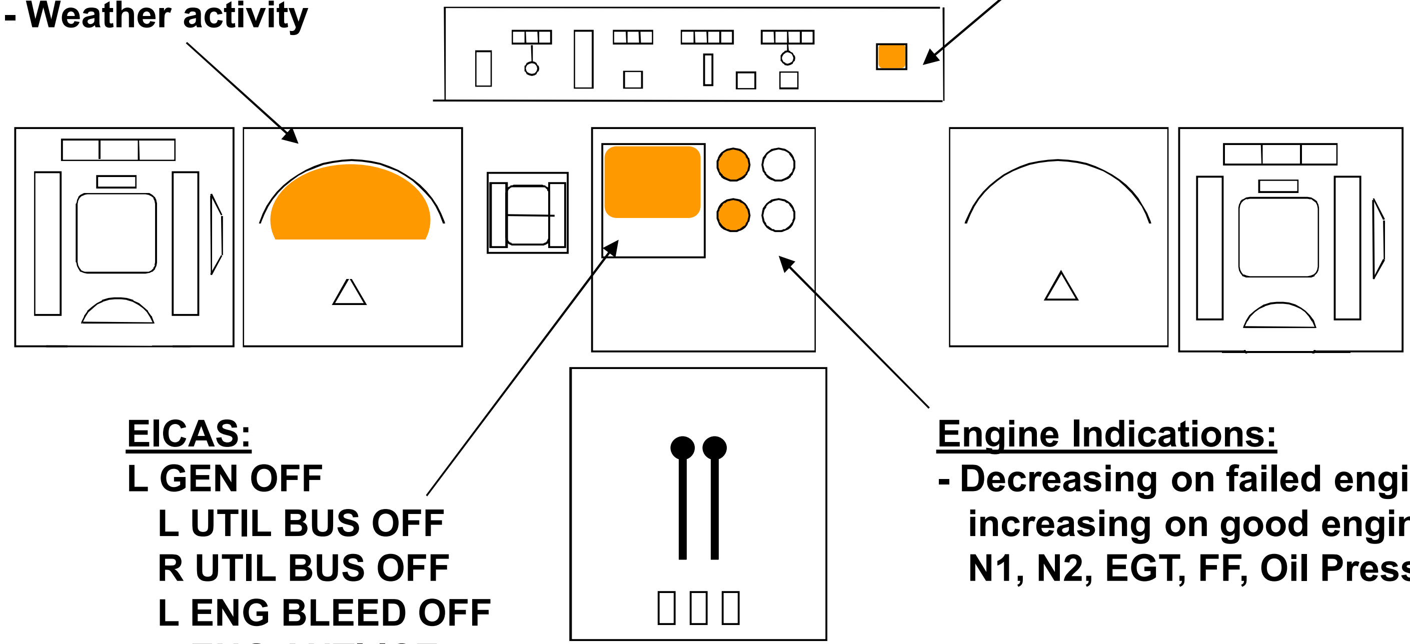
**Overhead Panel Lights ON**
- **Pack Off** (1)
- **Eng Bleed** (2)
- **Gen Off** (3)
- **Utility Bus** (4)
- **Center Fuel Tank Pumps** (5)
- **C2 Hyd Pump** (6)
- **Eng Anti-ice Valve** (7)




Appropriate Action:
Engine Fail non-normal checklist

**ND:**
**- Weather activity**

**MASTER CAUTION LIGHT AND BEEPER**



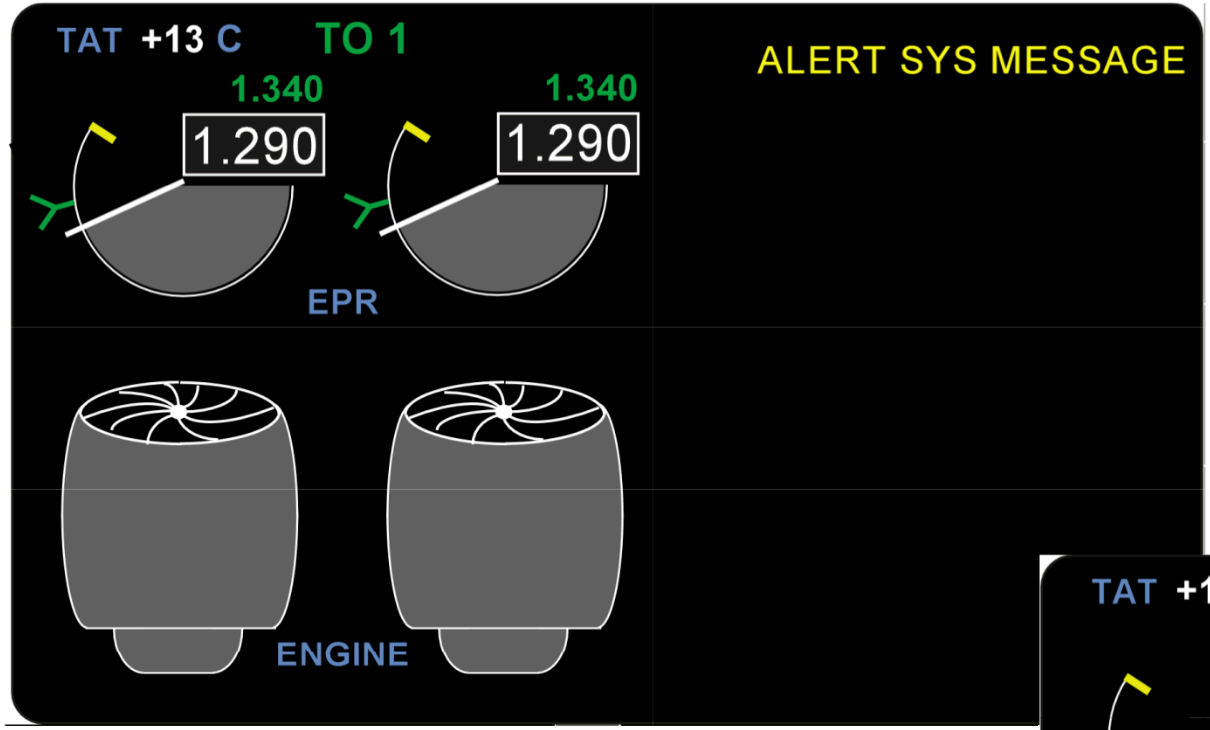
**EICAS:**
**L GEN OFF**
**L UTIL BUS OFF**
**R UTIL BUS OFF**
**L ENG BLEED OFF**
**L ENG ANTI-ICE**
**L ENG PACK OFF**

**Engine Indications:**
**- Decreasing on failed engine; increasing on good engine for N1, N2, EGT, FF, Oil Press**

Basic Thrust Parameter

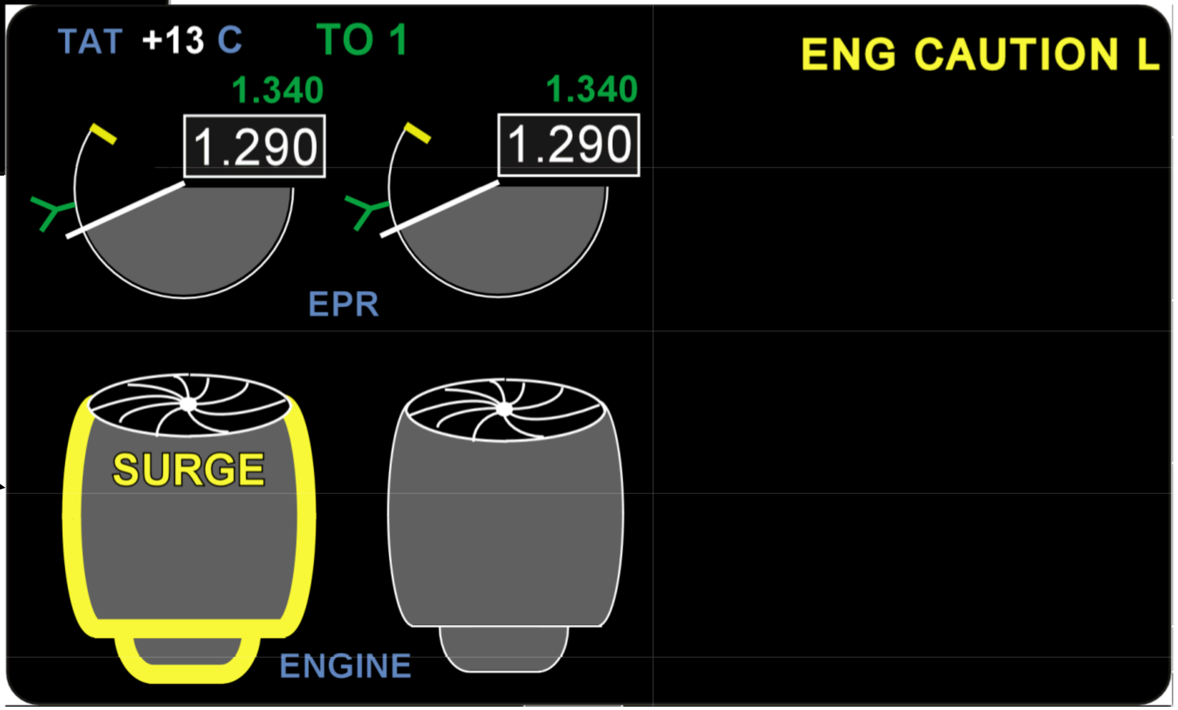
Centralized alerting

Engine Indication




- Operating State (Engine Availability)
  - engine running
  - engine not running
    - failed
    - shut down
    - engine starting (and status)
- Non-Normal State
  - which engine is affected?
  - what is the required action?
    - reduce throttle
    - shut down engine
  - why? what condition is present?

Deviation that caused the condition is revealed




Sikora, J. & Mumaw, R. (2004). Making engine displays more meaningful to flight crews. Proceedings of the International Conference on Human-Computer Interaction in Aeronautics, Toulouse, France.

# Helios 522 Accident

1 Pressurization was inadvertently set to MANUAL, preventing the airplane from pressurizing

2 At 12,000, Cabin Altitude Horn sounds (same horn as TO Config)

3 At 17,000, two messages appeared on Overhead Panel:
- Equipment Cooling
- PASS OXY ON


4 Single light on “6 pack” points to indicate there are 2 alerts

5 Equipment Cooling is near the front of the panel; PASS OXY ON is further back

6 Airplane continues to climb; Crew incapacitated due to O2 loss

Front

# Explosion of Alert Messages

<u>Qantas A380 Uncontained Engine Failure</u>

- QF 32;  Singapore to Sydney; 469 people on board
- 4 minutes after Take-off, engine no. 2 bursts, severely damaging other equipment
- 43 ECAM messages in first 60 seconds; many additional later (> 80 total)
- 50 minutes to sort through the non-normal checklists (NNCs)

"It was hard to work out a list of what had failed; it was getting to be too much to follow.  So we inverted our logic: Instead of worrying about what failed, I said 'Let's look at what's working.'"        *A380 Captain*

# Appropriate Solutions?

- The burden is on the pilot to integrate across low-level indications
- What should we provide operators?
  for NPP . . . . fault diagnosis and pointer to actions to contain/repair

  Commercial aviation . . . .
  - operational limitations
  - guidance for continued safe flight and landing

# New Approach for Managing Non-normals

Airplane system failure → Mission Compatibility

Airplane Capabilities

Maneuver Envelope

Changes to Operational Limitations (phase of flight)

Diversion Decision Making (if needed)

Mumaw, R.J., Feary, M., Fucke, L., Stewart, M., Ritprasert, R., Popovici, A., & Deshmukh, R. (2018). Managing complex airplane system failures through a structured assessment of airplane capabilities. NASA/TM-2018-291775. Moffett Field, CA: NASA Ames Research Center.

# What is a Capability?

Airplane System Components

- Hydraulic system
- Thrust Reverser
- Battery
- Air conditioning pack

Airplane Capabilities

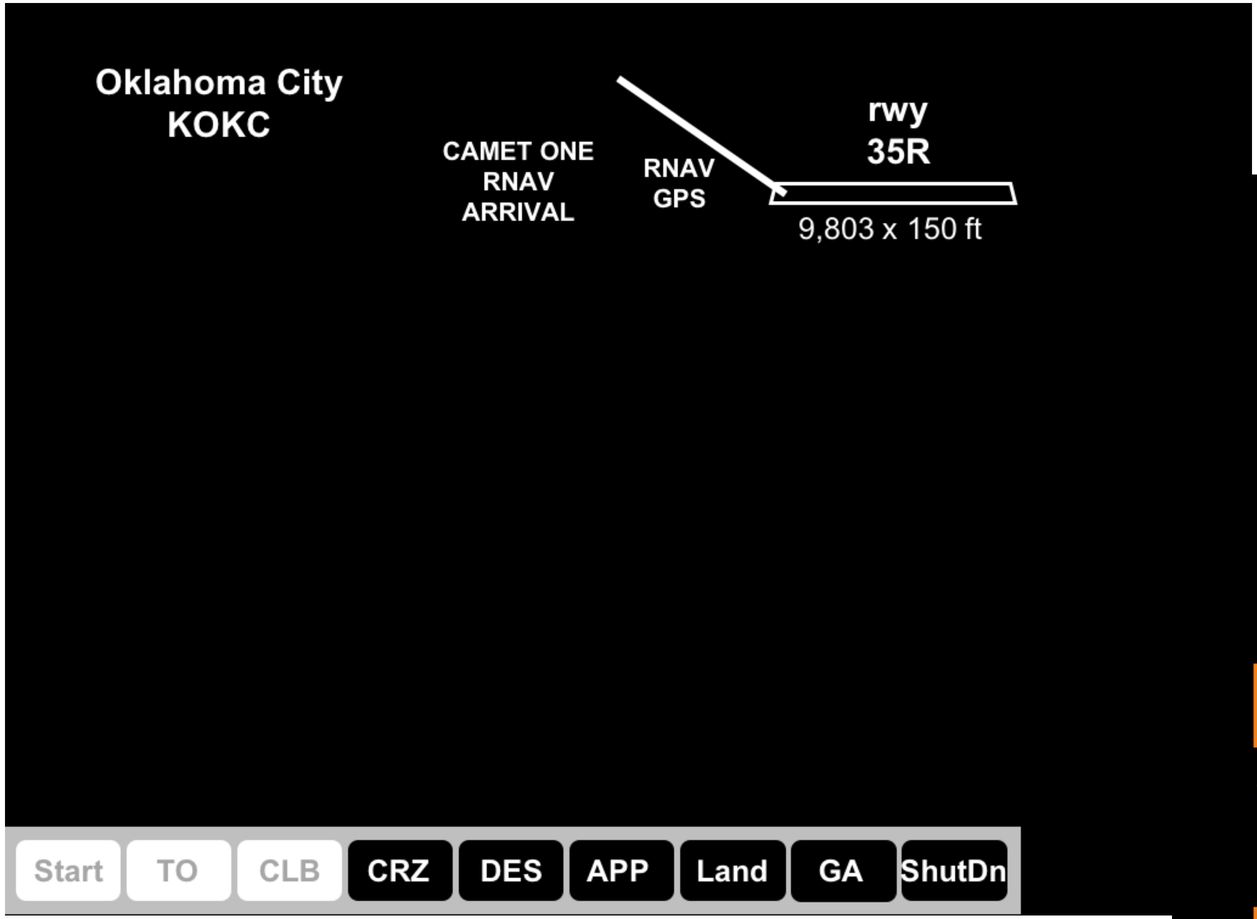
- Range / Endurance
- Stopping Distance (on runway)
- Ability to perform a specific approach
- Ability to enter RVSM airspace
- Maneuver envelope

Airplane system components have failed

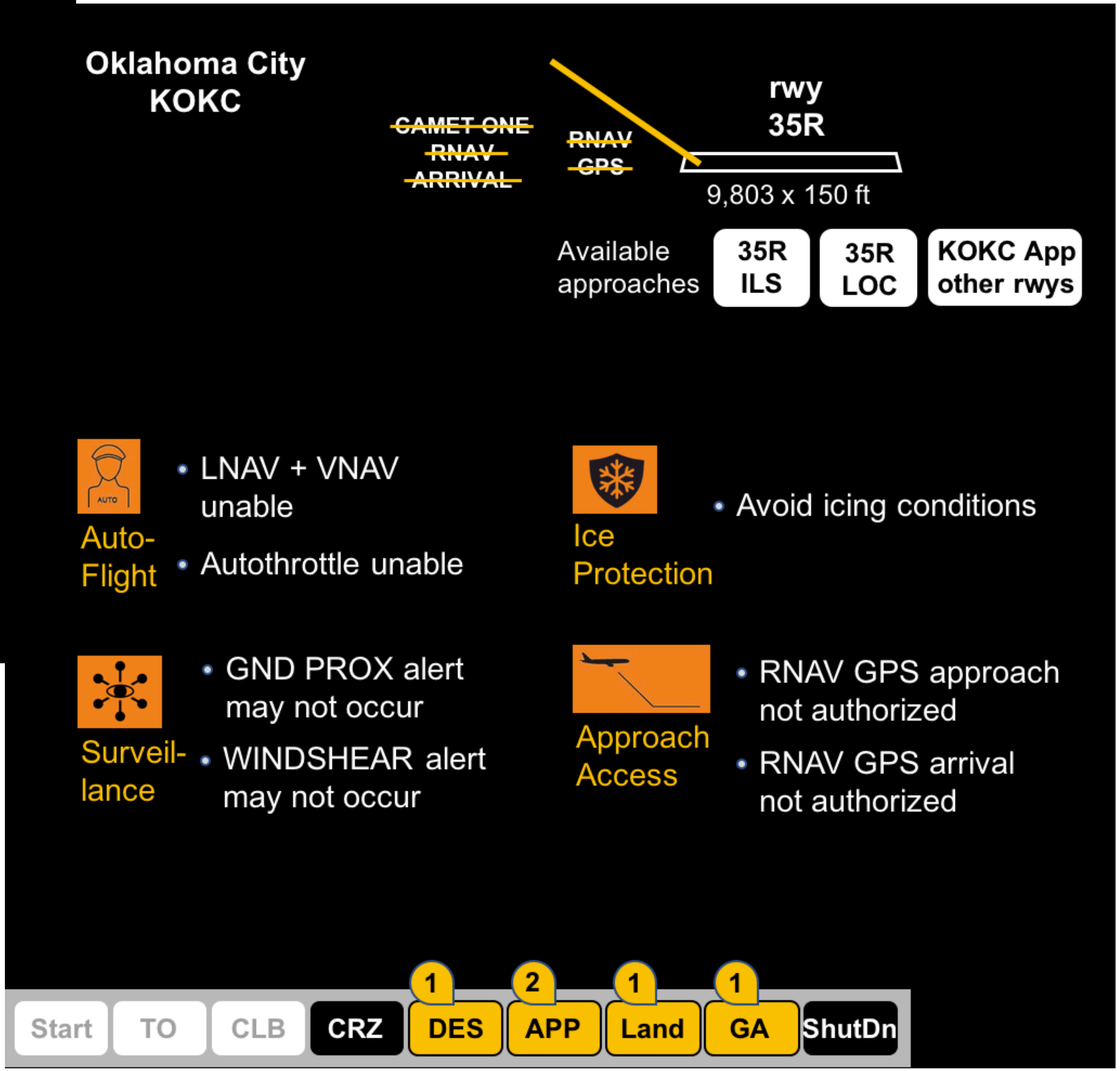
↓

What can I do?
Where can I go?

After an AC Bus Failure




Enroute to OKC, in Cruise.



# Initial Ideas about Airplane Capabilities

Can I Take–off?
Can I reach my planned destination?
Can I land?
Envelope

<u>Resources</u>
Electric Power
Hydraulic Power
Pneumatic Power
Equipment Cooling

Engines (state)

Navigation
Communication
Autoflight
Surveillance
Cabin/Cargo Environment
Ice Protection
Fire Detection & Extinguishing
Airspace Access
Approach Access
Landing Distance
Runway Directional Control
Fuel Supply

# Big Picture Take-Aways

- In complex, engineered systems, there is a legacy of SS-SI that has slowly evolved over the years ( . . . except for engines).

- System operators strive to push beyond the system interface (finish the design) and the procedures to understand system state and manage their system actions.

- A close look at several cases shows that the flight deck effects presented to pilots can place a large burden on the flight crew. We need to change the language of the interface to be more compatible with operations.

- We should be designing an interface that:
  - presents system state and operational objectives more clearly
  - supports both RB and KB performance

# Determining Influence on Performance

- How can we go from potentially confusing flight deck effects to determine how well pilots should be able to perform a task?
- Context is response to a non-normal situation, such as a system failure that requires a flight crew response for continued safe flight and landing

# Analysis Framework: Rasmussen Model

Trained priorities place action behind other activities.

The required action(s) cannot be initiated immediately, and there is no persistent reminder for the flight crew about those action(s).

**Prioritize**

Action violated routinely without negative safety consequences.

**Intentional Deviation**

Taking the action will have considerable consequences associated with cost or the potential for injury.

Only the symptoms of the event can be observed, no explanation is given.

Indications can be (at least partially) explained by automatic system action.

**Understand**

**Select Action(s)**

Checklist to be executed is an un-annunciated checklist.

**Detect**

Normal indication, non-normal in this context.

Pilot must compare to internal standard / non-normal event does not manifest in an indication and can only be felt by the pilot.

**Execute**

**Feedback**

Execution requires complex coordination between controls.

Action to be taken breaks familiar pattern of actions.

**Error Detection**

**Error Recovery**

# Reliability: Performance Helps and Hinders

**Detect**

DET-2 – Critical indicator is available only to one crewmember and is unlikely to be picked up by another.
DET-5 – Normal indication, non-normal in this context.
DET-6 – Other automation or system action occurs to obscure or mask primary event.
DET-8 – Pilot must compare to internal standard

**Understand**

EXP-4 – Only the symptoms of the event can be observed, no explanation is given.
EXP-11 – Indications can be (at least partially) explained by automatic system action.
EXP-13 – Indications appear in multiple systems and require knowledge of system inter-connections to integrate into a coherent explanation.

**Select Action**

SEL-5 – Checklist to be executed is an un-annunciated checklist.
SEL-10 – No action guidance is provided

**Prioritize Action**

PRI-7 – The required action(s) cannot be initiated immediately, and there is no persistent reminder for the flight crew about those action(s).

**Intentional Deviation**

DEV-6 – There is significant uncertainty or unknown risk associated with taking the action (e.g. the action is not reversible).
DEV-7 – Criterion for taking action is ambiguous or difficult to determine or requires judgment call.
DEV-9 – Taking the action may lead to reduced availability of safety systems, equipment, or instruments.

**Execute**

EXE-10 – Controls are not placed near important indicators that determine execution.
EXE-19 – Execution requires a difficult coordination between crew members.
EXE-23 – Execution requires closed-loop monitoring of the actions effects

**Error Detection; Error Recovery**

# Help/Hinder Analysis

| Detect | Understand | Select Action | Prioritize | Intentional Deviation | Execute |
|---|---|---|---|---|---|
| Indications part of standard scan | Overwhelmed by secondary indications | No guidance | Interface establishes priority | Actions are compatible | Controls clearly marked |
| System action masks engine failure | Possible explanation: other event | | Training establishes priority | Interface gives clear understanding | Near indicators |
| Attention directed somewhere else | Indications require knowledge to integrate | | Needed to continue operating | Delay in actions triggers warning | Actions different |
| | Requires flight crew coordination | | | No perceived negative consequences | Actions break pattern |
| | | | | | Requires cont control |
| | | | | | Physically demanding |
| | | | | | Requires complex coordination |
| | | | | | Requires closed-loop monitoring |
| | | | | | Difficult conditions |

- Relevant HELP factor
- Relevant HINDER factor

# Help/Hinder Analysis

| Detect | Understand | Select Action | Prioritize | Intentional Deviation | Execute |
|---|---|---|---|---|---|
| Crew attention likely on EICAS | | | | | Formal checklist exists |
| EICAS part of standard scan | | | | | Controls are near indicators |
| | Multiple messages/indications point to same conclusion | | | | Controls clearly marked |
| | Condition statement explains event | | | | Control appearance changed |
| | | Checklist condition matches FD effects | | | |
| | | Indication directly points to checklist | | | |
| | | | Priorities established by indications | | |
| | | | | Actions not related to situation | |
| | | | | Checklist gives understanding of action’s effects | |
| | | | | Uncertainty or risk with taking action | |
| | | | | Action may lead to reduced availability | |
| | | | | Action may have costly consequences | |
| | | | | Perception action can be delayed | |
| | | | | Delaying may resolve problem | |

- Relevant HELP factor
- Relevant HINDER factor

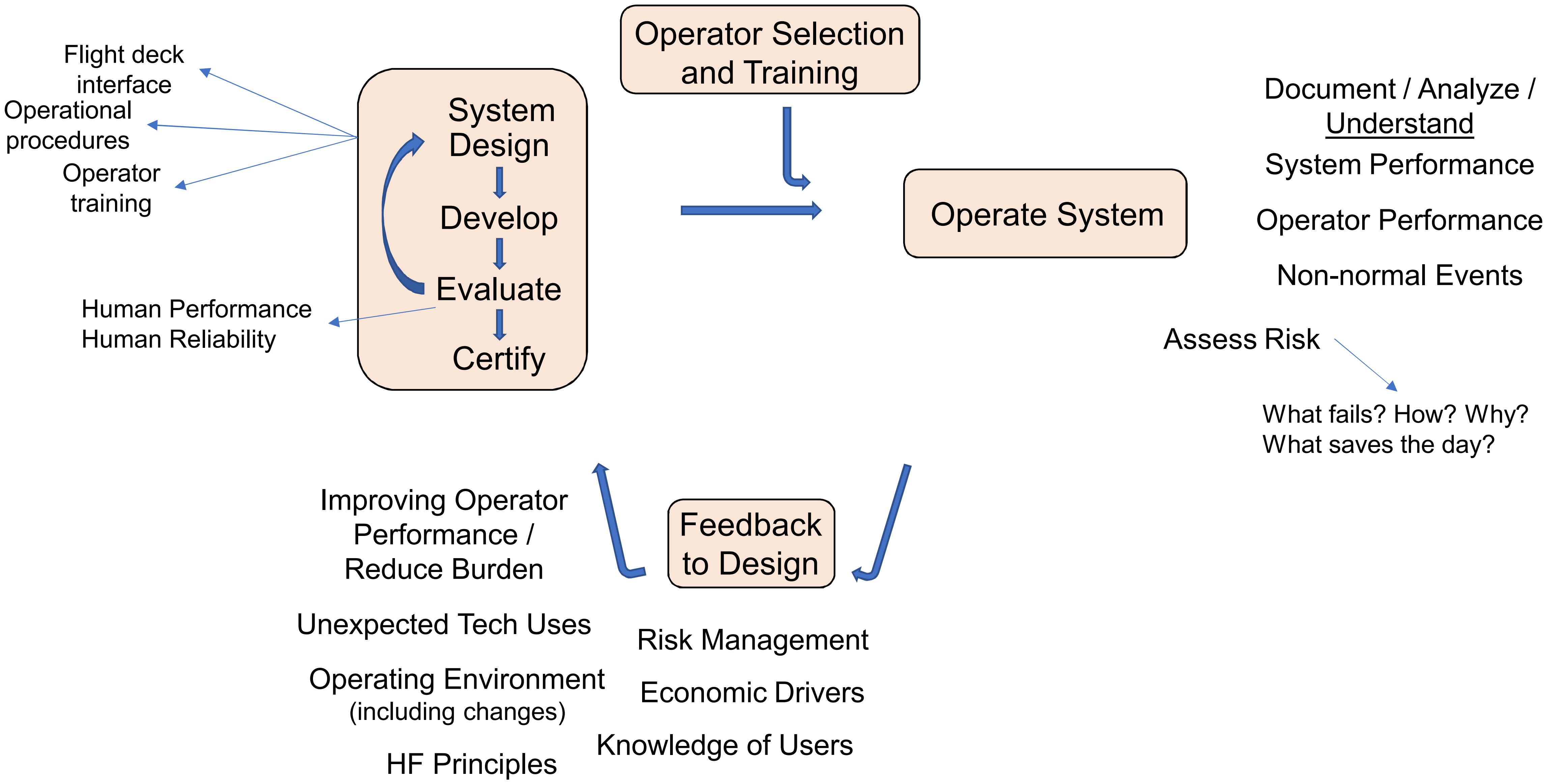
# FD Cue Analysis Take-Aways

- Offers a thorough review of how well the flight deck effects and procedures support identifying and performing the appropriate actions.
- Does not assign an error probability but a back door to quantitative analysis.
- Unlike HRA, allows for consideration of wrong diagnosis and intentional deviations
- Provides essential function of identifying design weaknesses.


Thanks for your time!

# Back-Up

# The Role of HF in the Operation of Complex Systems



Humans (system users/operators) are adaptive:
you can give them a system/training/procedures but they will not do what you expect them to do
Support skilled performance; Anticipate and manage weaknesses. What is skilled perf?

Finishing the design work (and insights into monitoring)
- activities observed; focus on monitoring
- monitoring as problem solving (more observable)
- transition from old to new: display management/overview

Procedures: prescription vs decision aid
- malicious procedural compliance
- Emilie's work in NPP: actions to support 2 objec
- Av cases in which you had to do something other than follow EICAS
  - unreliable airspeed
  - 6 EICAS messages but ENG FAIL
- KB perf happens; need to support it
- can move to ACM here (inherent problems with strings of actions tied to individual failures)

SO, expectation to follow procedure . . . . but
how well does interface support that procedure

Intrinsic → Extrinsic

How well can you manage human behavior?
What are the cues in the environment?
How much can we expect humans to reliably not follow cues

- Helios, as an example
- invalid airspeed has no cue

CREW as a tool to identify cues
- Air France 447 and unreliable airspeed
- HX bypass valve; assumptions about pilot

CREW as effective tool in looking at human reliability
- backing off of assigning a value
- allows you to look at errors of commission (BIG)

Importance of quant tools and measures
(engineering world)

Example of Training Time
- how to predict training time
- TTM, # rules,

Tool for SD ???

Seeing HF through Operations

- Air France 447 → unreliable airspeed → testing of CREW
- CREW Heat exchange bypass valve

- ANA 737 → no alerting on automation failure → automation issue / added an alert
- Flash Air et al → search for SD → work with TNO to build a model
- CAST ASA JSAT → alerting? → alerting analysis
- 1996 FAA report → mode confusion → SAFM and evaluation → Plan B display
- mis-diagnose → presentation of non-normals → airplane capabilities
- SAMG → data certainty → unreliable airspeed → change in indications (787 case)
- something on procedures? Boeing upgrade? Emilie's study / Kim's story
  - the Canadian monitoring work? Kim's story and finishing the design
- ASIAS use for understanding HP; didn't really work

- role of the interface & expanding how we evaluate it
  → expectations feeding into design
- reduce burden on the operator / flight crew (from SS-SI)
- assessing risk
- documenting human performance (errors . . . safety?)
- a toolbox of analysis tools ("human error" as a starting point)
  (maybe mention the idea of "failures in training")
- managing non-normals (prevalence of system components)

Finishing the design /
Understanding cues for performance

Procedures: prescription or decision aid

Managing non-normals / developing an operational language

Assessing Human reliability
(in an engineering world)

Dedicated displays vs flexible workstation and the need for an overview display

Ever-expanding set of evaluation issues
(deeper understanding of crew performance and failures)

Markers of learnability (TTM, etc)

Autoflight solutions