Fault Detection
&
Consequence Prevention
in Real Time

A View from the Industry Trenches

Max O. Hohenberger

Introduction

- There are two main drivers for continuous improvement in the area of Fault Tolerance:

- SAFETY.

- RELIABILITY.

Fault Recognition

- “ Will you tell me my fault, frankly as to yourself, for I had rather wince, than die. ” Men do not call the surgeon to commend the bone, but to set it....”.

  Emily Dickinson

- Whether it’s the temperature input to a reactor trip system, the elevator controls on a 747, or the safety shutdown for a high pressure boiler, **you can’t address what you don’t know is broken.**

Fault Detection / Consequence Prevention: Definitions

- **Fault:** The partial or total failure of a device.
- **Detection:** The ability to recognize the functional ability of a device.
- **Consequence:** Something produced by a cause or following from a set of conditions.
- **Prevention:** The ability to overcome an undesirable outcome from a given set of conditions or circumstances.

Failure Modes

- **Fail-Action (Fail-Safe):** If a fault occurs or the energy source is lost, the protective system initiates the protective action. Also known as a de-energize to trip design.

- **Fail-No-Action (Fail-to-Danger):** If a fault occurs or the energy source is lost, the protective system will not be able to take the desired protective action. Also known as an energize-to-trip design.

Fault Detection

- **Deviation Alarm**:
  - Value of the sensor is automatically compared with redundant sensors for validity checking.
  - If the difference exceeds a preset tolerance, an alarm is triggered.

- **Diagnostics**:
  - Real-time artificial intelligence that compares current status bits for conformance with pre-defined rules.
  - Alarms are generated whenever the rules are violated.

Fault Detection
(continued)

- **Testing:**
- Simulated process demand conditions are imposed on the system to verify functionality & find any hidden faults.
- Provisions are made in the design to facilitate on-line testing as much as possible.
- If a fault is detected, repairs are made ASAP to restore full protective functionality.
- In cases where repairs cannot be readily accomplished, alternate protection is placed in service or operations are taken to a stable, safe state until the repairs can be made.

Control of Defeat

- **Control of Defeat (COD):**
- Whenever a protective device is taken out of on-line service for Testing, PM, or repair, a system known as Control of Defeat is employed.
- COD system specifies the alternate protection to be used while the device is out of service, notifies all potentially impacted personnel, and requires written approval for Defeating the device.
- Once the device is returned to on-line service, the Defeat system is closed out and normal operations resume.

COD Failure Example

- "The (collision warning) system was not working at the time," said Roger Gaberelle, a spokesman for Skyguide, the Swiss air traffic controllers in charge of airspace over southwestern Germany.
- (Reuters) - “Swiss air traffic controllers said on Wednesday an automatic collision warning system had been switched off for maintenance when two jets crashed into each other over Germany, killing 71 people.” (July 02)

COD Failure Example

(continued)

Fault Tolerance

- **Redundancy:** The ability to tolerate faults is enhanced by the use of multiple components. This includes such things as redundant sensors/logic solvers/output devices.
- **Multiple Sensors:** Multiple input devices which can be used for voting/validity checking/median value selection.
- **Independent Technologies:** Use of different sensor/ output types to avoid common cause failure modes.

Fault Tolerance
(continued)

- **Triple Modular Redundant (TMR):** Three independent PLC's used in a 2-o-o-3 (2-out-of-3) voting arrangement such that the loss of any single processor will not result in loss of the protective function, nor in an unnecessary trip of the protected equipment.
- **Redundant Outputs:** Two or more final elements, each independently capable of providing the desired protective function, used in tandem with each other.

Fault Tolerance
(continued)

- **Simplex System** (single input/single logic solver/ single output): A single fault results in the loss of protection and/or unnecessary shutdown.

- **Redundant System** (multiple inputs/multiple processors/multiple outputs): A single fault will result in an immediate alarm but will not result in loss of protection nor in an unnecessary shutdown.

Fault Tolerance
(continued)

- Fault tolerant designs to avoid common cause failures for multiple I/O and logic solvers:
- - Use of separate taps for multiple sensors
- - Use of multiple power sources
- - Distribution of I/O to prevent single card failure from impacting all I/O related to a single function
- - Use of redundant/distributed wiring paths
- - Environmental controls for moisture, lightning, etc
- - Rigorous factory acceptance and site use testing.

Fault Tolerance
(continued)

- **Fault Tolerant Designs/Methods:**
- - Use of analog transmitters versus switches
- - Use of sealed capillary transmitters versus wet-leg sensors
- - Positive feedback on output circuits
- - Slight time delay on most trip inputs
- - Fireproofing on critical actuators/circuits to give increased operating time before failure in the event of a fire

Fault Tolerance / Consequence Prevention
(continued)

- Interactive training of operations/maintenance personnel on protective system operation
- Simulated emergency training, both initial and refresher.
- Evergreen review of protective system adequacy based on unit changes, performance history, unit manning, etc.
- Design verification through both qualitative and quantitative review exercises.

Fault Response

- **Covert Faults:** Hidden or non-self revealing faults. Since there is no fault detection, there is no fault response. This could result in a fail-to-danger situation. Such a fault would normally only be found during periodic manual Testing w/o smart diagnostics.

- **Overt Faults/Simplex systems:** Obvious or self-revealing faults. Overt faults in simplex systems normally result in an unnecessary shutdown. The majority of protective system designs are fail-safe, so the process goes to the safe state upon a single overt fault condition.

Fault Response
(continued)

- **Overt Faults/Redundant Systems:**

- - Normal result of a single overt fault is an alarm with a degradation from a 2-o-o-3 voting system to a 1-o-o-2 voting system.
- - Any subsequent fault would result in the designed protective system action.
- - The protective system may take additional precautionary action to minimize the consequences of any further faults as shown on the following slide.

Fault Response
(continued)

- **<u>Overt Faults/Redundant Systems</u>: (continued)**
  - Upon fault detection, the system may take one of a number of options, depending on fault and potential consequence:
    * Continue at full production rates with alarm only
    * Gracefully decrease process to lower rates
    * Implement a total process shutdown.

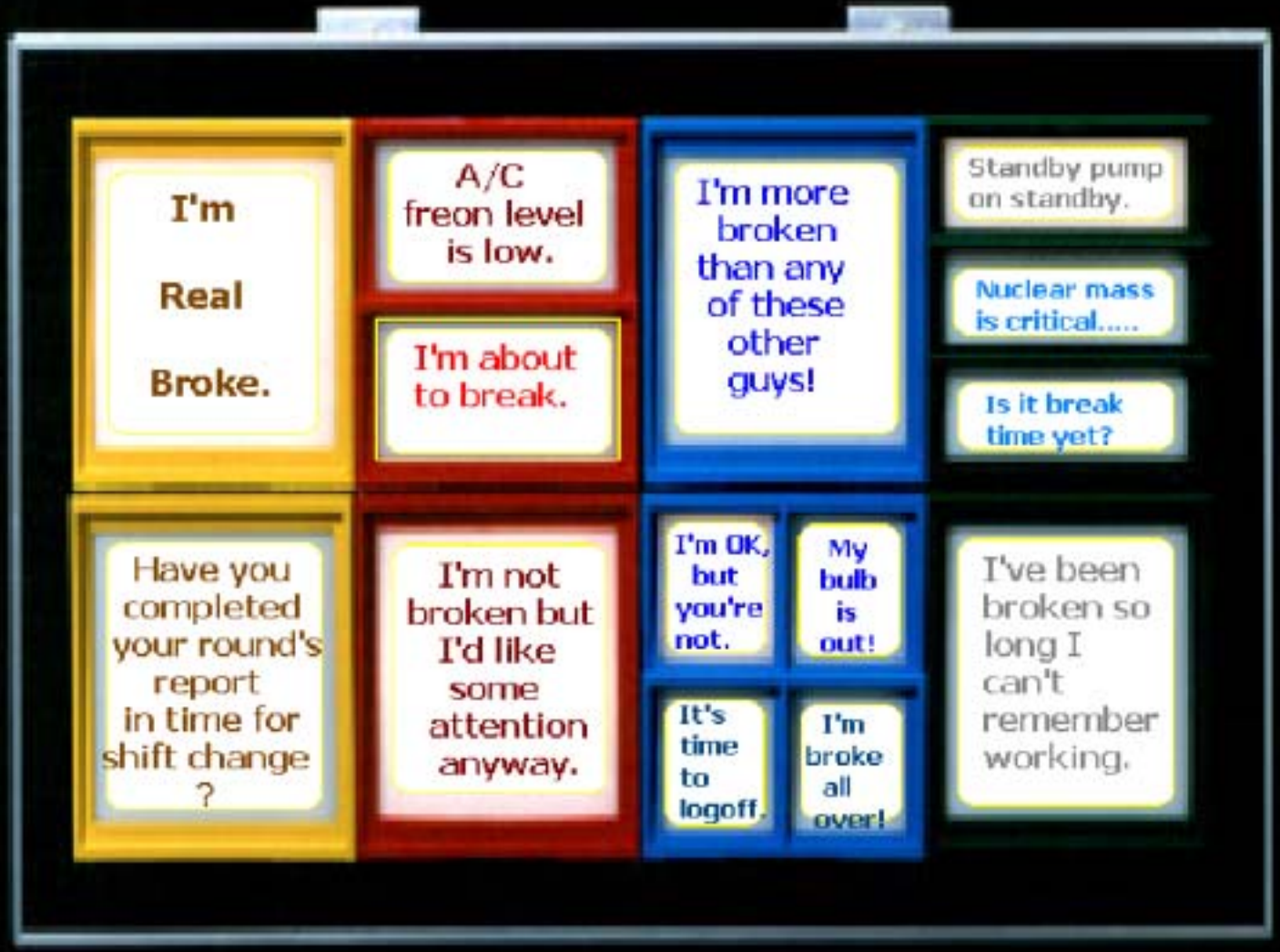
- Upon fault detection, a COD would be implemented, alternate protection put in place, and repair would be implemented ASAP to restore functionality and reliability.

Wish List Items

- Improved alarm suppression to prevent the major alarm flood associated with a rapidly degrading process situation:
- Safety Critical alarms always remain active
- Operations Critical alarms temporarily suppressed by conscious operator action.
- Operations Important alarms automatically suppressed until sufficient process stability returns.

Alarm Flood Example

(**Highly** Exaggerated for Effect)



Wish List Items
(continued)

- Improved diagnostic capabilities for sensors, logic solvers, and final elements. This includes process condition sensing, such as for leadline fouling, icing, valve sticking, etc. Additional / advanced use of artificial intelligence would be one possibility for further enhancements in this area.

Wish List Items
(continued)

- Improved on-line, self-testing capability of sensors and final elements:
- - Testing needs to be non-disruptive to process but sufficient to be representative of device capability
- - Automatically initiated (time or condition based) and self-documenting

Wish List Items
(continued)

- Guidelines/standards around the use of spread spectrum radio equipment for critical system applications. IEEE has done some preliminary work in the general area of industrial use but none yet specifically concerning protective system usage.

Wish List Items

(continued)

Where are the most faults occurring in protective systems?

Sensor

40 %

Logic Solver

5%

Final Element

55 %

Wish List Items

(continued)

Where is the lion's share of research in reliability/diagnostics/base innovations being seen?

Sensor

25 %

Logic Solver

60%

Final Element

15 %

Summary

- Joint discussions such as this workshop afford us with the opportunity for academia/industry to gain a deeper joint understanding of the needs in the safety system area and to plant the seeds for the growth of possible solutions.
- By the two of us working together, we can provide control suppliers with ideas/ways to improve the ability to detect and tolerate faults in protective systems while maintaining the **SAFETY** and **RELIABILITY** required to meet the process and human demands of industry and society as a whole.

Thanks for Your Interest !