knowledge

Honeywell

2015 Honeywell Users Group Americas
Forty Years of Innovation.

Why not in my DCS?

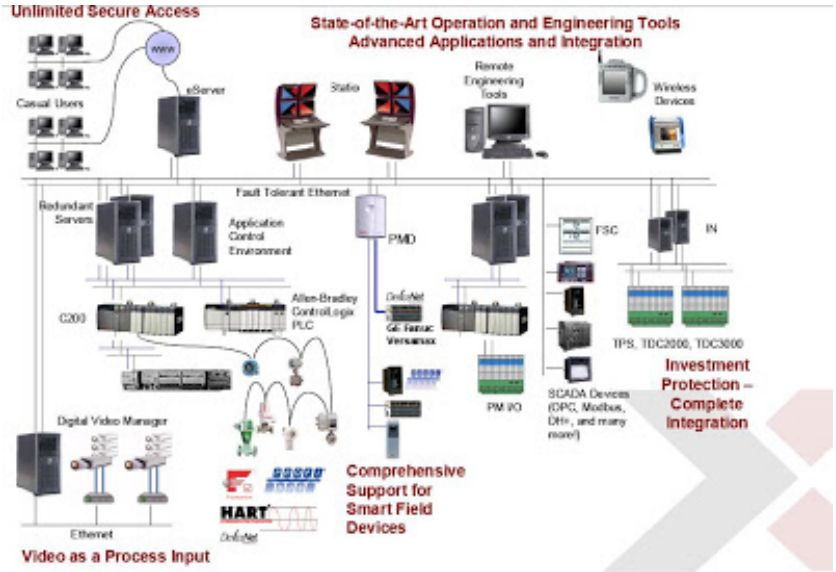
Critical safety safeguards in a DCS are not a good idea

Leoncio Esteves-Reyes, Performance Materials Technologies

Introduction

Honeywell

- If I have this

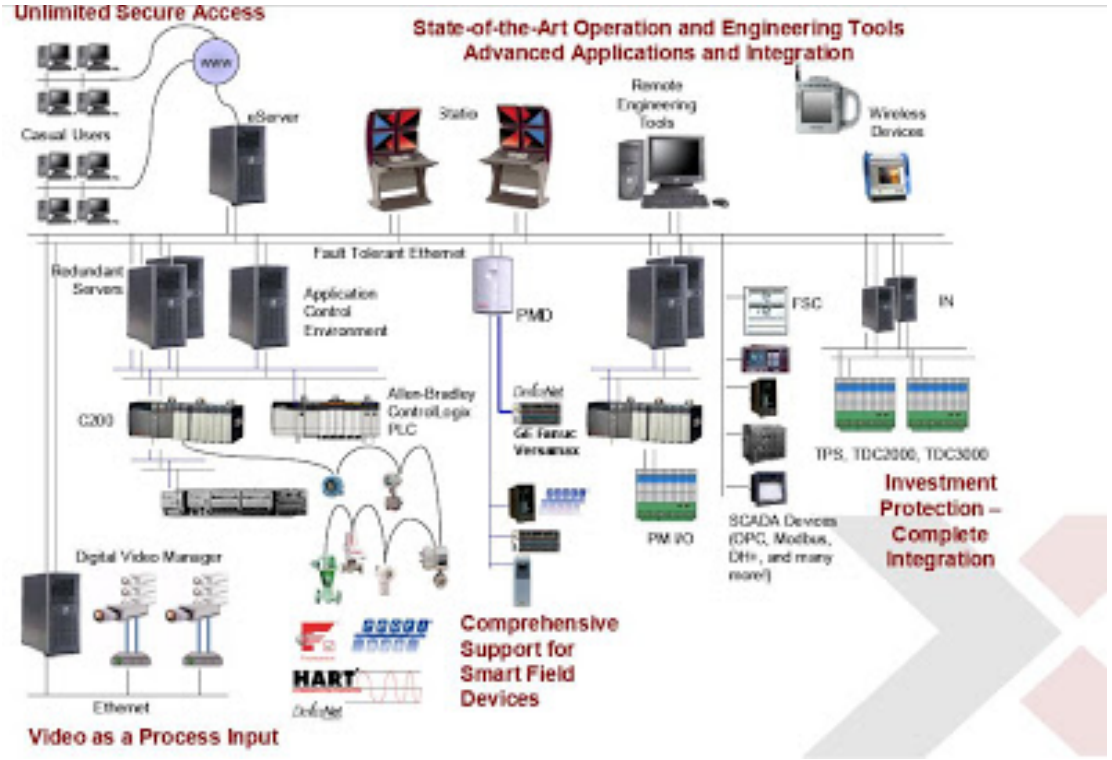


- Why do I need that?

This is your DCS' mission

Honeywell

- Drives plant operations within normal range
- Always acting: sensing and intervening
- Generates actions and alarms
- Informs, so operators can act

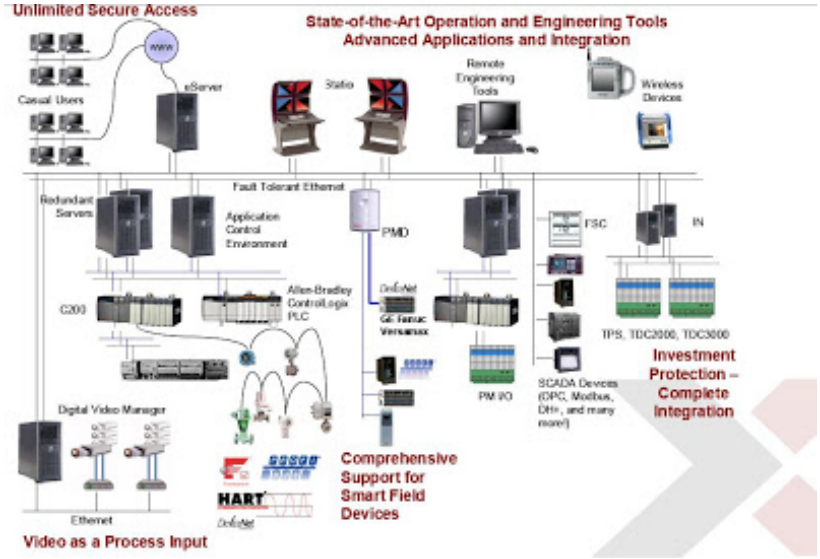


Can the DCS act like an SIS?

Honeywell

- With the right coding, will this…

…become that?



Let’s check for compliance

Honeywell

IEC 61508 written to help design and develop SIL rated products for any industry.

IEC 61511 and ISA84.00.01 (almost identical) written to help analyze, design, implement, install, commission and maintain SIL loops for the Process industry.

IEC 61511 (ANSI-ISA 84) says

Honeywell

An SIS:

- Implements SIF(s) to keep the process safe
- The SIF(s) are defined by their SIL
  - Success rate at keeping process safe state
  - Four levels of probability
- Is composed of three elements
  - Sensors, Logic Solvers and Actuating Devices

What about the SIL?

Honeywell

SIL:

- Four levels used to specify SIS requirements
- Based on probabilities of success over time

SIL Levels:

- 1 → Lowest
- 4 → Highest

Standards say this is SIS' mission

Honeywell

- **Brings process back from the brink and takes the process to a safe state**
- **Acts infrequently and sparingly**
- **Only informs after taking corrective action**

Let’s compare BPCS and SIS

Honeywell

Hardware:

- Redundancy
- Failure
- SIL

Software:

- Programming language
- Firmware
- Diagnostics
- Application complexity

Let’s compare BPCS and SIS (II)

Honeywell

Functionality:

- Main use
- Demand
- Place as protection layer
- Controller interactions
- Response time

Let’s compare BPCS and SIS (III)

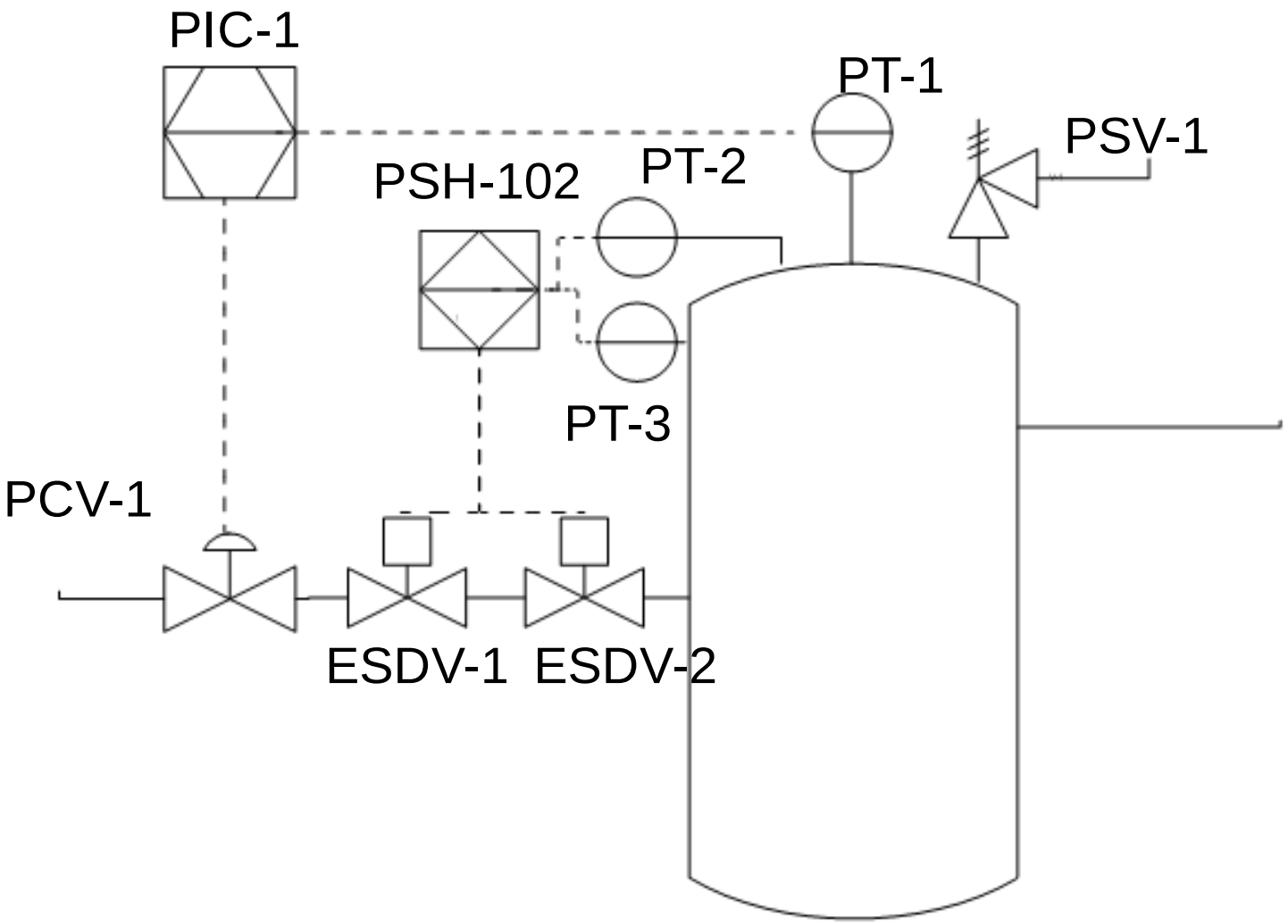
Honeywell

Operator Intervention:

- Management of Change (MOC)
- Operator mistakes
- Logic changes
- Handling by-passes

An application from industry

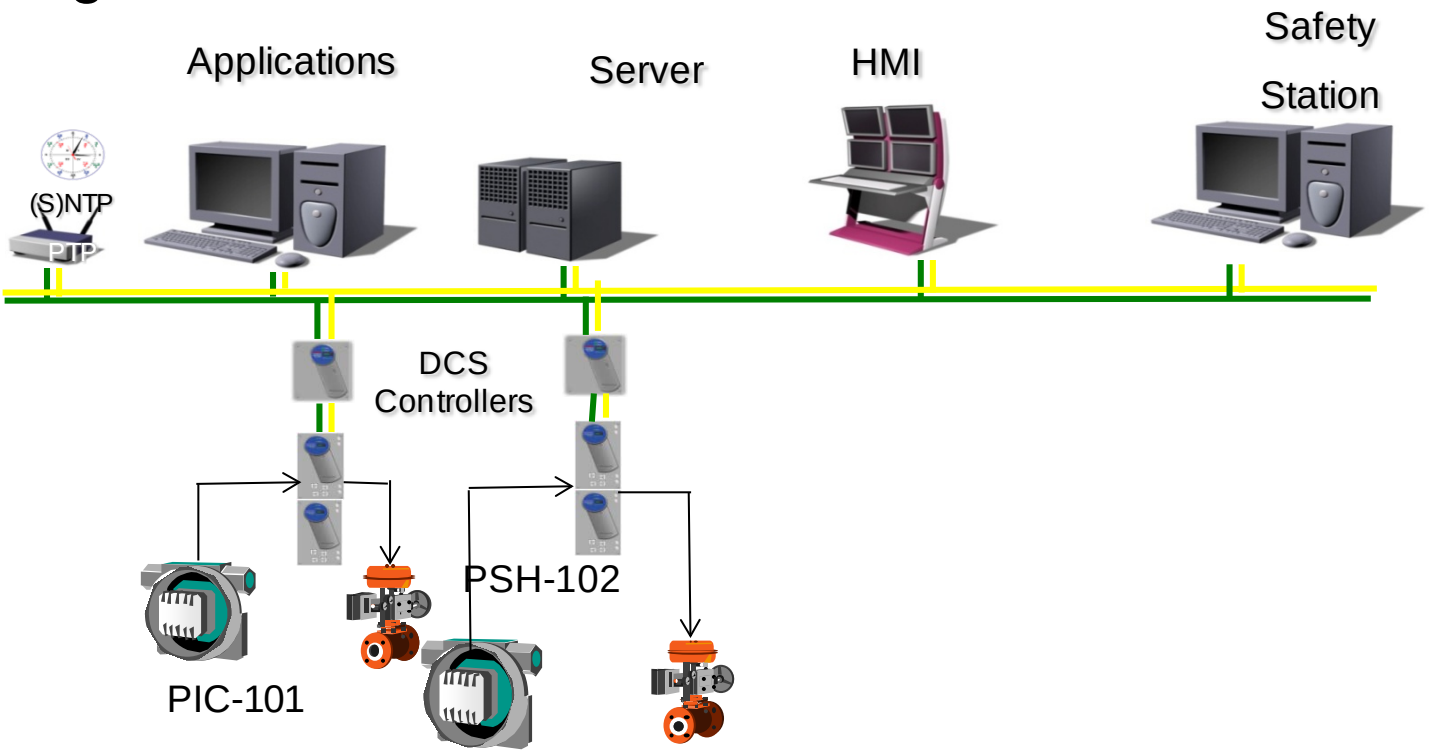
Honeywell



BPCS credits

Honeywell

- So why is BPCS given ONLY ONE credit in ISA 84.00.01 ?
- Why can't I take additional credit if I have a configuration as below for PIC-101 and PSH-102 ?

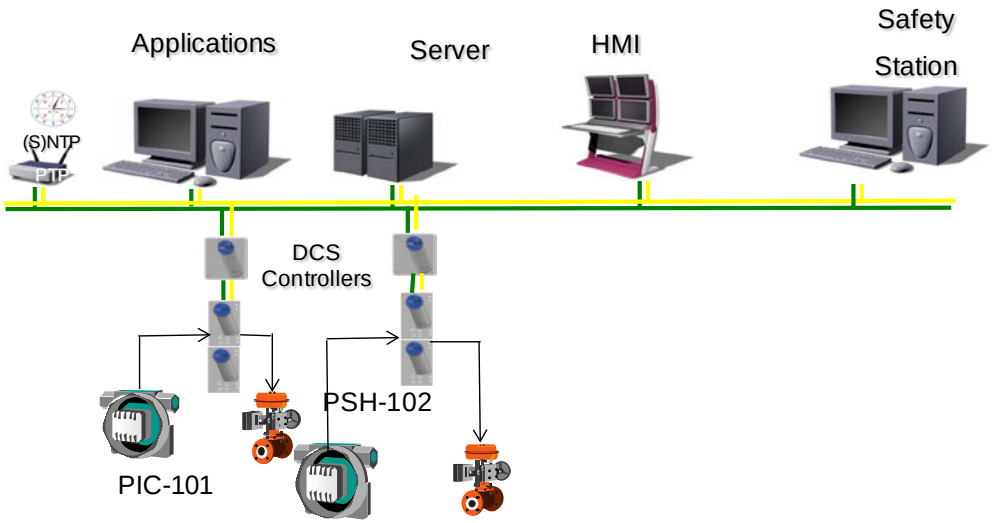


For BPCS, let's see what happens if…

Honeywell

Operator Intervention:

- Puts 101 in manual and, after a few days…
- PSH-102 is by-passed



Application Software:

- New "Go To" loop applied before PSH-102 logic…
- Never validated (not required)

For BPCS, let's see what happens if… (II)

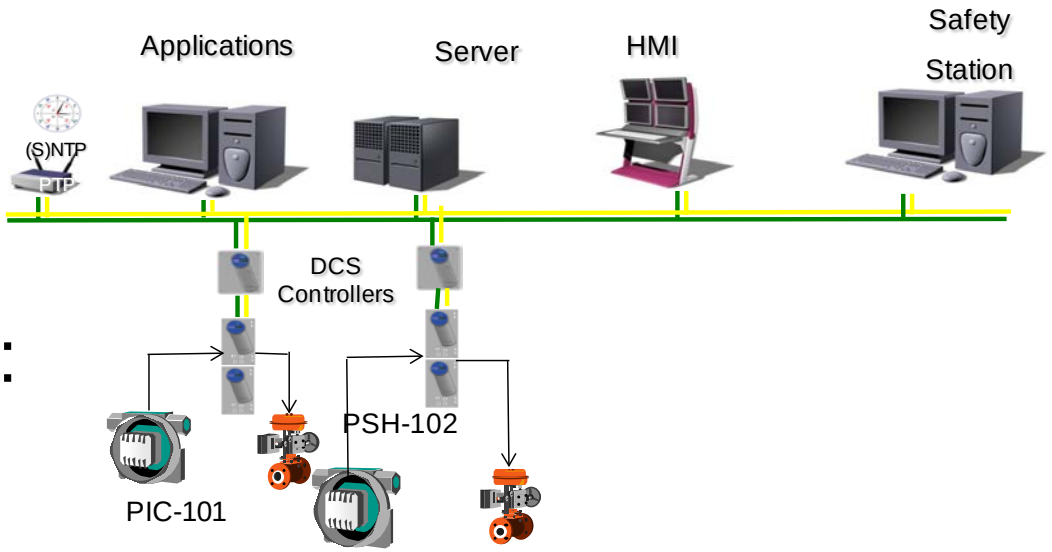
Honeywell

Firmware:

- **DCS OS is upgraded and…**
- **Bug affects all PID controllers**

Third Party Interface:

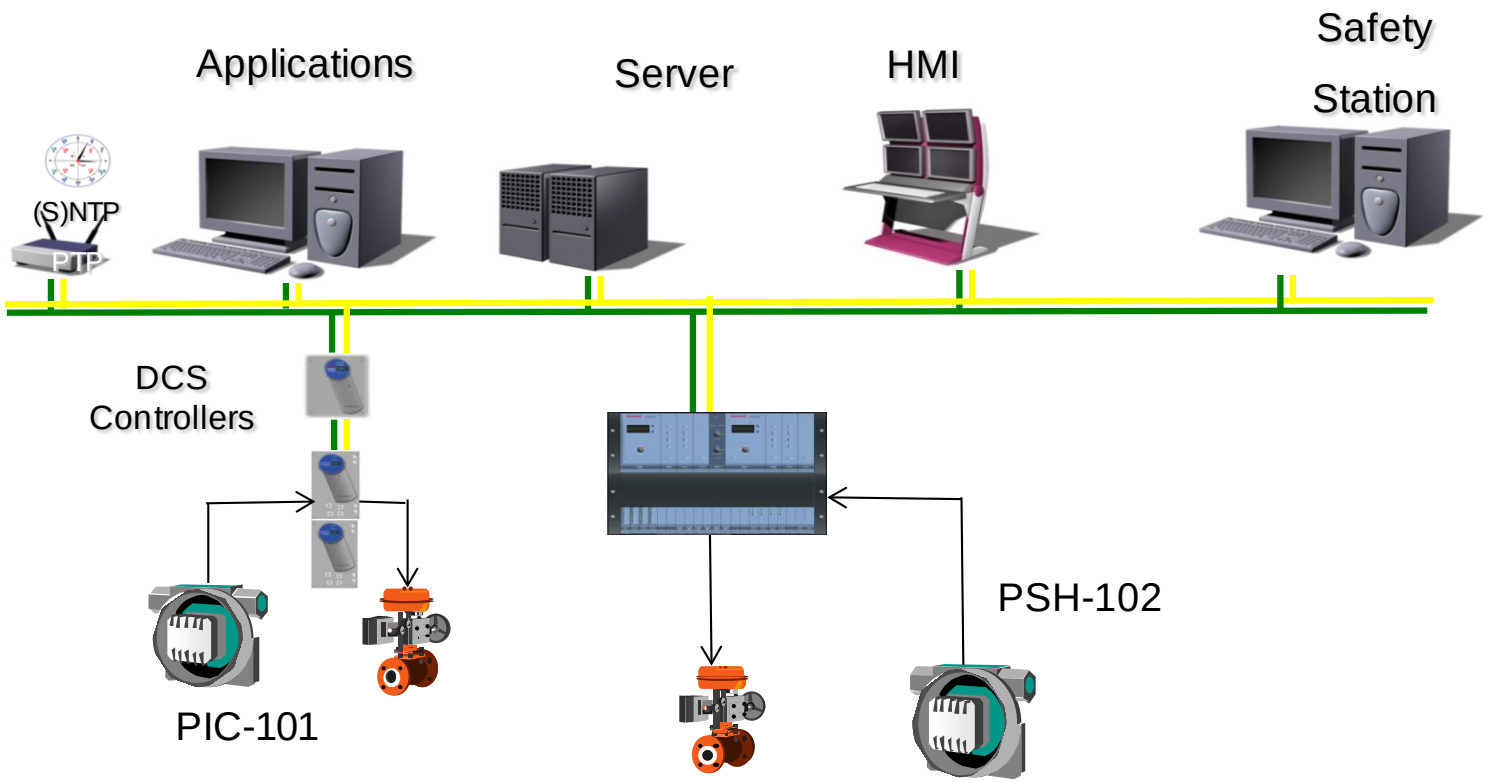
- **A local PLC sends a garbled message to DCS…**
- **Local logic is affected**



SIS credits

Honeywell

- PIC-101 is part of BPCS
- PSH-102 is part of SIS



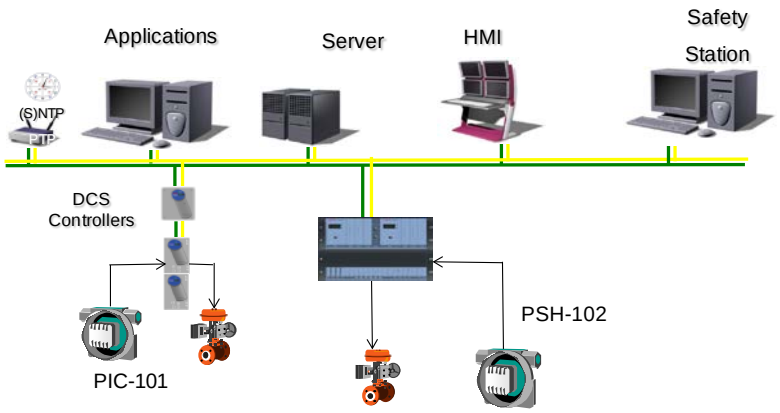
Let's see what happens if…

Honeywell

Operator Intervention:

- **Puts 101 in manual and, after a few days…**
- **PSH-102 in SIS is by-passed**

- PIC-101 is part of BPCS
- PSH-102 is part of SIS



Application Software:

- **New "Go To" loop applied before PSH-102 logic in SIS**

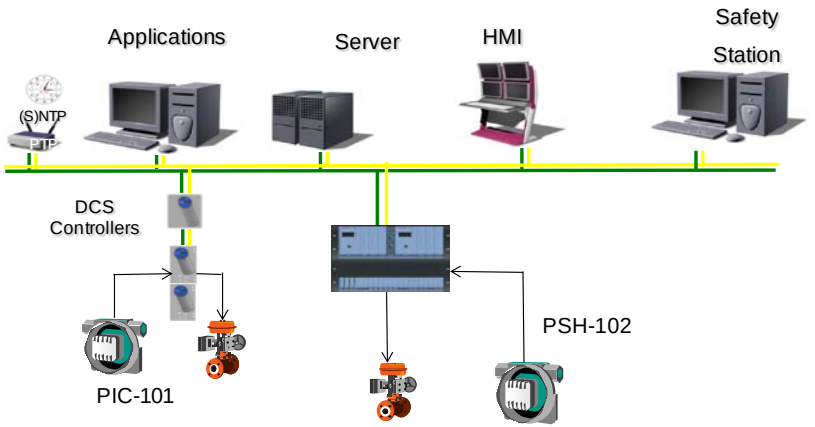
Let's see what happens if… (II)

Honeywell

Firmware:

- **DCS OS is upgraded and SIS OS upgraded…**
- **Bug affects all PID controllers**

- PIC-101 is part of BPCS
- PSH-102 is part of SIS



Third Party Interface:

- **A local PLC sends a garbled message to DCS…**
- **Local logic is affected**

To avoid risks and disaster

Honeywell

Need to add or modify DCS

- Add diagnostics
- Modify firmware
- Forbid operator changes
- Forbid exchanges with other controllers

In other words:

Redesign the DCS to make it behave as an SIS

Why bother if we already have designed SIS'?

Conclusions

Honeywell

BPCS and SIS have distinct and specific roles

Let's leave each do its job

The standard is clear about the characterization of a BPCS, as a system

"…which does not perform any safety instrumented functions with a claimed SIL ≥ 1"