CSA SINGAPORE | SG Passion Made Possible

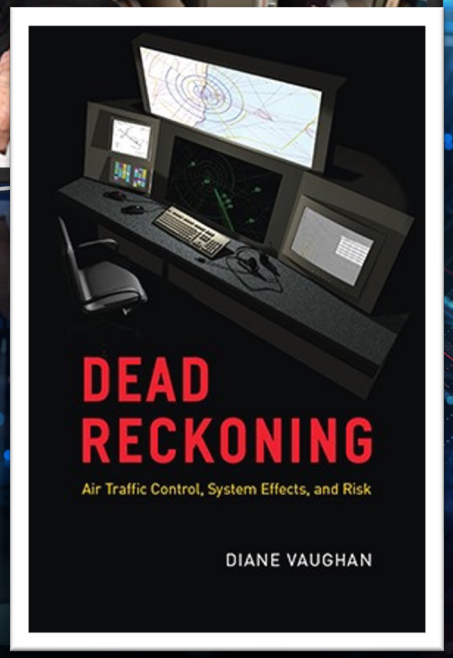
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

22 – 23 AUGUST 2023

Normalization of Deviance in the Confluence of Process Control, Safety Systems, and Remote Internet Access

What is Normalization of Deviance?

Dr. Diane Vaughn



- In the understanding of safety and risk, Vaughan is perhaps best known for coining the phrase "normalization of deviance", which she has used to explain the sociological causes of the NASA Challenger and Columbia disasters.
- Dr. Vaughan defines this as a process where a clearly unsafe practice comes to be considered normal if it does not immediately cause a catastrophe:

... "*a long incubation period [before a final disaster] with early warning signs that were either misinterpreted, ignored or missed completely*.

How Did We Get Here?

OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

How Did We Get Here?

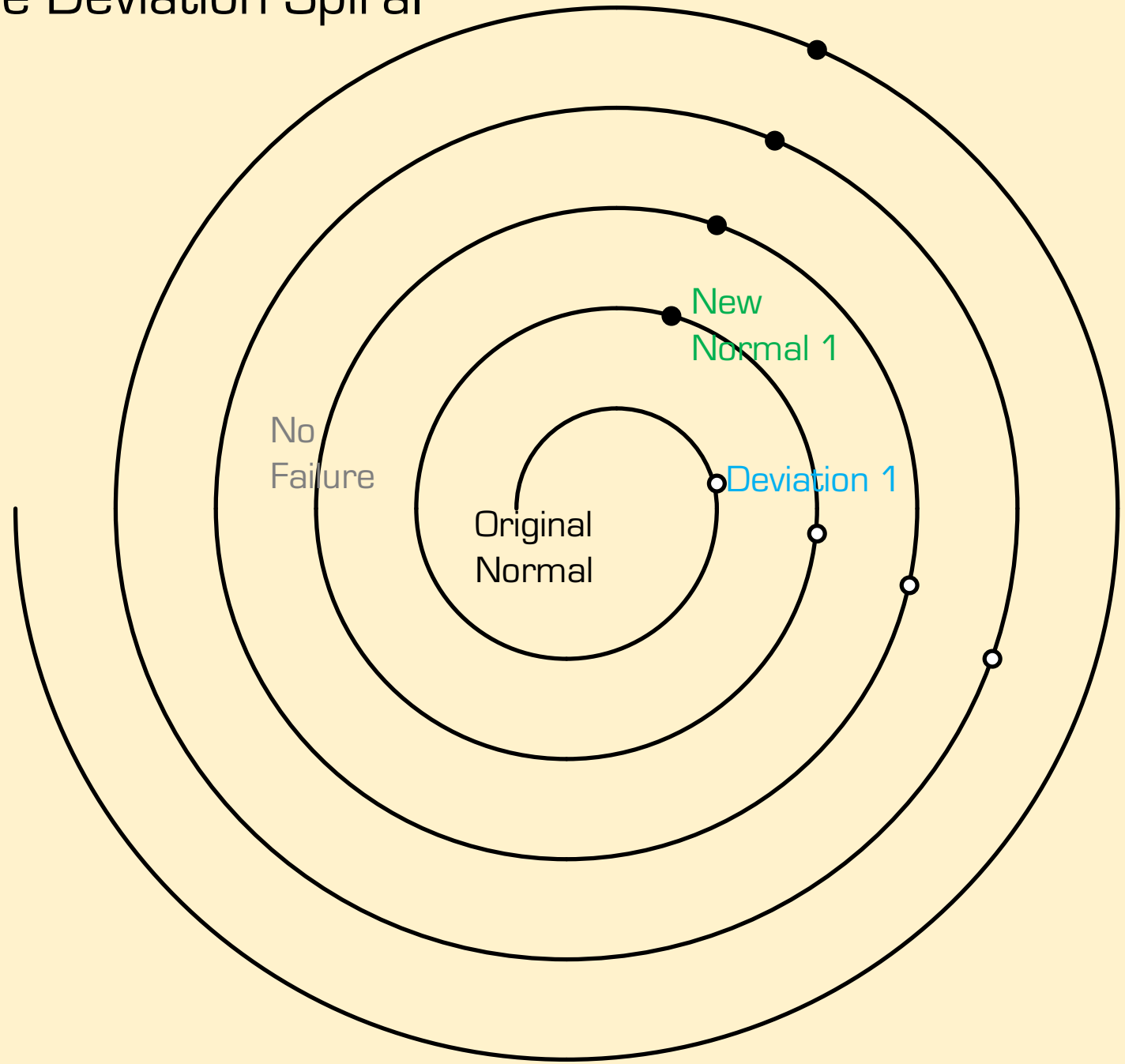
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

1st Generation Safety Systems

- Introduced in the late 1980's
- Special purpose "Safety PLCs" introduced to improve safety and availability
- Employ redundancy and voting techniques (2oo3 or TMR) to enhance safety and availability
- TÜV certified to DIN/VDE standards (AK1-AK6)
- Serial / proprietary bus hi/lo level communications
- Examples:
- Triconex Tricon
- ICS Triplex Regent
- August Systems

The Deviation Spiral

1st Generation Systems – 1980's



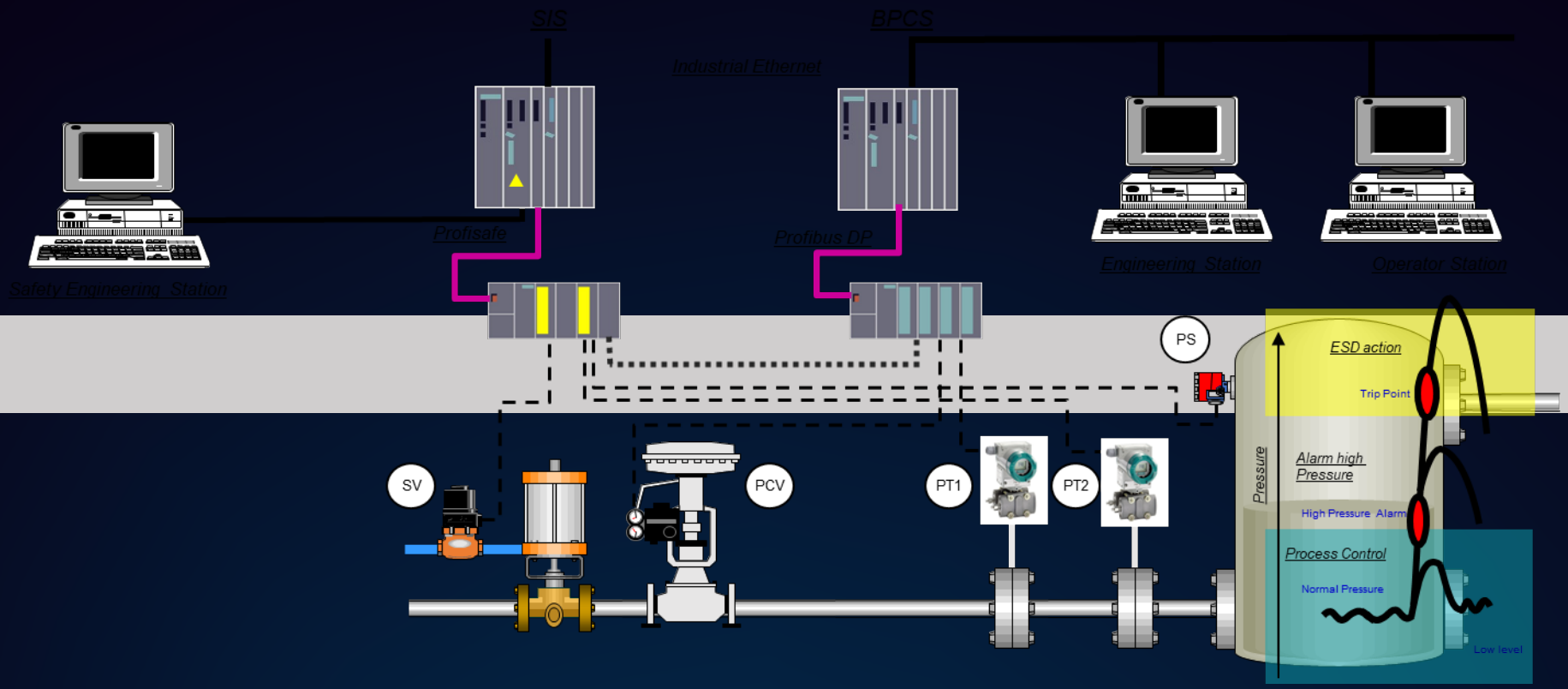
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

2nd Generation Safety Systems

- Introduced in the 1990's
- Employ high levels of self-diagnostics (D) coupled with redundancy and voting techniques (1oo2D or DMR) to provide comparable levels of safety & availability with less hardware (lower cost) than 1st Generation systems
- TÜV certified to DIN/VDE (AK1-AK6) and IEC 61508 (SIL1 –SIL3) standards
- Windows-based IEC 61131-3 Programming Tools
- Improved integration with DCS systems
- Serial / proprietary bus hi/lo level communications, and 10BaseT
- Examples:
- Moore QUADLOG
- HIMA H41q/H51q
- ABB Master Safeguard

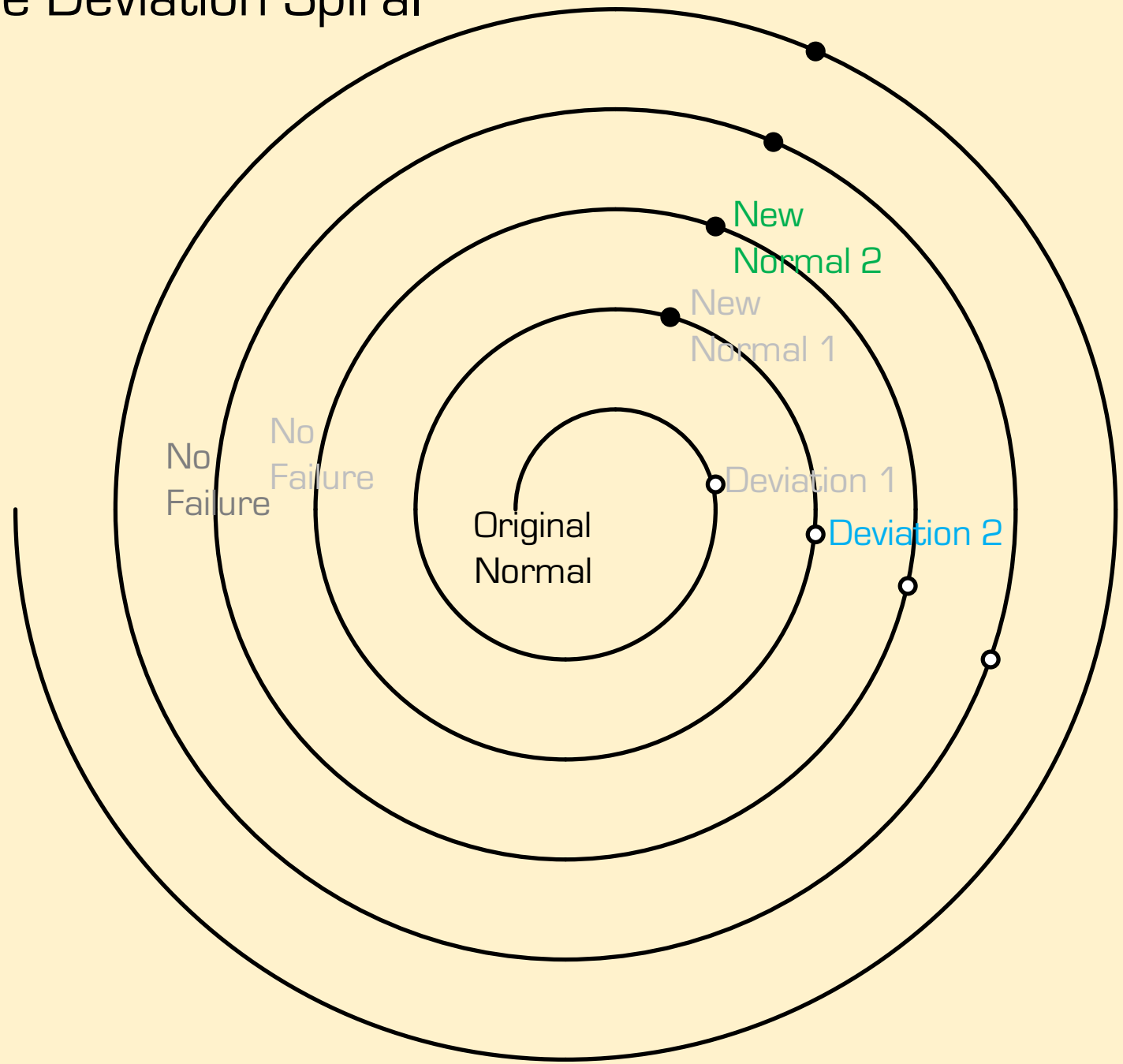
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Deviation 2, New Normal 2



Courtesy of Siemens USA

The Deviation Spiral



1st Generation Systems – 1980's

2nd Generation Systems – 1990's

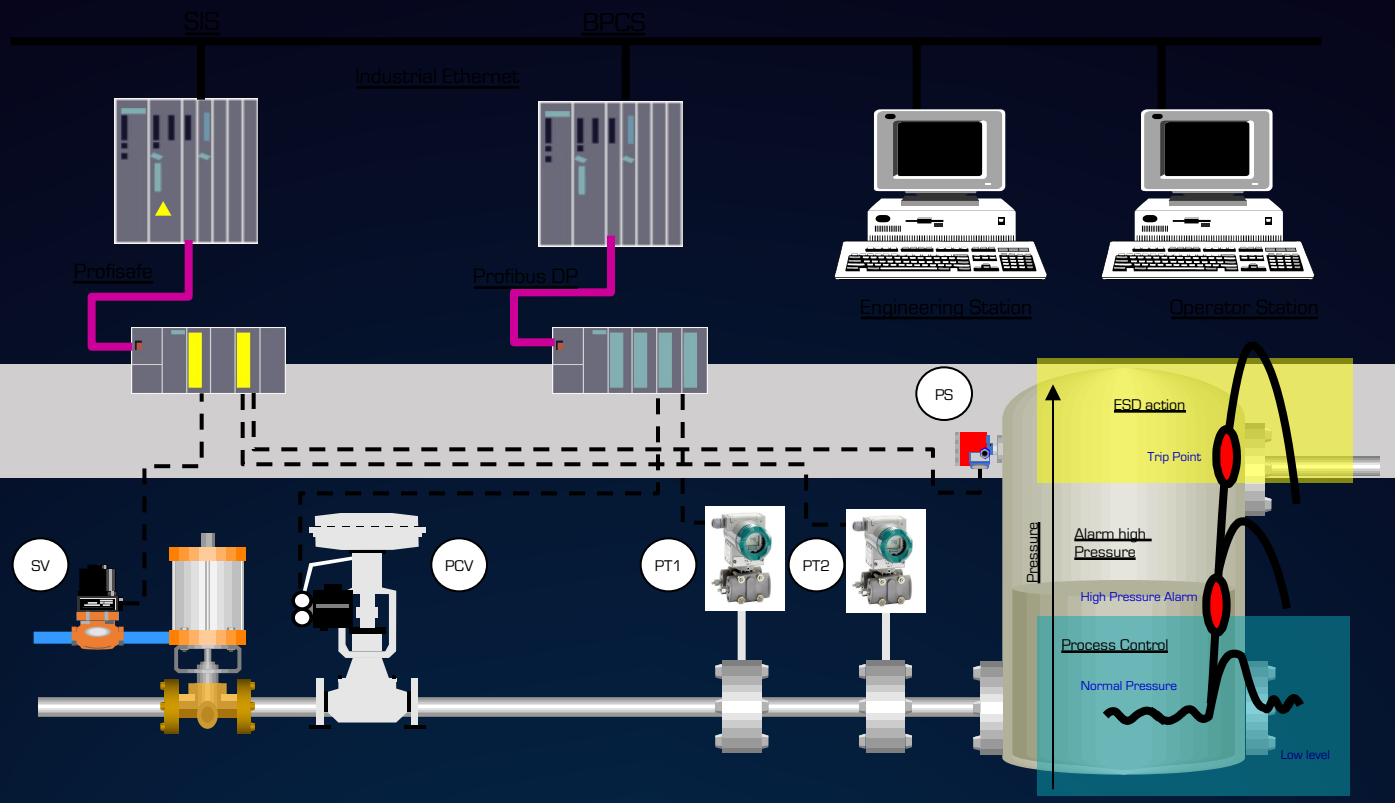
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

3rd Generation Safety Systems

- Introduced in the early 2000's
- Employ very high levels of self-diagnostics (D) to achieve high safety
- Highly modular and scalable
- TÜV certified to IEC 61508 (SIL1 – SIL3) standards
- All offer tight integration with respective DCS systems
- Some offer advanced programming tools
- Some integrate safety fieldbus technology
- Examples:
- Siemens PCS7F S7-F/FH
- Emerson DeltaV SIS
- Yokogawa ProSafe-RS

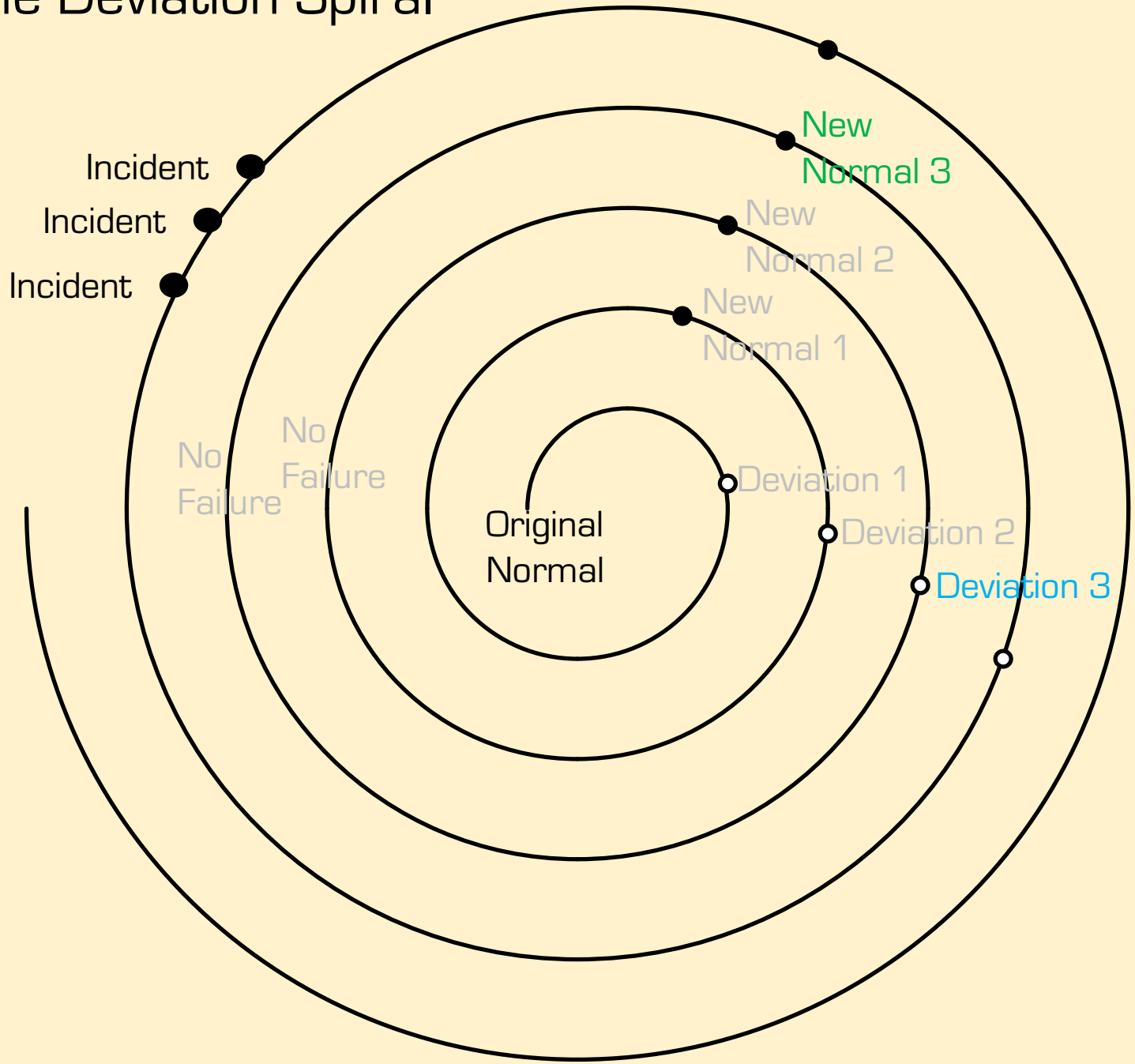
OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Deviation 3, New Normal 3



Courtesy of Siemens USA

The Deviation Spiral



1st Generation Systems – 1980's

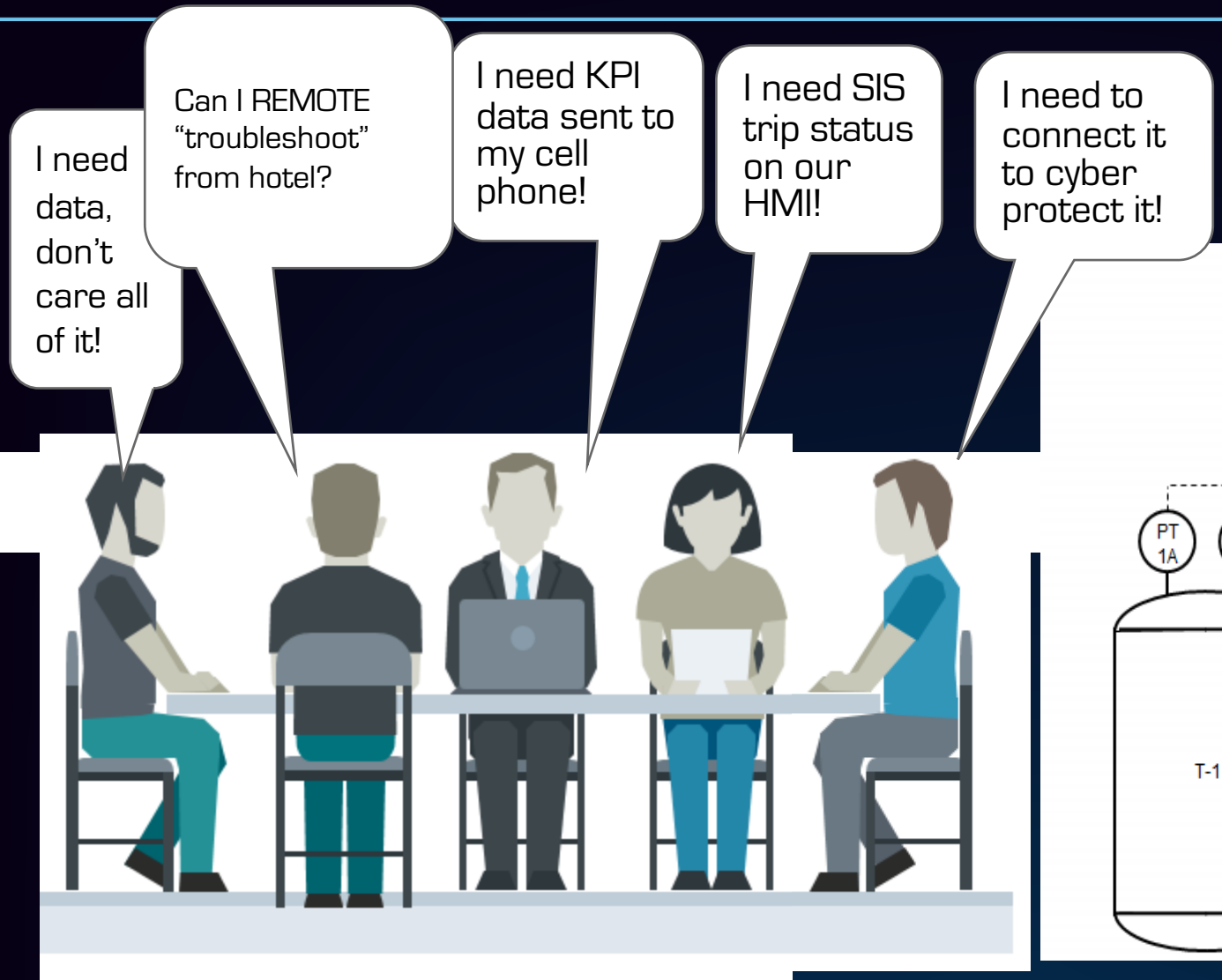
2nd Generation Systems – 1990's

3rd Generation Systems – 2000's

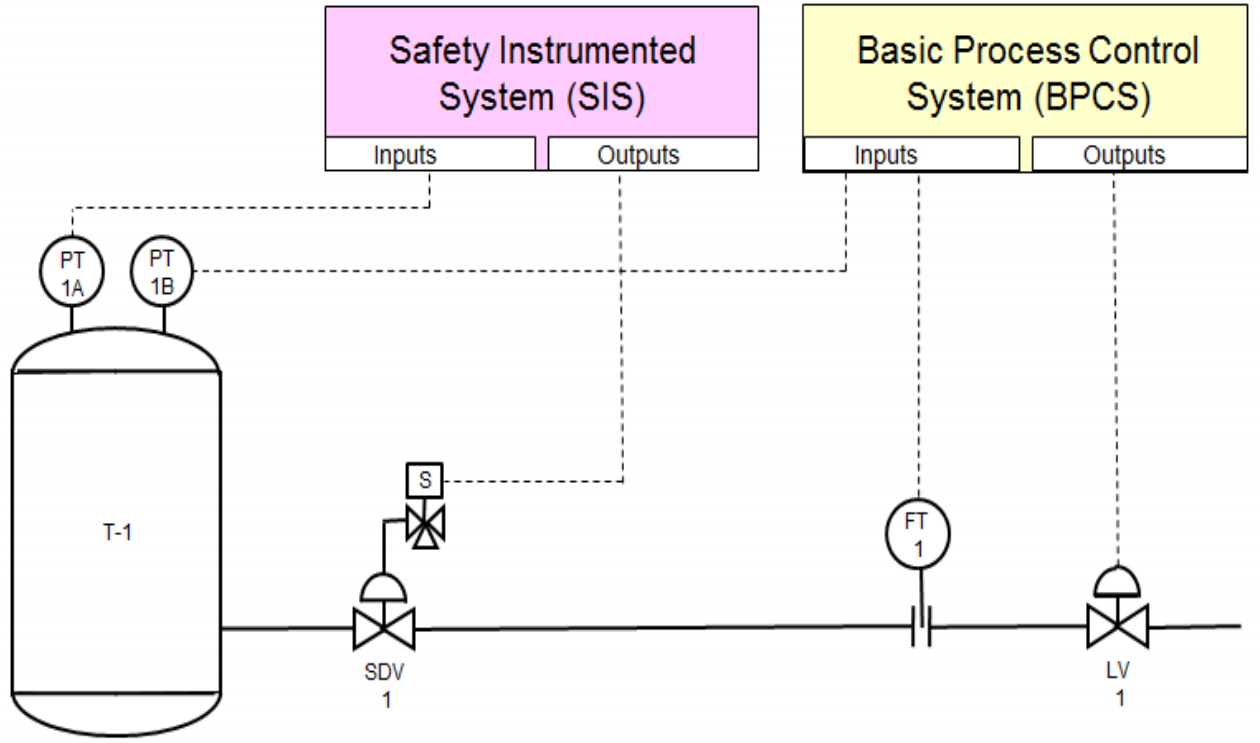
- 2002 – ISA99 Committee is Established
- 2007 – ANSI/ISA 62443-1-1 (99.01.01); Terminology, Concepts, and Models
- 2009 – ANSI/ISA 62443-2-1 (99.02.01); Establishing an Industrial Automation and Control Systems Security Program
- 2013 – ANSI/ISA 62443-3-3 (99.03.03); System Security Requirements and Security Levels
- 2013 – NIST Special Publication 800-82, Rev 1; Guide to Industrial Control Systems (ICS) Security
- 2015 – NIST Special Publication 800-82, Rev 2; Guide to Industrial Control Systems (ICS) Security
- 2018 – ANSI/ISA/IEC 62443-2-4; Security Program Requirements for IACS Service Providers
- 2018 – ANSI/ISA/IEC 62443-4-1; Security Product Development Lifecycle Requirements
- 2019 – ANSI/ISA/IEC 62443-4-2; Technical Security Requirements for IACS Components
- 2020 – ANSI/ISA/IEC 62443-3-2; Security for industrial automation and control systems, Security risk assessment for system design
- 2022 – NIST Special Publication 800-82, Rev 3ipd; Guide to Operational Technology (OT) Security

- 1987 - English Health & Safety Executive; Programmable Electronic Systems for use in Safety Applications
- 1993 - AIChE CCPS; Guidelines for Safe Automation of Chemical Processes
- 1996 - ANSI/ISA 84, S84.01:1996; Application of Safety Instrumented Systems for the Process Industries
- 1998-2000 - IEC 61508; Functional safety of electrical/electronic/programmable electronic safety-related systems (multiple parts)
- 2003 - IEC 61511; Functional safety: Safety Instrumented Systems for the process industry sector
- 2004 - ANSI/ISA-84.00.01-2004 (IEC 61511-1 Mod); Functional safety: Safety Instrumented Systems for the process industry sector
- 2010 - IEC 61508-1thru4; Functional safety of electrical/electronic/programmable electronic safety-related systems (multiple parts)
- 2016 - IEC 61511-2; Functional safety: Safety Instrumented Systems for the process industry sector + Cyber clauses
  - 2017 –ISA-TR84.00.09 – Cybersecurity Related to the Functional Safety Lifecycle
- 2019 - NFPA 85 - Boiler and Combustion Systems Hazards Code

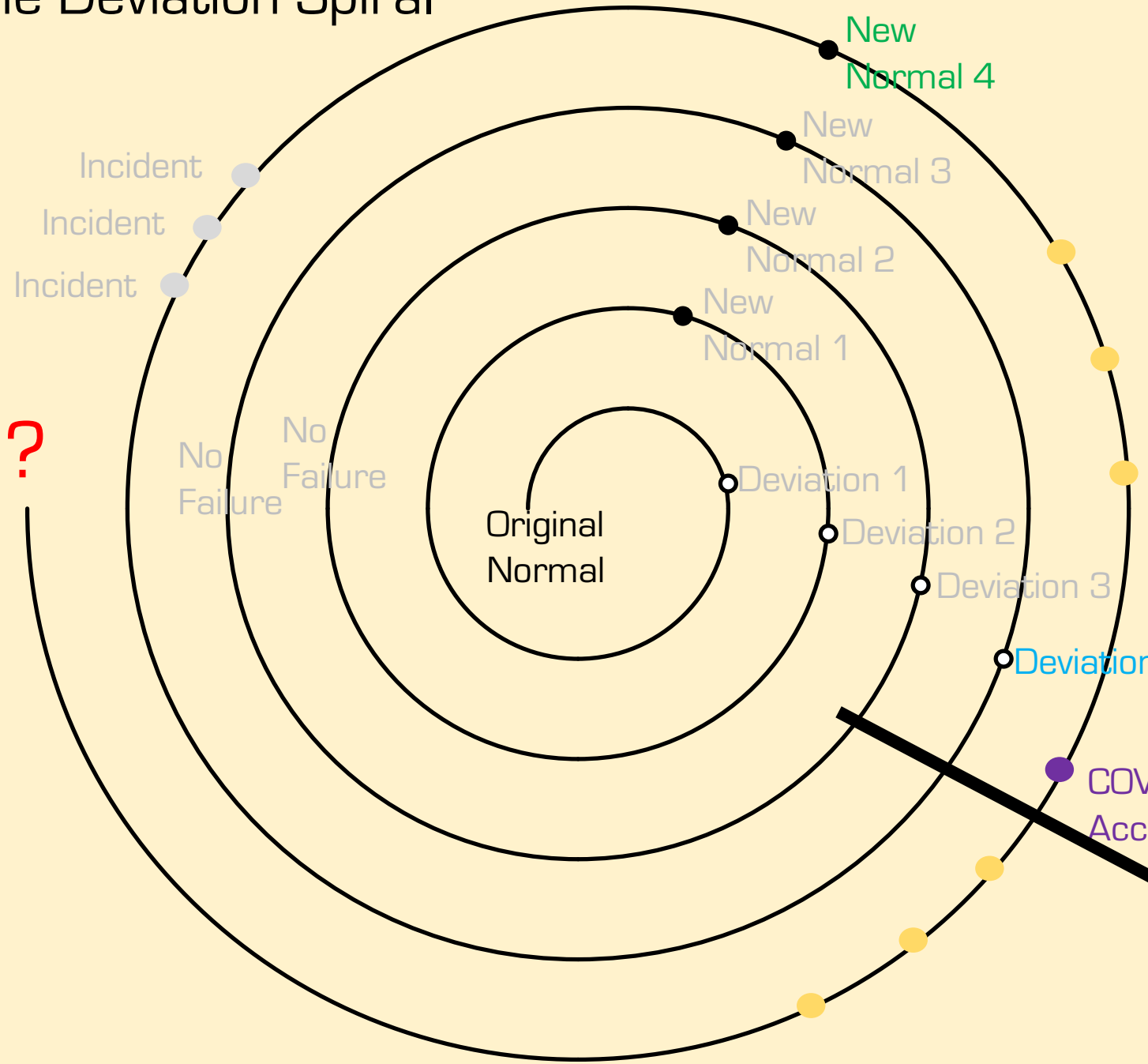
Deviation 4, New Normal 4



A system composed of sensors, logic solvers, and final control elements for the purpose of taking the process to a safe state when pre-determined conditions are violated.



The Deviation Spiral

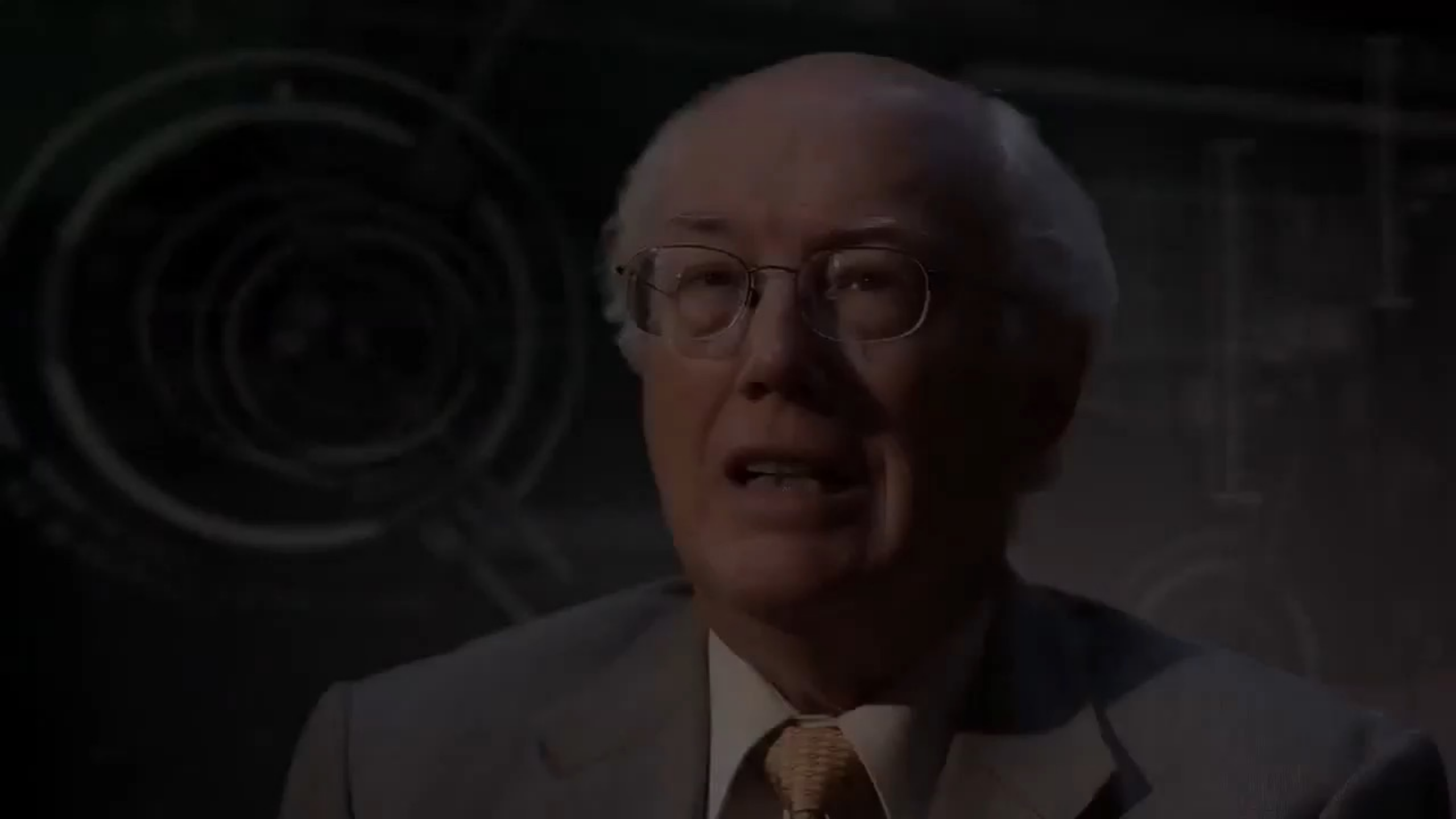


1st Generation Systems – 1980's

2nd Generation Systems – 1990's

3rd Generation Systems – 2000's

4th Generation Systems – 2020 - NOW



OPERATIONAL TECHNOLOGY CYBERSECURITY EXPERT PANEL FORUM 2023

Cyber-informed Engineering, CSA - CCoP2.0, ISA/IEC 62443

- Consequence-Focused Design
- Engineered Controls
- Secure Information Architecture
- Design Simplification
- Resilient Layered Defenses
- Active Defense
- Interdependency Evaluation
- Digital Asset Awareness
- Cyber-Secure Supply Chain Controls
- Planned Resilience
- Engineering Information Control
- Cybersecurity Culture

The Future is up to YOU!

Embrace a bright future by proactively recognizing and rectifying normalization of deviance.

Cultivate a culture of growth, where learning from past deviations becomes a stepping-stone to excellence.

Together, we can celebrate the power of continuous improvement, forging a path toward safer, more innovative, and extraordinary achievements!

Upcoming CIE Presentations and Outreach

Save the Date: Cyber-Informed Engineering Practitioner's Workshop

– Multiple presentations and panels for CIE practitioners

Cyber-Informed Engineering ***Practitioner's Workshop***

Save the Date

Sept. 6, 2023
11am - 5pm ET

Register for the workshop:

https://mccrary.auburn.edu/events/cie-practitioners-workshop/