The Human Factor in OT Cybersecurity: Culture, Engineering Practices, and Risk Ownership

Marco (Marc) Ayala, ISA Fellow
President, InfraGard Houston, National Sector Chief – Energy, ABS
Cyber CoE – Technical Director - Global

Agenda – Our Journey Today

- What it is: The human side of ICS/OT cybersecurity
- What we must identify: Culture, drift, and normalization of deviance
- What we must work toward: Practical, people-centered safeguards
- The future: Building environments where people protect the system

problem → identify → act → future

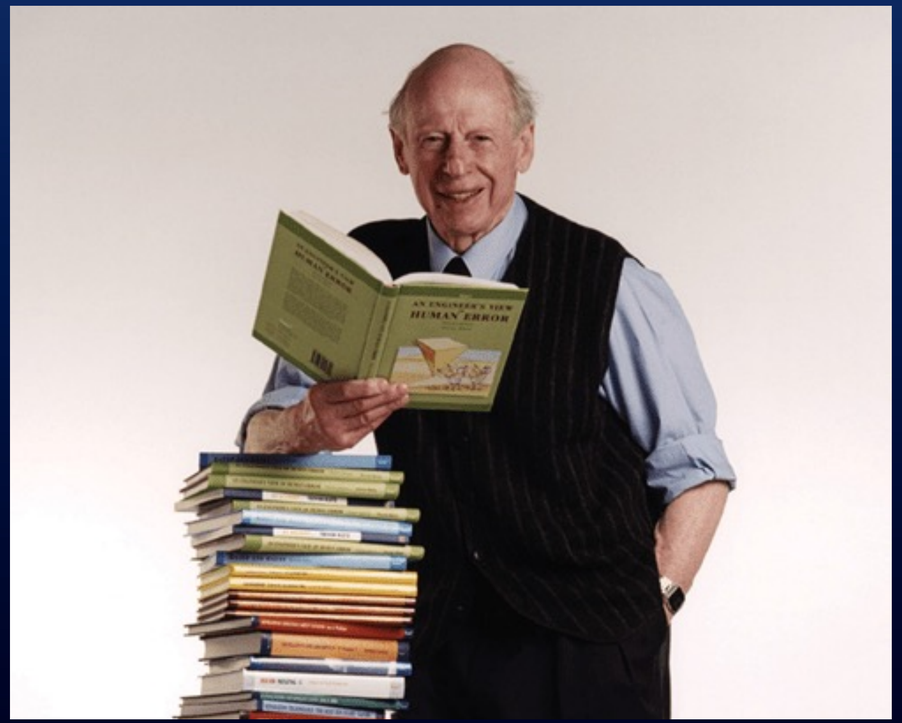
My Lens – Practitioner Perspective

- 30+ years in ICS/OT, safety systems, incident response, risk assessments across numerous sectors
- Seen firsthand how production pressure quietly reshapes “acceptable” risk
- Goal today: Turn insight into prevention

What It Is – Cybersecurity in Automation & Safety Systems Is a People Problem

- Technology (firewalls, patches, segmentation) is necessary but insufficient
- Everyday human factors — shortcuts, production pressure, “we’ve always done it this way” — drive risk
- Organizational culture silently shapes behavior

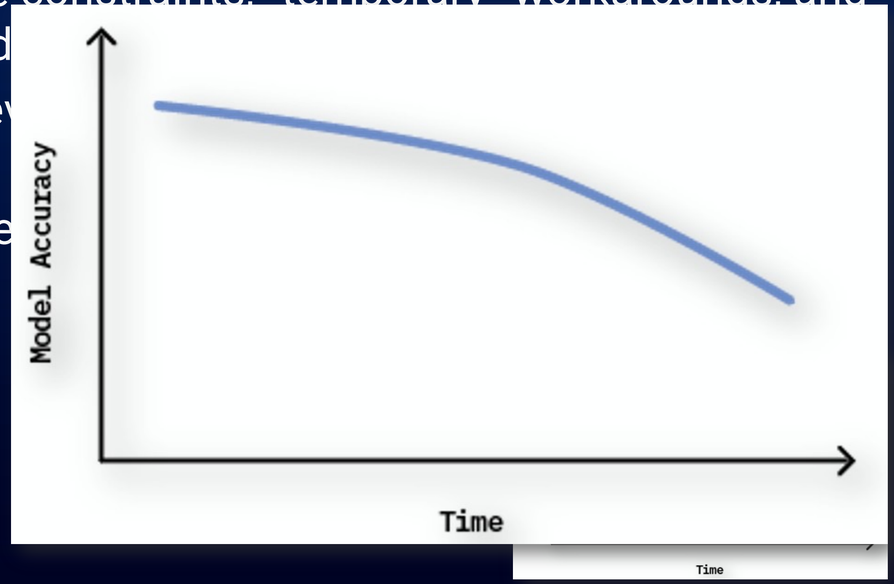
Culture Shapes Risk in ICS/OT



- Safety and cybersecurity cultures are **intertwined** in automation & safety systems
- Leadership signals, incentives, and day-to-day norms matter more than policies on paper
- Reference: Dr. Trevor Kletz – **“Accidents are not due to ‘human error’ alone; organizations design the conditions for them”**

Defining “Drift” – The Gradual Erosion of Defenses

- Definition: The slow, incremental movement away from established safe and secure practices over time, often without anyone noticing
- Caused by: production pressure, resource constraints, “temporary” workarounds, and the belief that “nothing bad has happened
- In automation & safety systems: small dev patching, or access controls accumulate
- Result: The system quietly becomes more



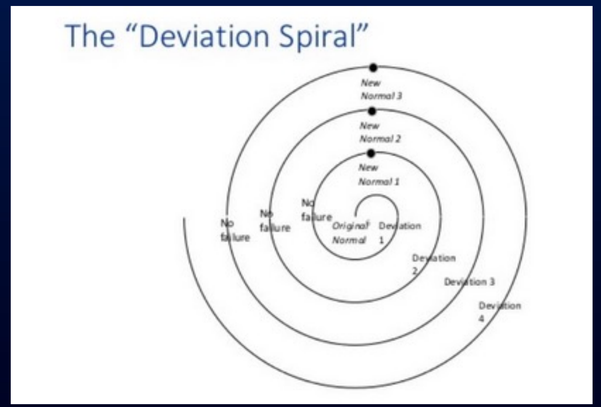
The Slow Erosion – Drift Happens

Everyday examples in ICS/OT:

- Bypassed interlocks that stay bypassed
- Controller keys in “Remote Program” and not “Run”
- Shared credentials or overly permissive remote access
- “Temporary” changes that become permanent
- Production pressure quietly overrides security and safety hygiene
- Risk becomes invisible to leadership and operators alike

Normalization of Deviance – The Core Mechanism

- Dr. Diane Vaughan’s concept (from her analysis of the Challenger disaster)
- How drift turns into the “new normal”
- Gradual acceptance that deviant practices are acceptable because “we’ve always done it this way” and no disaster has occurred yet



What We Need to Identify – Signs of Drift in Your Environment

- Increased workarounds or procedural deviations
- Tolerance of known vulnerabilities in safety systems
- Production-over-security decision patterns
- Weak behavioral signals from leadership

Real-World Lessons – Applying Vaughan, Kletz, and Clark

- Dr. Vaughan: Normalization in high-stakes technical cultures
- Dr. Kletz: Move beyond blaming individuals — redesign the system
- Dr. David Clark (Clark-Wilson integrity model): Formal controls for data integrity and separation of duties in commercial/industrial systems…

…he stated that the internet was never designed for critical infrastructure backhaul comms – ever!

Early Warning Systems That Actually Work

- Behavioral metrics + technical drift detection
- Regular “deviation audits” (not just compliance audits)
- Near-miss reporting without blame (BBS, BBCy)
- Anomaly detection in both cyber and operational data

What We Need to Work Toward – Stronger Behavioral Signals

- Leadership that visibly prioritizes security as safety
- Incentives aligned with long-term resilience, not just uptime
- “Just culture” that encourages reporting of drift

Practical Actions – Awareness & Training

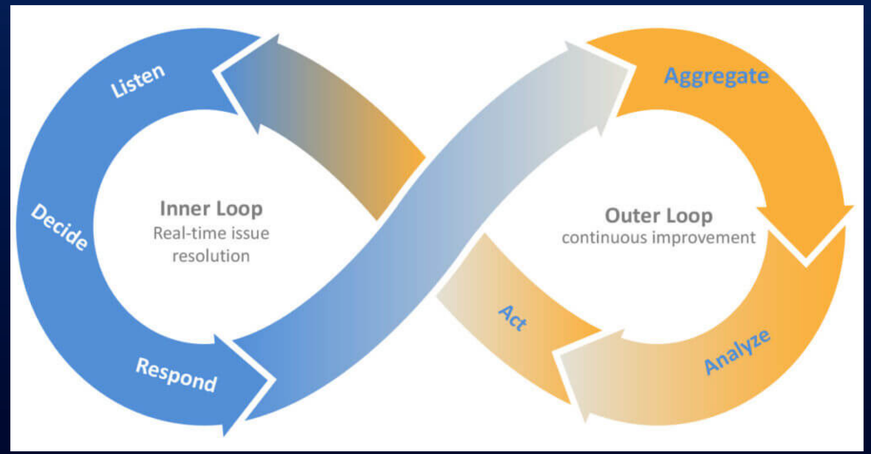
- Move beyond “click here” training to scenario-based, OT-specific simulations
- Incorporate human factors and normalization awareness
- Make security part of operational excellence, not a separate silo

Inherent Safety Applied to Cybersecurity (Kletz's Wisdom)

- Design systems so the secure path is the easiest path
- Minimize attack surface by default (segmentation, least privilege)
- Secure By Deployment strategies is a MUST
- "What you don't expose can't be exploited"

Building Early Warning & Response Capabilities

- Cross-functional drift review teams
- Metrics that track both technical compliance and cultural health
- Continuous learning loops from near-misses



The Future – People as Part of the Protection

- Mature safety cultures extended to cybersecurity
- AI-assisted drift detection that augments human judgment
- Resilient organizations that treat normalization as the enemy, not the operator

Key Takeaways

- Cybersecurity in automation & safety systems is fundamentally a human and cultural challenge
- Identify normalization of deviance early (Vaughan)
- Design inherently safer systems (Kletz) and apply integrity models (Clark)
- Leadership, training, and early warning systems turn people into the strongest layer of defense

Thank You + Call to Action

- **Start one “drift audit” in the next 30 days**
- **Foster open conversation about normalization in your teams**
- Questions?

Marco (Marc) Ayala
@ICS_SCADA

ABS Consulting
An ABS Group Company

Marco Ayala, ABS Center of Excellence
National Sector Chief – Energy
AMSC Outer Continental Shelf GOM/GOA
Marco.ayala@infragardhouston.org