

Securing Legacy Safety Instrumented Systems (SIS) Without Disruption

Marco (Marc) Ayala, ISA Fellow

President, InfraGard Houston, National Sector Chief – Energy,
ABS Cyber CoE, Technical Director Global

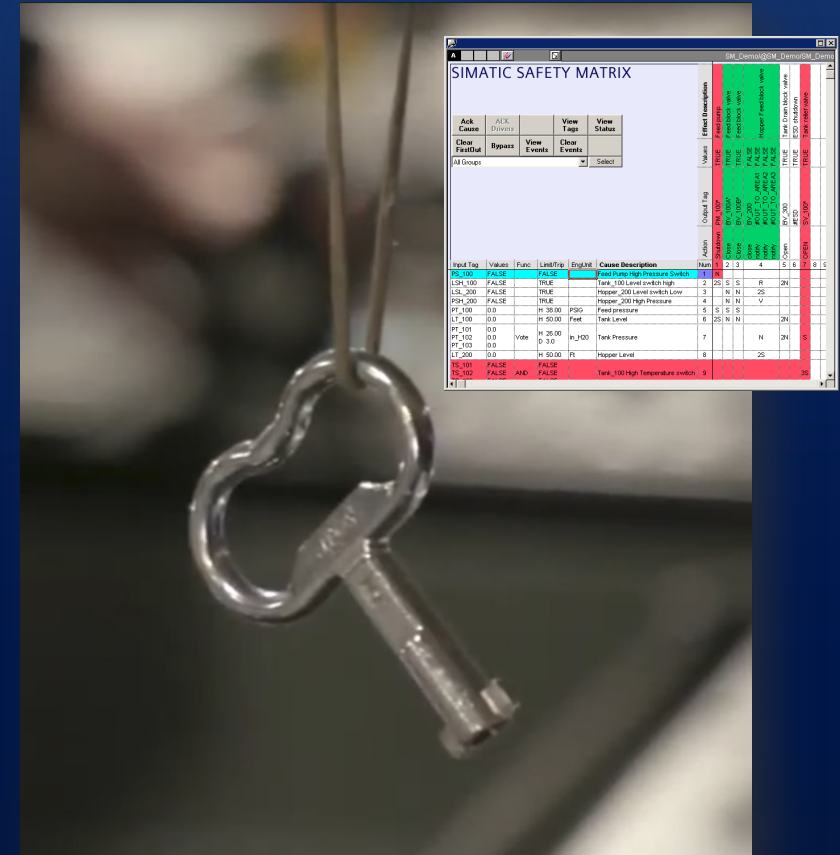
Agenda

- The Reality of Legacy SIS in Today's Operations
Legacy SIS reality and the risks from digitalisation
- Practical compensating controls that actually work
- Standards alignment and building a fortified perimeter
- Monitoring, change management and key takeaways



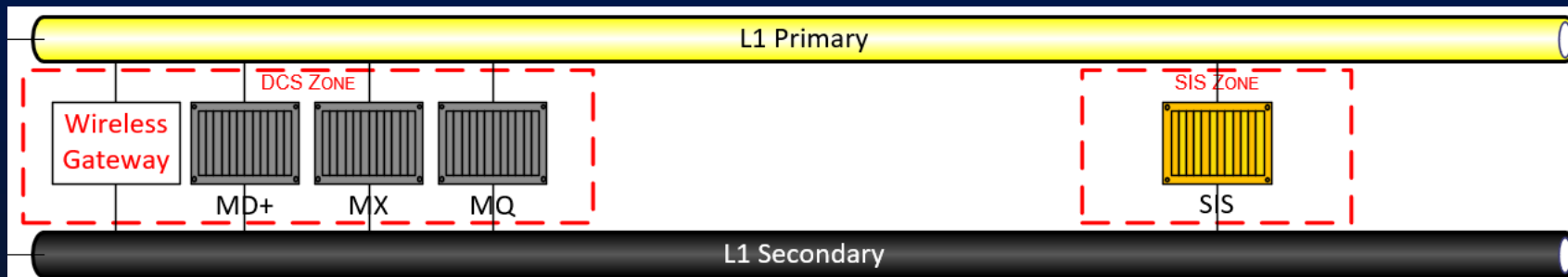
The Legacy SIS Challenge

- These systems were built to run for decades — patching or upgrading risks safety certification and operations
- Any change can threaten the certified protection layers
- Full rip-and-replace is usually too expensive or disruptive right now
- We're left protecting high-consequence assets that were never designed for today's threats



Digitalisation Brings New Risks

- Connectivity initiatives across Singapore and the region are opening new pathways
- These pathways didn't exist when the systems were commissioned
- Cloud integration and remote access significantly increase the attack surface
- Legacy SIS now face sophisticated cyber threats on top of their original design



What Actually Works – Lessons from the Field with Hands-On Experience

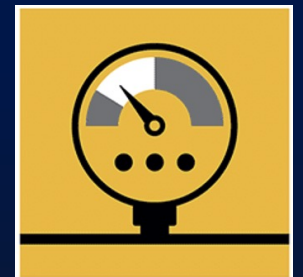
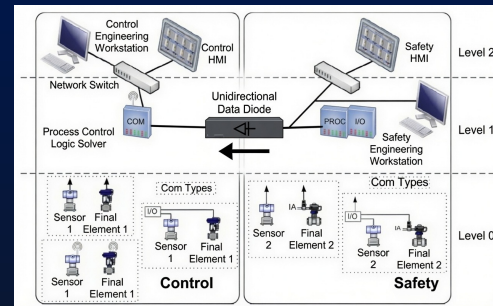
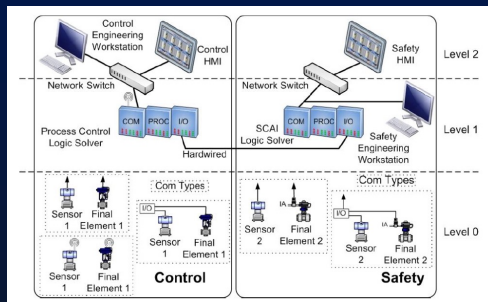
- Protecting live, high-consequence SIS without ever touching the certified core (bottoms up approach)
- Focus stays on maintaining safety integrity while dealing with real threats
- Traditional air-gapping and segmentation have clear limits once you need data flowing
- Practical compensating controls that fit how plants actually run deliver the best results



Realistic Compensating Controls *Without Disruption*

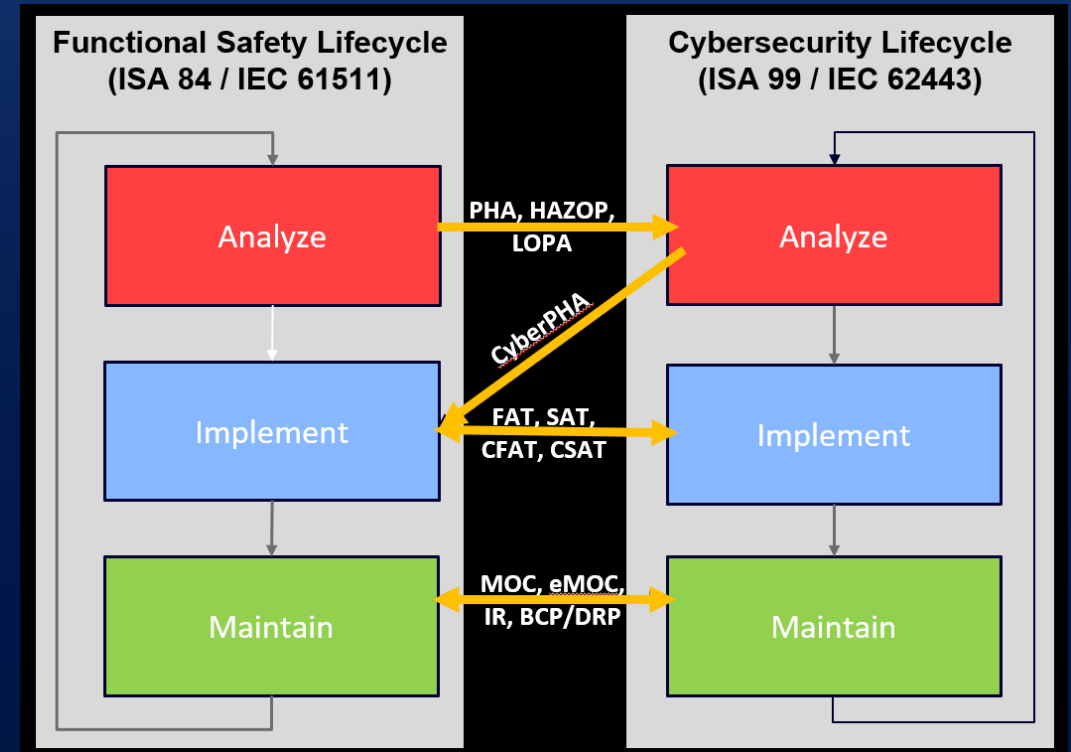
- Keep everything outside the SIS core so safety integrity levels stay intact
- Lower level isolated (non-switched) communications to the BPCS
- Unidirectional gateways and smart monitoring give good protection in real deployments
- Choose solutions that don't add new failure modes to safety functions

These let operations continue while cutting cyber risk significantly



Standards Alignment – IEC 61511 & ISA/IEC 62443

- IEC 61511 already expects us to consider cyber risks to safety functions
- ISA/IEC 62443 gives the practical toolkit – zones, conduits and security levels
- Mapping the two lets us align risk assessments and show clear compliance
- Together they support both safety integrity and cyber protection without conflict



Fortifying the Perimeter Around the Core

- Treat the SIS as a protected zone with very strict boundaries
- Lower-level comms, or data diodes enforce one-way flow out of the core
- Build monitoring and data extraction layers in a controlled DMZ around it
- This approach lowers the chance of a successful attack while still allowing business data



Monitoring and Safe Change Management

- Passive monitoring gives visibility without putting anything directly on the SIS
- Tailored anomaly detection on legacy protocols spots problems early
- Every change goes through formal Management of Change with both safety and cyber teams
- Testing and phased rollout keep everything stable and certified



Remote Access Policy – Full Stop

- Remote access to the SIS/SCS is strictly prohibited under all circumstances
- The SIS/SCS must remain fully isolated from any external or remote connectivity
- Safe alternative: Use a Safety Matrix on the BPCS populated exclusively from read-only registers in the SIS
- This approach maintains both safety integrity and cybersecurity without compromising the certified protection layers



Key Takeaways

- Legacy SIS can be protected effectively without disruption or replacement
- Use compensating controls + fortified architecture + proper standards alignment
- The goal is lowering cyber likelihood while keeping safety integrity 100% intact
- These practical steps support digitalisation goals without compromising safety



Questions & Discussion

Thank you.

Happy to take questions on any of this — especially how it applies to your own legacy SIS environments.





Marco (Marc) Ayala ✓

@ICS_SCADA



Marco Ayala, ABS Center of Excellence
National Sector Chief – Energy
AMSC Outer Continental Shelf GOM/GOA
MarAyala@absconsulting.com



THANK YOU