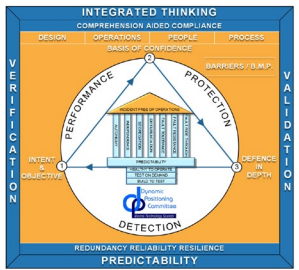
Dynamic Positioning Committee

Marine Technology Society

Addressing Cyber Security and Cyber Threat Resilience by Design

Christian Wiedemer, Jason Aspin and Ed Bourgeau

Aspin Kemp & Associates



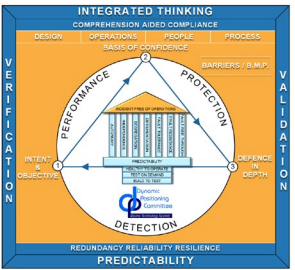
ASPIN KEMP & ASSOCIATES

marine technology SOCIETY

Opportunity runs deep™

Contents:

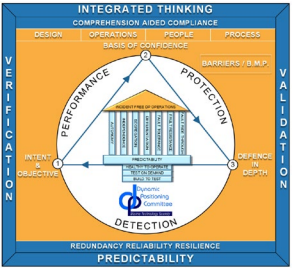
1. Understanding the objectives
2. Leveraging a learner mindset
3. Defining the boundary conditions
4. Using a ‘Minimalist’ approach to design
5. Ways to achieve resilient systems
6. Validation by testing (A build-to-test mindset)
7. Conclusion



1. Understanding the objectives

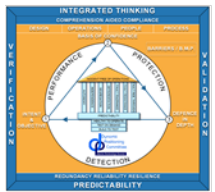
Clear definition of mission objective:

- Why are we interfacing with Process Control and automation devices?
- What do we wish to do with the information we receive?
- We will not write data into the industrial process (intentionally or inadvertently).
- Mission objectives will not impose a burden on the Process Control and Automation Devices or impact its intended performance.
- Scope Creep will not be permitted.



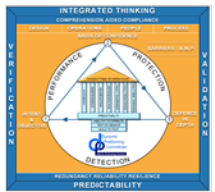
2. Leveraging a Learner Mindset

- Humility to reach out to the domain experts.
- Spend the time to understand and align on the vocabulary. (Two-way communications)
- Understand and address the concerns of the diverse stakeholders.
  - Do not be dismissive of any concern!
  - Treat every concern as significant and close out with effective verification and validation
  - Address by design and not rely on risk assessing your way out of the concern!



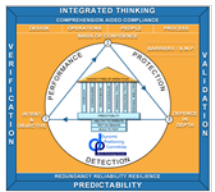
3. Defining the Boundary Conditions

- Interfacing equipment should not impose any additional burden on the process control and automation devices which could impact its performance.
  - Broadcasting vs polling
  - Interrupts
- Principles of autonomy and not defeating the redundancy concept to be adhered to. Validation by testing is a requirement.
- Failure or erroneous behavior of the interfacing equipment should have no impact on the equipment it is interfacing with.
- Understanding, identifying and ensuring that the DMZ is not compromised.
- Threat Vector under consideration is the connectivity to the www. Interfacing equipment is not to provide an exploitable tunneling opportunity.



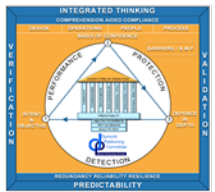
4. Using a Minimalist Approach

- Multi use functionality of interfacing equipment is a bane. Only needed functionality should be made available.
- Minimize the number of interfaces and dependencies. Elegance in simplicity facilitates effective verification and validation.
  - Validation burden reduced.
  - Transparency (at appropriate level)(hardware and software).
  - Not reliant upon ‘security by obscurity’ or proclamations of ’proprietary’.
- Defend against scope creep and enforce robust ‘Management of Change (be prepared to challenge respectfully).



5. Ways to Achieve a Resilient System

- ‘Data Diodes’ and data diode functionality.
  - Interfacing equipment.
  - Equipment which is interfaced with.
- Eliminating unused functionality and protocols not essential for mission objectives.
- Adhere to ‘Seven Pillars’ principle and MTS DP Committee Iconography for Predictability.



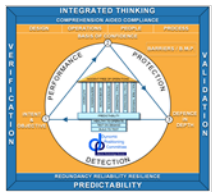
6. Validation by testing

- Demonstrate efficacy of measures by planning and conducting a comprehensive penetration test . A replicant interfacing system must be made available for testing purposes.
- Test scenarios to incorporate output (concerns) of HEMP exercises.
- Test scenarios should include verification of resilience of interfaced equipment even with full administrative access to interfacing equipment.

7. Conclusions

IMPERATIVES

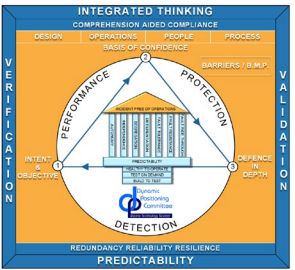
- A Learner Mindset.
- Equipment interfacing with process control and automation devices demonstrate resilience to cyber threats.
- Recognizing vulnerabilities of readily available multi function devices.
- Divergence from the ‘minimalist’ approach increases the vulnerability and burden of verification and validation.
- Addressing by design is far more effective than attempting to ‘risk assess’ your way out of it.
- Adherence to “Seven Pillars’ and MTS DPC Iconography is an enabler to addressing Cyber Security threats by Design.



marine technology SOCIETY
Opportunity runs deep™

ASPIN KEMP & ASSOCIATES™

Thank You & Questions



Dynamic Positioning Committee
Marine Technology Society