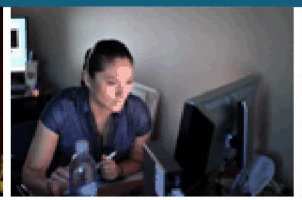
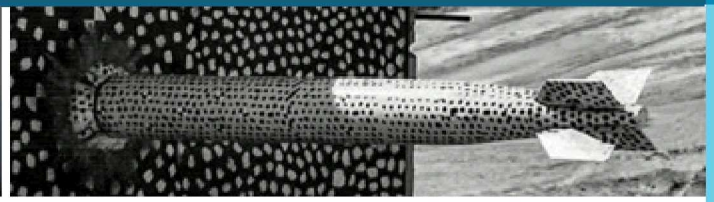
SAND2020-7294C

Analysis of National and International Standards to Identify Priority Control Methods





Michael T Rowland; Jacob James

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Sandia National Laborat
laboratory managed anc
Technology & Engineeri
LLC, a wholly owned su
International Inc., for th
Energy's National
Administration under co

Objective

- Current cyber security approaches are dominated by protection of an asset through application of recommended cyber security controls
- International and National Standards provide:
  - Risk management approaches
  - Control measure catalogues
- Number of controls and number of assets are too large to enable efficient deployment and management
- Are there a small number of common controls that should be prioritized that address the majority of the risk?
  - The objective was not achieved due to the high degree of uniformity among cyber security controls catalogues

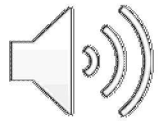
Methodology

1. Review of the Standards
2. Mapping of similar control methods
3. Identification of priority controls
4. Evaluation of priority controls using case studies

Result: International and National Standards are highly correlated and this results in very few substantive differences in the recommended control sets.

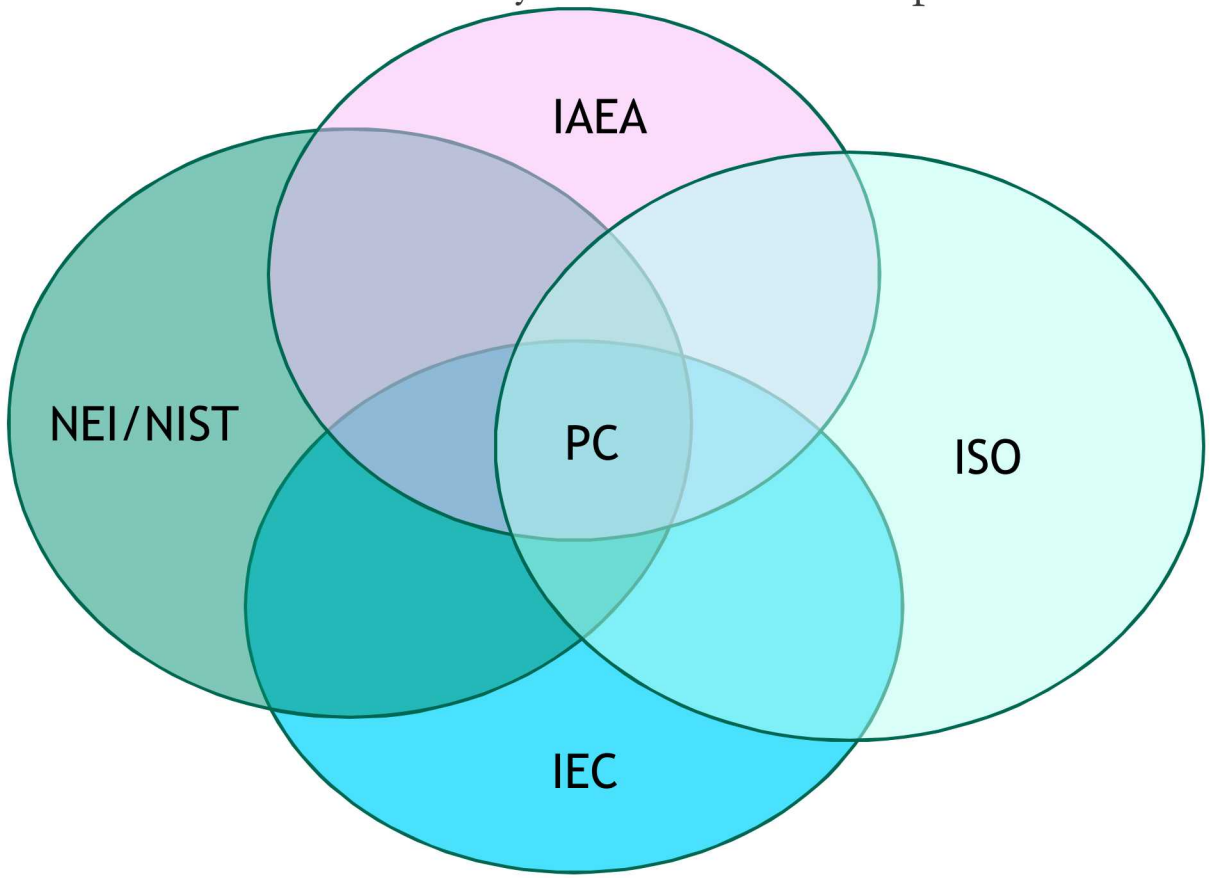
Standards Reviewed

1. IAEA Publications
   - IAEA NSS 17 – Computer Security at Nuclear Facilities
   - IAEA NSS 33-T – Computer Security of I&C at Nuclear Facilities
   - IAEA NSS 23-G – Security of Nuclear Information
   - IAEA NST047 – Computer Security Techniques at Nuclear Facilities (Draft publication, NSS 17-T Revision)
2. Nuclear Specific Standards
   - IEC 62645 – Nuclear power plants – I&C systems – Requirements for security programmes for computer-based systems
   - IEC 63096 – Nuclear Power Plants – I&C and Electrical Power Systems – Security Controls (FDIS 2020 version)
   - NEI 08-09 Rev 6 – Cyber Security Plan for Nuclear Power Reactors
   - NEI 13-10 Rev 5 – Cyber Security Control Assessments
   - CSA N290.7-21 – Cyber Security for Nuclear Facilities (Draft June 2020 version)
3. OT Cyber Standards
   - IEC 62443-2-1 Ed 2 - Security for industrial automation and control systems – Part 2-1: Security program requirements for IACS asset owners (CDV 2019 draft)
   - IEC 62443-2-2 Ed 1 - Security for industrial automation and control systems – Part 2-2: IACS Security Program Ratings (CD 2020 draft)
   - IEC 62443-3-3:2013 – Industrial Communication networks – Network and system security – Part 3-3: System security requirements and security levels
4. ISMS Standards
   - ISO 27002:2013 - Information technology — Security techniques — Code of practice for information security controls
   - US NIST sp800-53 Rev 4 - Security and Privacy Controls for Federal Information Systems and Organizations
5. Industry Good Practices/References
   - CIS Controls v.7.1 (formerly SANS Top 20)
   - US CISA CRR NIST Cybersecurity Framework Crosswalks April 2020
   - US CISA Cybersecurity Framework Implementation Guidance



Mapping of Similar Control Methods

- **Hypothesis:** The union of control methods from multiple standards (IAEA, ISO, IEC, NEI/NIST) associated with independent communities will provide for those controls that are highly valued by all.
- This aim was to determine if this would identify a small subset of prioritized controls (PC).



Discovery

Discovery: Insufficient independence of standards groups resulted in a large subset of individual controls (see CRR Crosswalk – April 2020)

- IAEA publications provide basis for IEC Nuclear Standards
- ISO Standards (27001) are used to reconcile clauses in IEC 62443
- ISO 27002 was basis for IEC Nuclear Standard 63096
- This interdependency led to a high degree of correlation which did **not** provide a **small number** of prioritized controls (i.e. common to all catalogues)
- The union of standards resulted in near total overlap of recommended controls.

Figure Ref: A. Duchac (IAEA) – IEC SC45A Presentation – Las Vegas, 2015

US CISA CRR NIST Cybersecurity Framework Crosswalks April 2020

Function	Category	Subcategory	CRR References*	Informative References
Identify (ID)	**Asset Management (AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. **CRR References**** AM:G2.Q1 – PIF AM:G2.Q3 – PIF AM:G2.Q4 – PIF AM:G4.Q1 – PITF AM:G4.Q2 – PITF AM:MIL2.Q1 AM:MIL2.Q4	**ID.AM-1:** Physical devices and systems within the organization are inventoried***	AM:G2.Q1 – T AM:G2.Q3 – T AM:G2.Q4 – T	• CIS CSC 1 • COBIT 5 BAI09.01, BAI09.02 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	AM:G2.Q1 – T AM:G2.Q3 – T AM:G2.Q4 – T	• CIS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2, A.12.5.1 • NIST SP 800-53 Rev. 4 CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	AM:G2.Q5	• CIS CSC 12 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1, A.13.2.2 • NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	AM:G2.Q1 – T	• CIS CSC 12 • COBIT 5 APO02.02, APO10.04, DSS01.02 • ISO/IEC 27001:2013 A.11.2.6 • NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	AM:G1.Q2 AM:G7.Q1 AM:G7.Q2	• CIS CSC 13, 14 • COBIT 5 APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 • ISA 62443-2-1:2009 4.2.3.6 • ISO/IEC 27001:2013 A.8.2.1 • NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	AM:MIL2.Q3 CM:MIL2.Q3 CCM:MIL2.Q3 VM:MIL2.Q3 IM:MIL2.Q3 SCM:MIL2.Q3 RM:MIL2.Q3 EDM:MIL2.Q3 TA:MIL2.Q3 SA:MIL2.Q3	• CIS CSC 17, 19 • COBIT 5 APO01.02, APO07.06, APO13.01, DSS06.03 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1 • NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

https://us-cert.cisa.gov/sites/default/files/c3vp/csc-crr-nist-framework-crosswalk.pdf

Other significant observations - Standards

- Nuclear Standards (NEI 08-09 Rev 6, IEC 63096) are conservative in their application of a graded approach, requiring an overwhelming majority to be applied to all SSEP digital assets (regardless of risk)
- NEI 13-10 and CSA N290.7-20 aim to improve grading of requirements and imposition of controls.
- Equivalence in Nuclear between air-gap and deterministic secure isolation device (e.g. data diode) and heavy use of administrative controls (policy, procedures) is problematic when evaluating other standards and good practices.
- IEC 62443-3-3 has a good grading of control requirements based on risk (correlated with Security Levels – SL)

Security Level	# of Security Requirements
SL1	37
SL2	60
SL3	90
SL4	100

Challenges with using control catalogues

Sufficiency
(objective, what needs to be achieved)

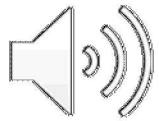
- Is the appropriate level of protection provided?
- Risk is correlated to level of threat
  - Example – IEC 62443 SLs are graded according to the capability, motivation, and resources of adversary.
- Risk is correlated to safety classification but not directly one-to-one
  - Effects of cyber-attacks on critical systems can not be completely known.
- Risk informing the level of effort (and by relation the number of measures) that will be sufficient/necessary must address a high degree of uncertainty.
- The correct outcome is ambiguous.

What is a sufficient level of detail for inventory of hardware and software?

Efficiency
(how, the manner in the objective is achieved)

- Is the required protection provided with minimal wasted or redundant effort?
- Control efficacy given a certain threat is generally qualitatively assessed
  - Example – boundary control effectiveness in ensuring all traffic is authorized.
- Difficult for controls to remain durable (lasting) against ever changing adversary TTP
- While correlated to testing, evaluation, and scenario based analysis, uncertainty in both efficacy and durability of the control is significant
- The correct level of efficiency is ambiguous

How to perform these inventories and document the results in the most efficient manner?



Conclusion

- Global standards organizations do not have the required level of independence to differentiate their control catalogues to allow for a substantially reduced priority control list
- Nuclear Standards would benefit from evaluating how to increase adoption of a graded approach similar to IEC 62443-3-3.
- Due to the uncertainty with the evaluation of future characteristics of an 'intelligent adversary[1]', cyber-security risk management and therefore selection and prioritization of controls typically has a low degree of certainty or determinism.
- Further research on development of empirical/quantitative data sets to remove ambiguity and increase certainty is necessary to improve sufficiency and efficiency of cyber security outcomes.

Ref: UK ONR describes 'intelligent adversary' in paragraph 8 of http://www.onr.org.uk/documents/2017/risk-informed-regulatory-decision-making.pdf

Thank you