Polytechnic School of the University of Sao Paulo
Navy Technological Center in Sao Paulo

Physical, Corporate and Industrial Digital Security Convergence: Gaps to Close

Rodney Busquim e Silva
José Roberto Castilho Piqueira
Ricardo Paulino Marques
André Luis Ferreira Marques

International Conference on Physical Protection of Nuclear Material and Nuclear Facilities

IAEA, Vienna International Center, 13-17 November 2017

CLOSING THE GAPS

- Digital Systems are extensively used in NPP and FCF as part of PPS, IT and OT.
- Digital setups perform different functions according to their domain.

- Significant roles in acquisition, transmission, analysis, delivery and storage of essential data.
- There is a recent organization consensus that cyber security extends beyond IT.

- All cyber security regulations and implementations must follow similar trends as physical and digital security are tied together.

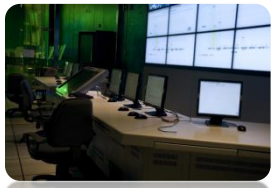
Computer Security for

PPS

- HW & SW convergence: TCP/IP
- Many digital PPS auxiliary systems (sensors, cameras, access control devices etc)
- Protection of nuclear materials and facilities
- Protection of sensitive information

IT

- Standard term for computer-oriented systems
- IT systems are typically based on open query and response
- Updates are not usually an issue
- Cyber security is well understood
- Many tools for TCP/IP protocols



OT

- SW & HW for automation and control
- Directly related to industrial production
- Cyber-physical: connected to the real world
- Designed to execute a specific task or process
- ICS systems have longer lifecycle
- Many protocols (not only TCP/IP)

Convergence: integration of elements under a unified governance with a more formal cooperation among logical, information, personnel, business, engineering and operational security.

Due to historical facts, an organization may have a harmonized governance throughout all the IT systems.

IT processes and platforms: responsibility of the CSO with a team of software, hardware and networking specialists.

OT processes: responsibility of the production managers with a team of engineering working towards business outcomes. Due to manager's tasks/objectives, the OT cyber strategy may differ from one unit to other.

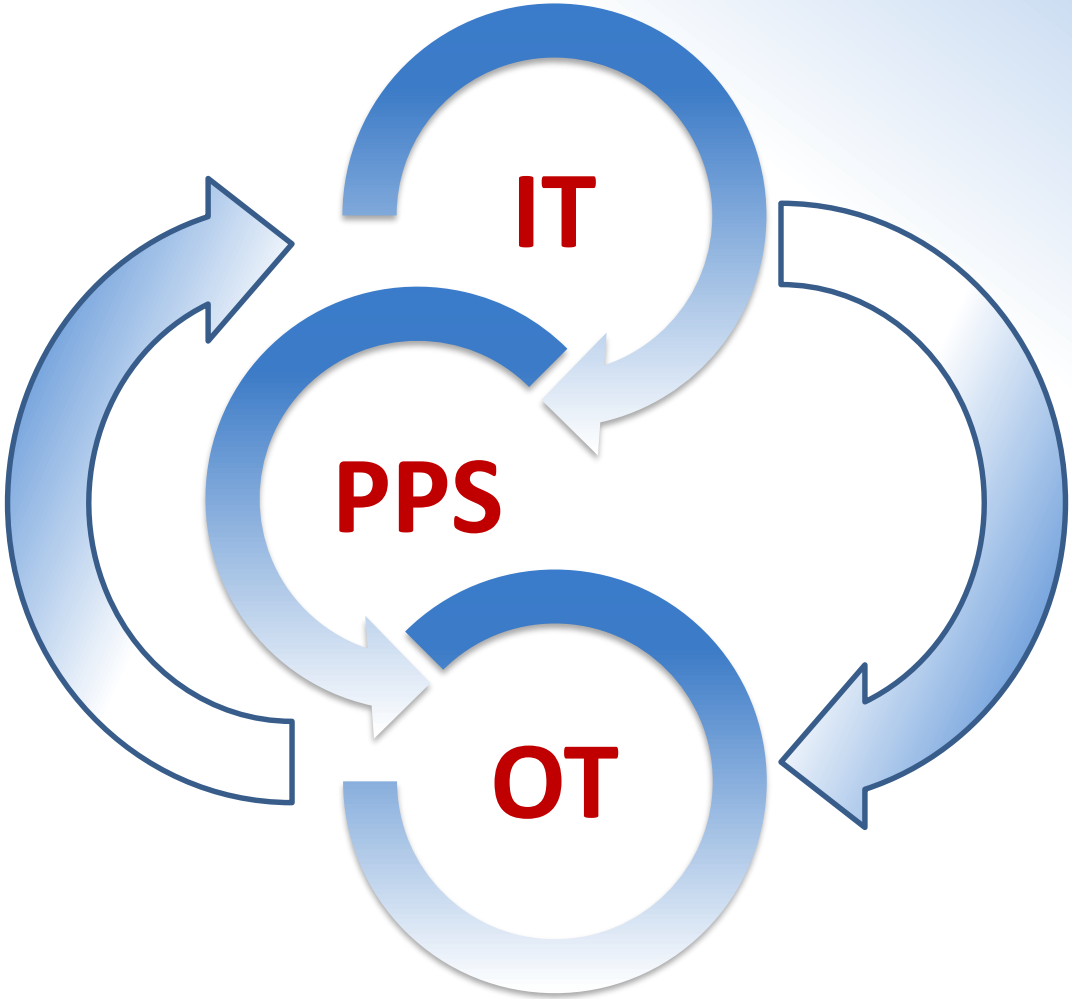
Computer based systems used for PPS , nuclear safety, and nuclear material accountancy and control should be protected against compromise and consistent with the physical protection threat assessment or design basis threat.

Cyber attacks may compromise all three domains: physical, corporate and ICS security. The interactions and interdependencies among these areas can not be ignored.

Crossover technologies – for example: PPS will not configure firewalls or give up control of the card reader system, IT may not be interested in guards & guns, OT may not be interested in cryptography and cameras.

PPS, IT & OT Cyber Security Management Occur

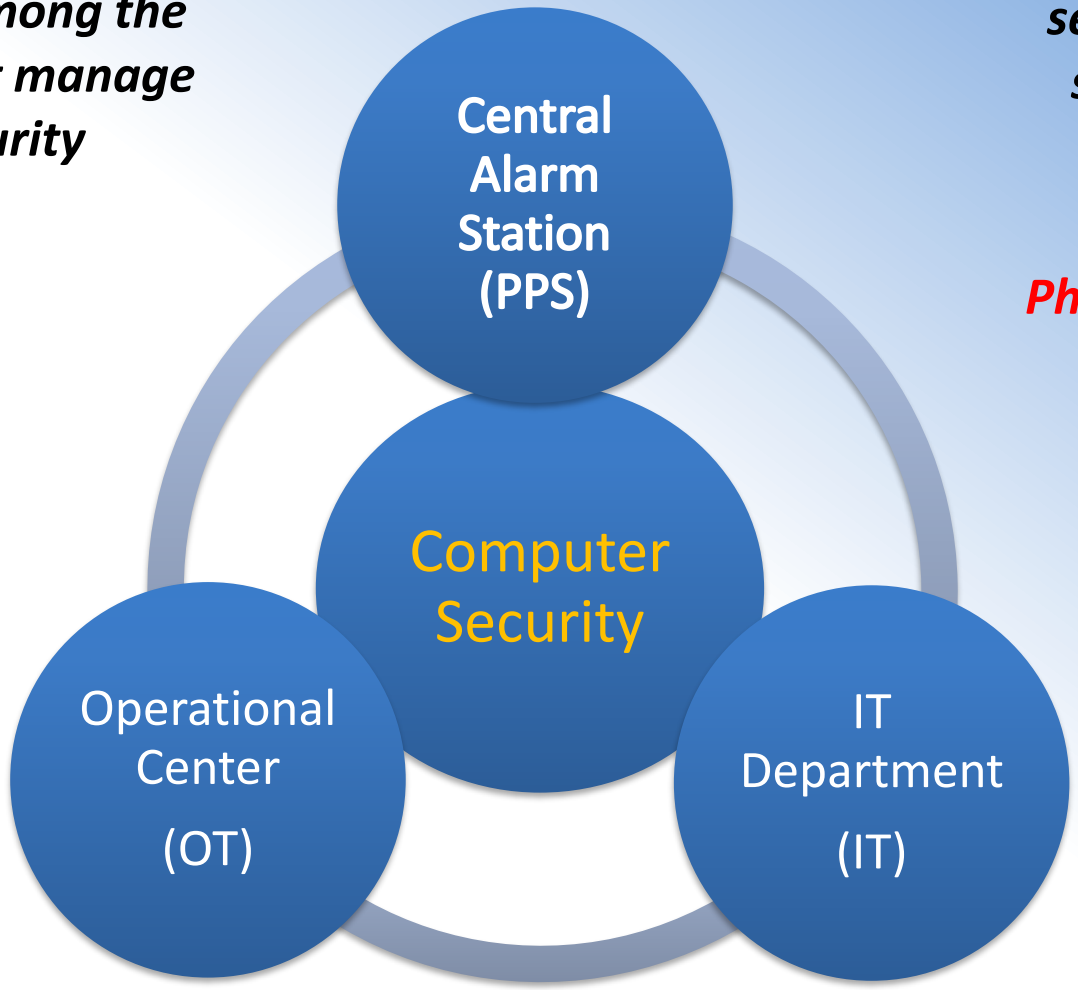
In many organizations, the operational, physical protection and corporate networks are not physically and logically integrated - yet?



- **at a central alarm station (CAS) for access and surveillance control.**
- **at an IT department (or similar) for corporate networks.**
- **and at operational level for industrial instrumentation and control.**

Separation or lack of integration among the 3 spheres that manage computer security

Could lead to critical security gaps: physical security and/or cyber attacks



Physical security attacks may compromise computer security

Cyber attacks may compromise physical, corporate and ICS security

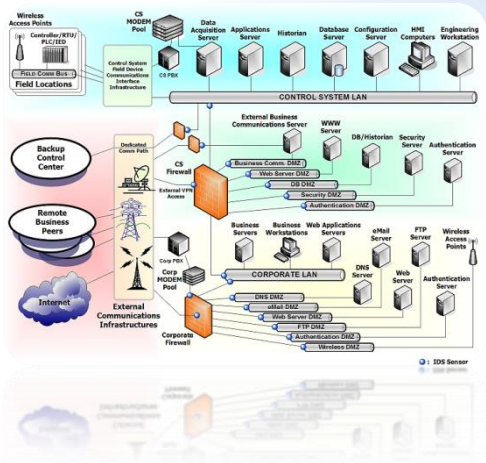
Computer Security Spheres

Systems engineering is an integrated and systematic multidisciplinary approach to: *i*) identify systems objectives and requirements; *ii*) perform system design; *iii*) evaluate system throughout design analysis considering (*i*)

Unified Governance Driven Factors

- Enterprise assets are highly IT/OT information-based dependent
- Loss of OT/IT network is a “revenue-impacting event”
- Digital PPS systems are IT technology dependent
- PPS and OT protect and deal with critical infrastructure
- PPS and IT systems protect critical data
- All spheres are very result-oriented regarding security
- Networking technology is converging to IoT (everything connected)

At technical level, the binary data, as transmitted throughout the PPS and also through the OT and IT networks, are the same.



GAPS TO CLOSE

Disconnection between managers and ICS/PPS/OT personal

Distinct ICS/PPS/OT teams background

OT/PPS not knowledgeable in digital security issues as IT

Learning curve is too steep for a single person

Understanding of the consequences of an attack by the OT & PPS/IT teams very different

Overlapping functional roles

Lack of integrated policies

Accountability gap due to legacy OT technology

Cybersecurity training and awareness courses focusing on OT and PPS, not only IT

CLOSING THE GAPS: UNIFIED GOVERNANCE

- Reduced operating costs through elimination of redundant processes
- Reduced costs due to better use of resources
- Increased control over distributed operations
- Improved security through an integrated approach for IT/PPS/OT cybersecurity
- Consistent risk management considering IT/PPS/OT cyber security technologies
- Improved management of all systems.
- Improved overall plant safety regarding digital systems.
- Adoption of an unified cyber security strategy.

Benefits

Life Cycle Conciliation

Management

Team Qualification

IT/PPS/OT Requirements

Barriers

CLOSING THE GAPS: REMARKS

- Securing IT data is as important as securing facility and OT/ICS.

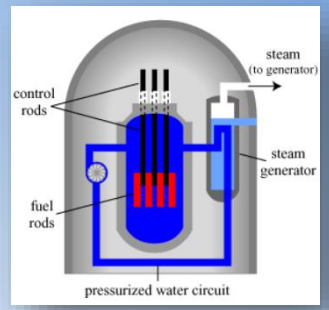
- Shorten the distance between managers and PPS, IT and ICS people: integrated polices.

- A single governance will increase connections among business planning, compliance, security, and prevention.

- It will allow, for instance, a more comprehensive security strategy having a single person, for example, the CSO, as a single point of contact for all cyber security issues.

CLOSING THE GAPS: REMARKS

- The acquisition/design of new equipment, and systems for OT/IT and PPS, should be under the same coordination, and the CSO team must participate in the selection process considering engineering aspects towards a threat-informed approach.



- These imply that the CSO team must have knowledge that includes engineering personnel that can work within the boundaries between digital systems and analogue, real world systems.

CLOSING THE GAPS: REMARKS

- The gap in knowledge and best practices between IT/OT/PPS staff and other employees can be narrowed by cyber security training courses and awareness.

- The gaps among corporate, physical and industrial digital security must be closed not as individual, separated domains, but as highly interconnected and interdependent entities.

The simple analysis of the architecture design and application of security measures may be replaced with an iterative engineering approach.

CONCLUSIONS

Cyber Security

- Facilities manage computer security in 3 spheres: IT department, operational center and CAS
- A single governance must guide physical, corporate and industrial cyber security
- Decision-makers must ensure securing IT data, OT/ICS and PPS are all equivalent
- Personnel involved in CS in each sphere have different background and understanding of threat
- Integrated skilled team must be in charge of procedures, policies and digital systems designs
- Clear and coordinated roles to avoid computer security accountability gaps.
- OT: proprietary technology running longer lifecycle, IT&PPS converging to TCP/IP

Thank you!

rodney@marinha.mil.br