Can a novel IT/OT SOC framework defend critical infrastructures against cyber threats?

Shane Sweeney, Supervisor - Paul Barry
MSc Cyber, Privacy & Trust

Introduction

Traditionally, IT was concerned with managing data and communications as the foundation of information flow while OT controlled physical devices and processes to ensure operational integrity in industrial settings.

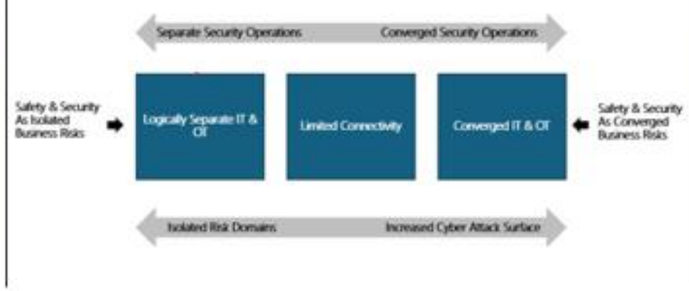
In the age of Industry 4.0, converging Information Technology (IT) and Operational Technology (OT) is no longer a trend, but a required strategic differentiator that drives improved organisational efficiency, innovation, and digital transformation, across critical infrastructure enterprises.

Managing the cyber risks associated with the convergence of these previously disparate domains is important for critical infrastructure organisations aiming to improve holistic resilience within the context of an ever-evolving cyber threat landscape and societal needs.

This research describes a novel framework that critical infrastructure organisations can leverage to mitigate the cyber risks associated with IT/OT convergence.

Literature Review, Case Study and Expert Interviews

Historically Separate IT & OT Domains



Evolution of IT-OT Convergence

Next Steps

Business View	CONTEXTUAL ARCHITECTURE
Architect's View	CONCEPTUAL ARCHITECTURE
Designer's View	LOGICAL ARCHITECTURE
Constructor's View	PHYSICAL ARCHITECTURE
Technician's View	COMPONENT ARCHITECTURE
Manager's View	MANAGEMENT ARCHITECTURE

Ref	Driver	Business Attributes
	Enterprise	
BD 1	Maintain regulatory compliance	Compliant
BD 2	Provide leadership in technology	Innovative, Technologically-Advanced
BD 3	Preferred customer service choice	Reliable, Cost-sensitive, Trusted
BD 4	Maintain Government confidence	Trusted
BD 5	Maintain financial efficiency	Cost-Effective

Architectural Methods to build Converged Cyber Capabilities

Theoretical SOC Framework

Research Questions

What cyber risks need to be considered when IT and OT business domains converge?

What architectural approaches can be used to design capabilities to mitigate these risks?

How can this approach be utilised to build a framework for converged IT & OT Cyber Security Operation Centres?

Can a novel IT/OT SOC framework defend critical infrastructures against cyber threats?

Research Methodology

A mixed-methods approach, including a literature review, case study analysis and subject matter expert interviews.

State of the Art

Cyber Technologies: AI and machine learning are driving predictive cyber threat analysis, helping keep pace with the evolving cyber threat landscape across IT and OT.

Risk Frameworks and Architecture Methods: Industry frameworks and standards such as AESCSF, ISA/IEC 62443 and SABSA are regulatory driven to ensure that cyber capapiltes align to business risk objectives

Ethics and Sustainability. Growing focus on designing security practices that will protect critical infrastructure while considering the long-term impacts on society and the environment.

Enhanced OT Cyber Threats: Increasing frequency and complexity of attacks on OT including the creation of specialised malware.

Early Indications

Strategic Imperative: IT/OT convergence is strategically driving operational efficiencies, innovation, and digital transformation across critical infrastructure providers.

Cyber Risks Evolving: IT and OT convergence introduces new cyber threats, so holistic detection capabilities across those domains are necessary to protect critical infrastructure assets.

SOCs Role: Security Operations Centers (SOCs) are crucial, acting as the cybersecurity hub for continuous threat monitoring and incident response.

Framework Gap: Existing standards lack a cohesive, business risk driven architectural framework for the development of IT/OT security capabilities.

References:

Garimella, P. K., 2018. *IT-OT Integration Challenges in Utilities.* Nepal https://ieeexplore.ieee.org/document/8586807, s.n., pp. pp. 199-204.

Katsikas, A. A. a. S., 2022. Unified IT&OT Modeling for Cybersecurity Analysis of Cyber-Physical Systems. *IEEE Open Journal of the Industrial Electronics Society,* pp. 318-328

NIST, 2023 . *Guide to Operational Technology - OT Security - National Institute of Standards and Technology.* [Online]
Available at: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf