Industrial Cybersecurity for the CISO – Part 3

Approach to Industrial Cybersecurity

Micro Learning Module

MLM-050-C

Industry	–	Process
Principal Role	–	Owner / Operator
Professional Role	–	CISO
Enterprise Phase	–	Master Planning

Author

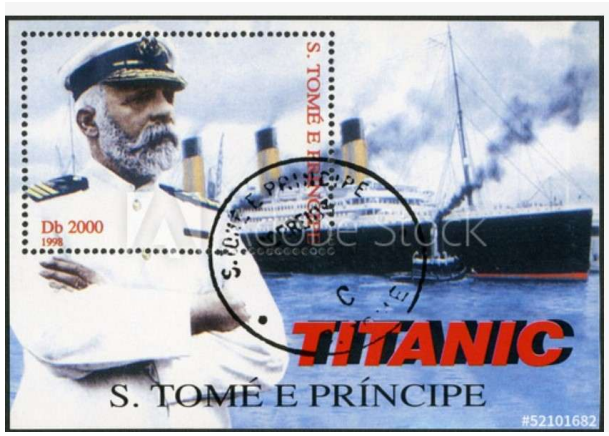
Vytautas Butrimas

Author's presented views are his own

Turn on your audio and click start to begin video

START

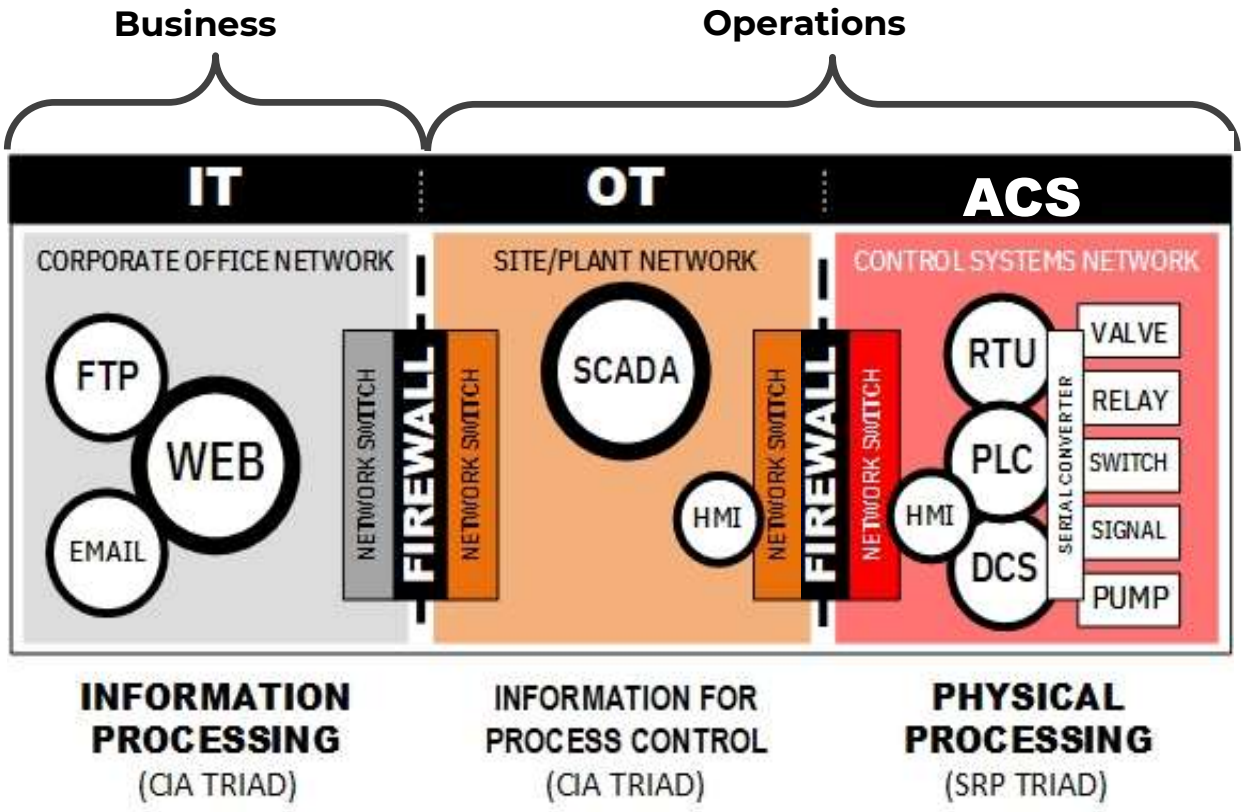
Being Aware of OT/ACS Security Challenges



Cpt. Edward Smith H.M.S. Titanic

Used with permission
http://cyberg.us/

IT, OT and ACS role in operations of critical infrastructure



Graphic used with permission of Bob Radvanovksy
http://icsmodel.infracritical.com/

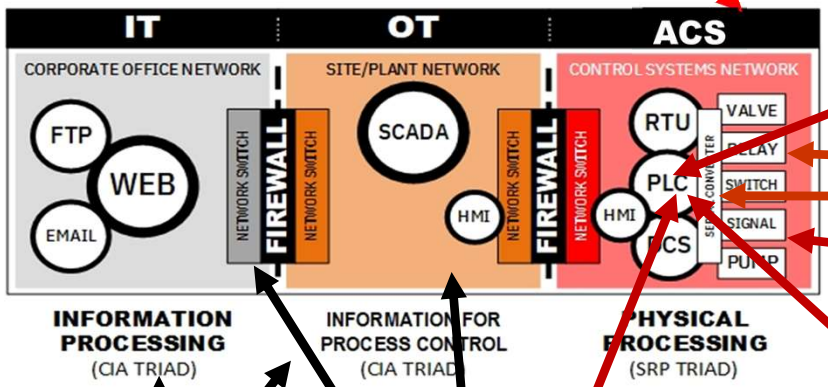
The Physical Process (ACS) is also a target

Saudi Aramco “wiper” 2012

Colonial pipeline “disruptionware” 2021

Falcon (EDR sensors) 2024

Steel Mill 2014/2022



Water 2023

Ukraine 2016

Ukraine 2015

Viasat/Enercon 2022

Stuxnet 2010

Triton SIS 2017
Saudi Arabia

Norsk Hydro 2019

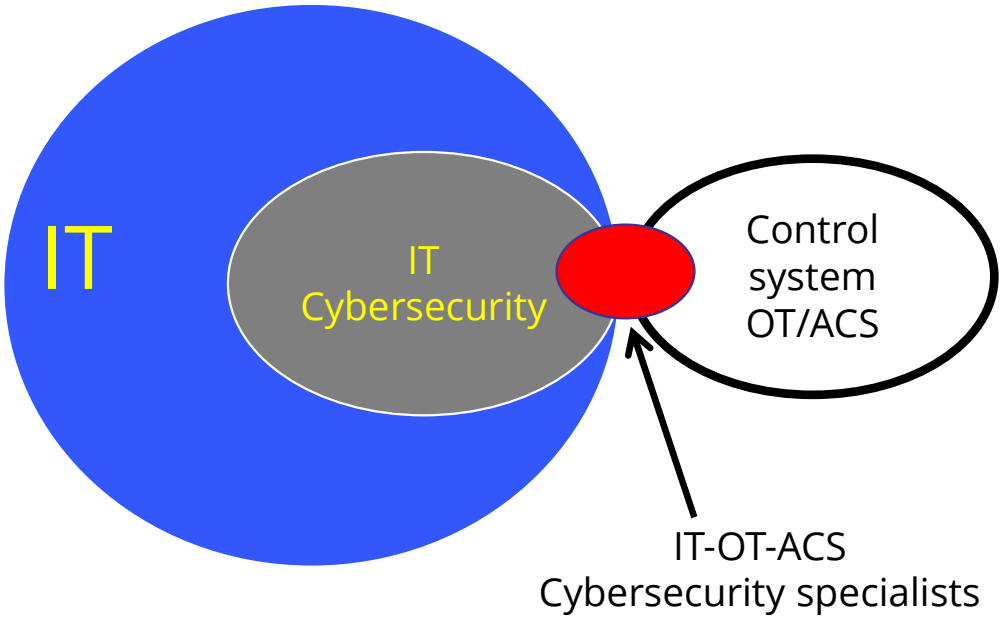
TSMC 2018

Typhoon (Volt, Salt, Flax) 2022-today

Graphic used with permission of Bob Radvanovksy
http://icsmodel.infracritical.com/

Cross-Trained Professionals Are Needed

Graphic used with permission of Joe Weiss



IT and ACS misunderstandings in policymaking

Listen to what the engineers are telling you!

"[Your proposed] cybersecurity requirements state that they are intended to address critical information infrastructure (including industrial control systems), however, your draft requirements do not address industrial control systems"

(Response to government draft regulations from a utility operator.)

Place yourself near your engineers and work as a team!



Photos by the author, used with permission

The team should contain experienced professionals who can converse in the language of engineering, industrial automation, OT, ACS, and Industrial IoT.

The CISO must see himself/herself as the hands-on coach of a winning team.

Do more than visit… Create multidisciplinary councils and go out into the field.

Key Messages

- Cross-trained professionals are needed to fill a serious gap
- Avoid IT and ACS misunderstandings in policy-making
- Place yourself near your engineers and work as a team

Author – Vytautas Butrimas

Vytautas Butrimas has been working in defense and cyber security roles for over 30 years including:

- Vice-minister at the Ministry of Communications and Informatics, Republic of Lithuania responsible for Information Society programs.
- Defense Policy and Planning Director, Lithuanian Ministry of National Defense (MoND) responsible for preparing the first Military Defense Strategy.
- Deputy Director responsible for IT security at the Communications and Information System Service (CISS) responsible for preparing the first National Defense System Cybersecurity Strategy
- Chief Adviser for the MoND of Lithuania with a focus on cybersecurity policy, including the national task force that wrote the Lithuanian Law on Cybersecurity
- Member (Presidential appointee) of the National Communications Regulatory Service's Council (RTT-Council)
- Cybersecurity Subject Matter Expert for the NATO Energy Security Center of Excellence (NATO ENSECCOE) who performed a Cyber Risk Study of the ICS Used in the NATO Central Europe Pipeline System (CEPS)
- Member of ISA 99 Workgroup 14 (Substation security profiles))
- Former Co-chair ISA 99 Workgroup 16 (Incident management)

Please click here to provide feedback on this MLM.