Oh Cyber Security doesn't affect me…right?

Colin Hamilton-Williams

October 21st 2019

Designing a brighter future

We live in an unprecedented time of human connectivity and functionality. We have come to expect more and more functionality from our devices, our offices and even our homes. As system designers, we are being asked to design, retrofit and upgrade systems to modern standards. This means not just thinking about what the customer needs, but what the customer will need and even making passive provision for things we haven't imagined yet…

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Overview

In this presentation we are going to discuss the application of Cyber Security, when to consider it, why to consider it and the benefits this brings from a Systems thinking concept. This topic will be discussed further through the following sections:

- Cyber Security
- Threat Vectors
- Systems Integration
- Lifecycle Influence on Cyber Security

Cyber Security

Oh Cyber Security Doesn’t Affect Me Right?

SNC·LAVALIN

ATKINS

Member of the SNC-Lavalin Group

Cyber Security

What is Cyber Security? In simple terms it is the defence or defensive strategies employed by a system to resist against both remote and local malicious or accidental actions. If we did not have Cyber Security then it would potentially be possible to hijack and control a system or systems potentially putting them into dangerous configurations.

Cyber Resilience

How does Cyber Security differ from Cyber Resilience? If we go back to our example of the seatbelt; Cyber Security is not crashing in the first place whilst Cyber Resilience is the seatbelt and airbag the prevent loss of life and injuries during the event of a crash. Thus, Cyber Security is the prevention of access to a system where Cyber Resilience focusses on recoverability and maintaining functionality, safety and integrity.

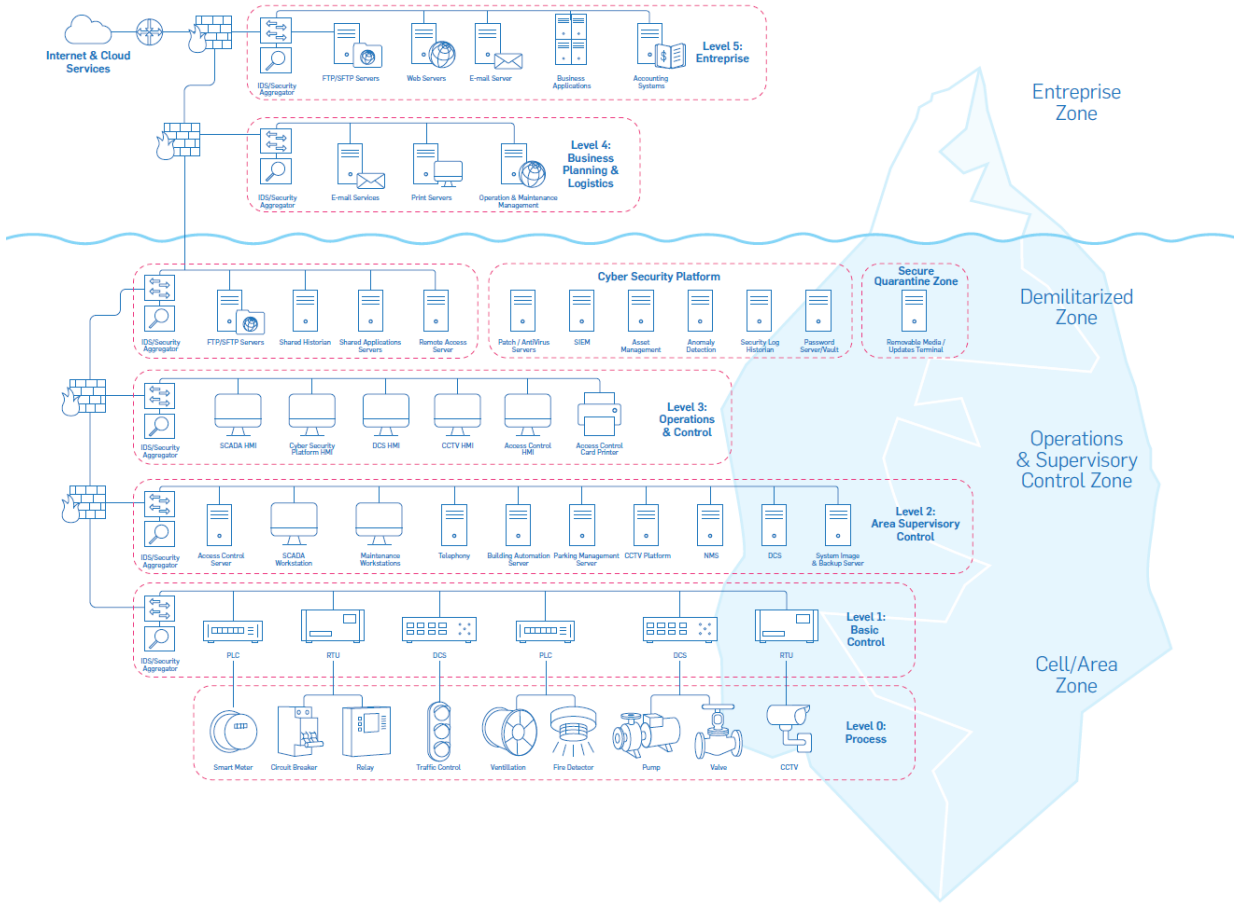
How is it achieved?

A cornerstone of the Cyber Security workstream is the Threat and Vulnerability Assessment (TVA). Gaining a system-level understanding of all the assets included within a digital ecosystem, their criticality, function and architecture is required to identify and analyze the threat vectors present in an industrial environment.

The Purdue Enterprise Reference Architecture was defined in ISA99 to capture Human-Machine-Interfaces (HMI) at the application level, through to the end-point assets, and “everything” in between.

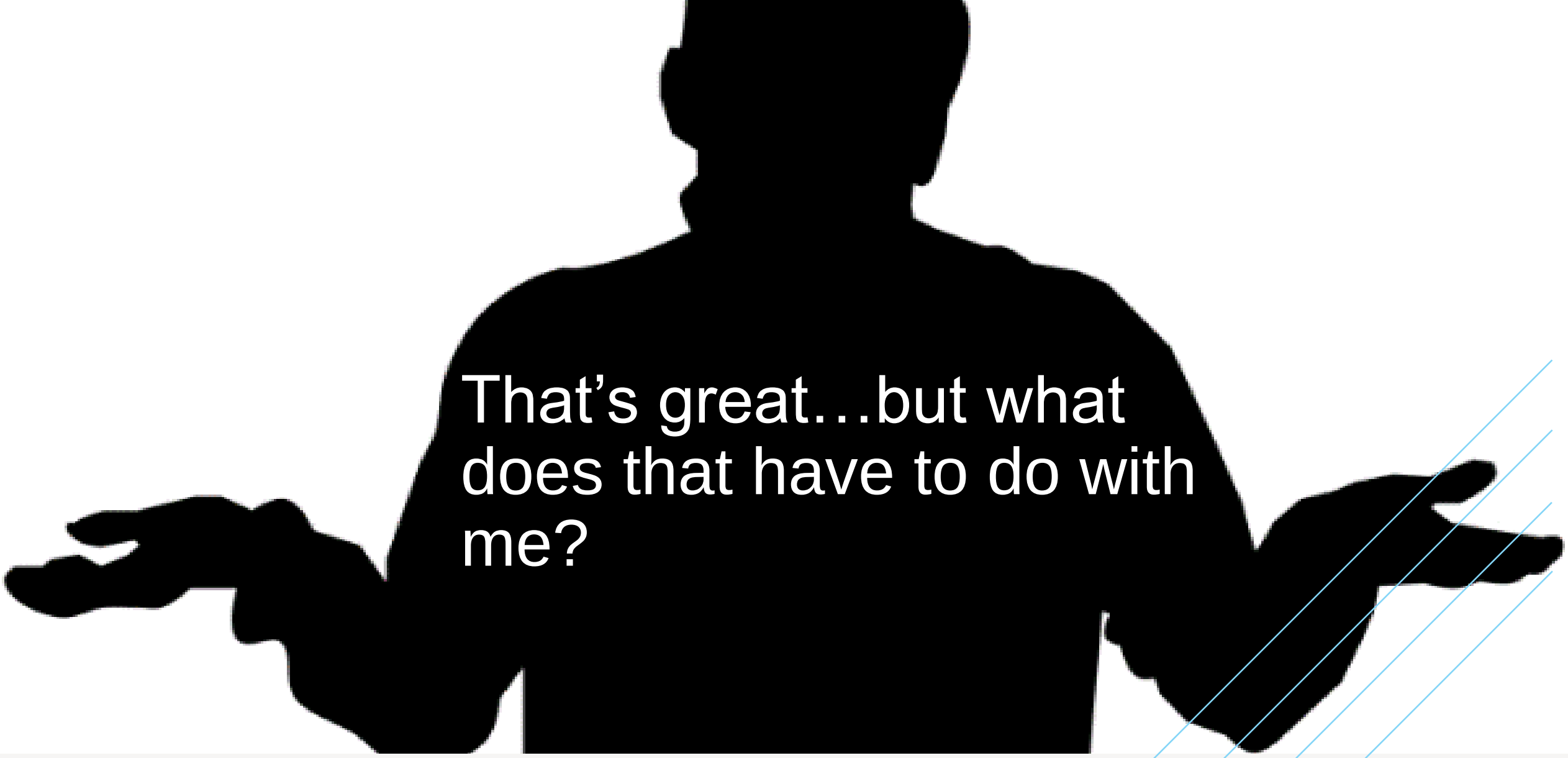
- **Enterprise zone (Level 5)**
- **Site business planning and logistics (Level 4)**
- **Demilitarized zone**
- **Operations and supervisory control (Level 3)**
- **Area supervisory control (Level 2)**
- **Local control (Level 1)**
- **Process (Level 0)**

The Purdue Enterprise Reference Architecture - Tweaked



SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group



SNC·LAVALIN

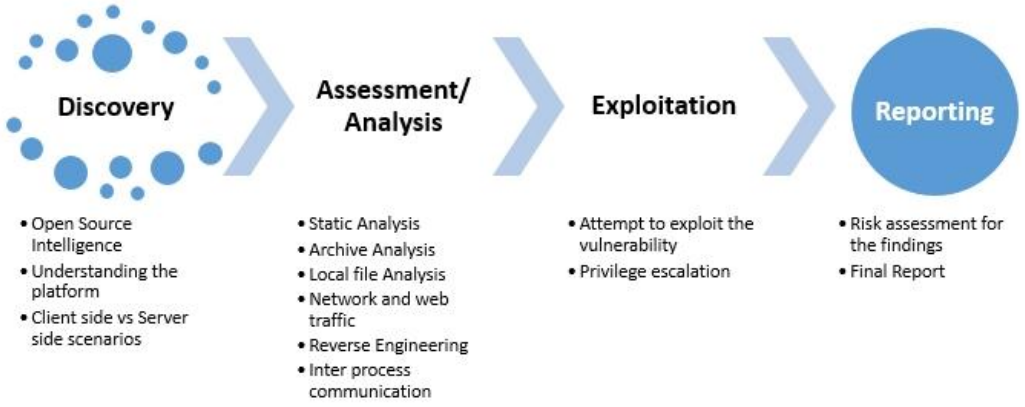
ATKINS
Member of the SNC-Lavalin Group

OSINT

Before we dive in, a couple of useful Cyber tools

Open Source Intelligence (OSINT)

› Intelligence gathering based on publically available information
› Now adopted by security organisations around the world
› Typical Pen-test using OSINT data methodology



Shodan

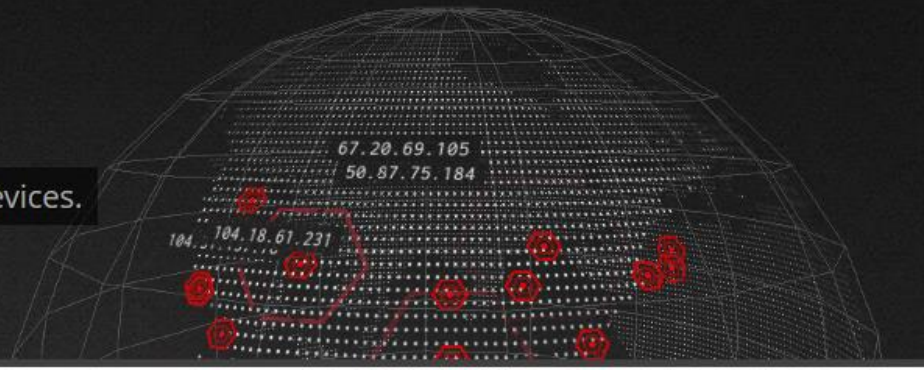
Shodan Developers Monitor View All...

SHODAN | Explore | Pricing | Enterprise Access | New to Shodan? | Login or Register

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account | Getting Started



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security

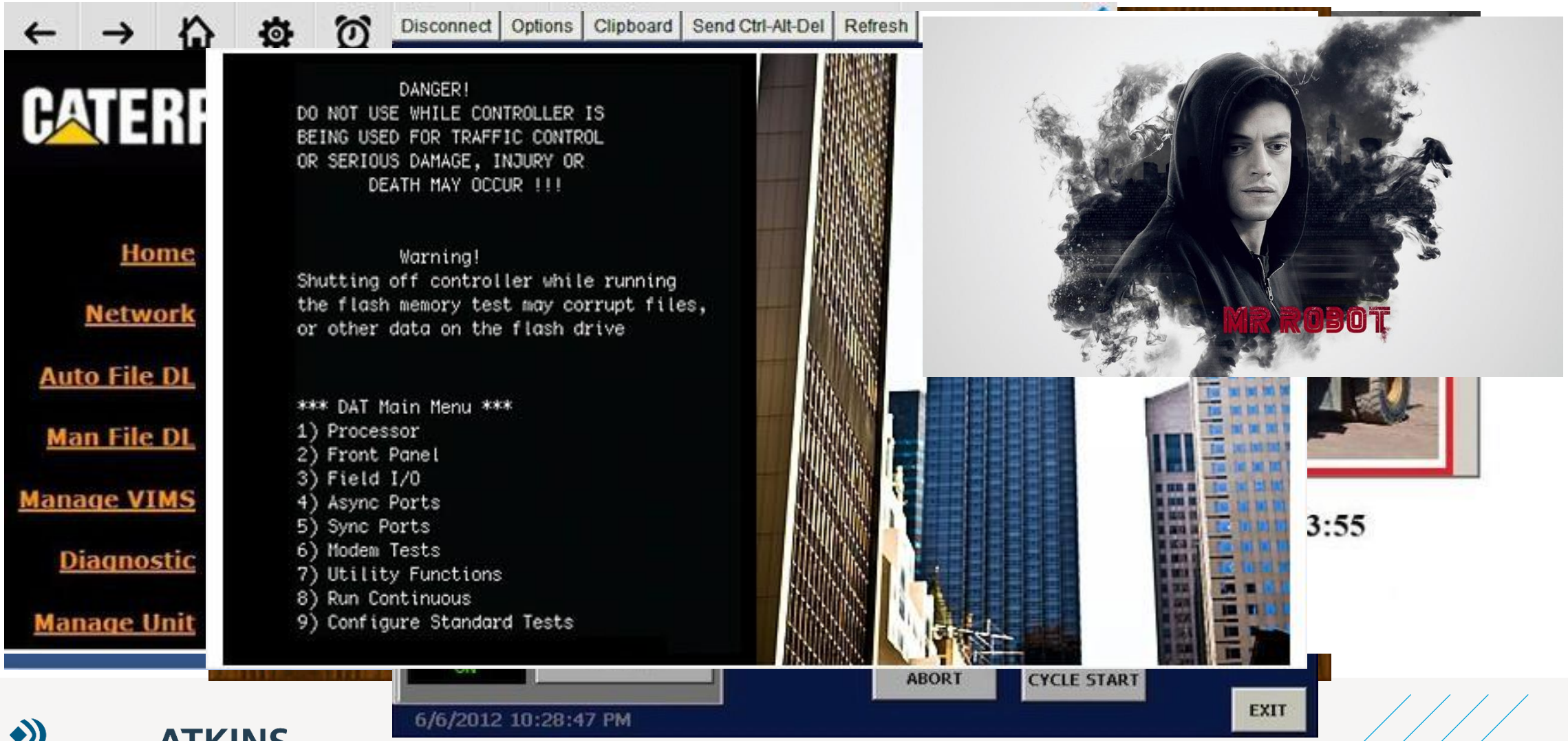
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

SNC·LAVALIN | ATKINS
Member of the SNC-Lavalin Group

A Crash Course In Bad Internet Practice



SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Threat Vectors

Ok, so that covers stupidity…but what other vectors are there?

- Humans!
- Malware
- Phishing and Ransomware
- Inadequate patching/outdated hardware and software
- Script Kiddies
- Data Miners
- And many more…

Some Ransomware Statistics

Stats for 2018

- Sonicwall just reported a 300 percent year-over-year growth in ransomware
- Global damage costs in connection with ransomware attacks are predicted to reach $11.5 billion annually by 2019.
- A previous report from Cybersecurity Ventures predicted ransomware damages cost the world $5 billion in 2017, up from $325 million in 2015 – a 15X increase in just two years.
- Cybersecurity Ventures predicts there will be a ransomware attack on businesses every 14 seconds by the end of 2019, up from every 40 seconds in 2016. This does not include attacks on individuals, which occurs even more frequently than businesses.
- Ransomware attacks on healthcare organizations are predicted to quadruple by 2020
- 91% of cyberattacks begin with a spear phishing email, which are commonly used to infect organizations with ransomware.

SNC·LAVALIN ATKINS Member of the SNC-Lavalin Group

Oh Cyber Security Doesn't Affect Me Right?

Systems Integration

SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

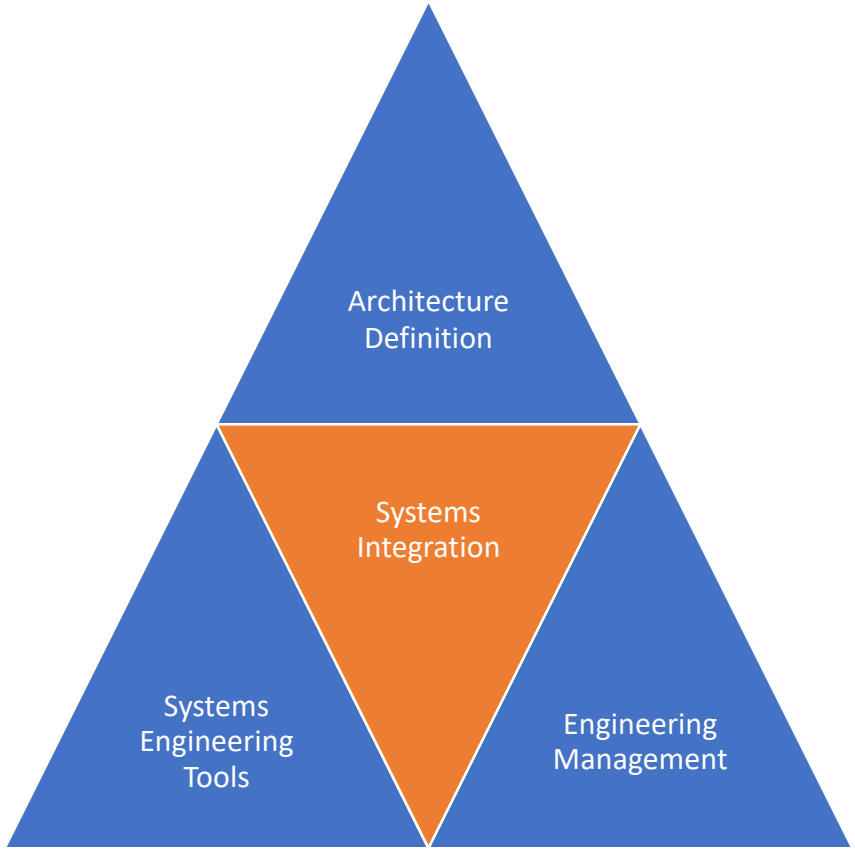
Many problems, some solutions

Whether a small upgrade or a greenfield new systems, the mitigations are still the same:

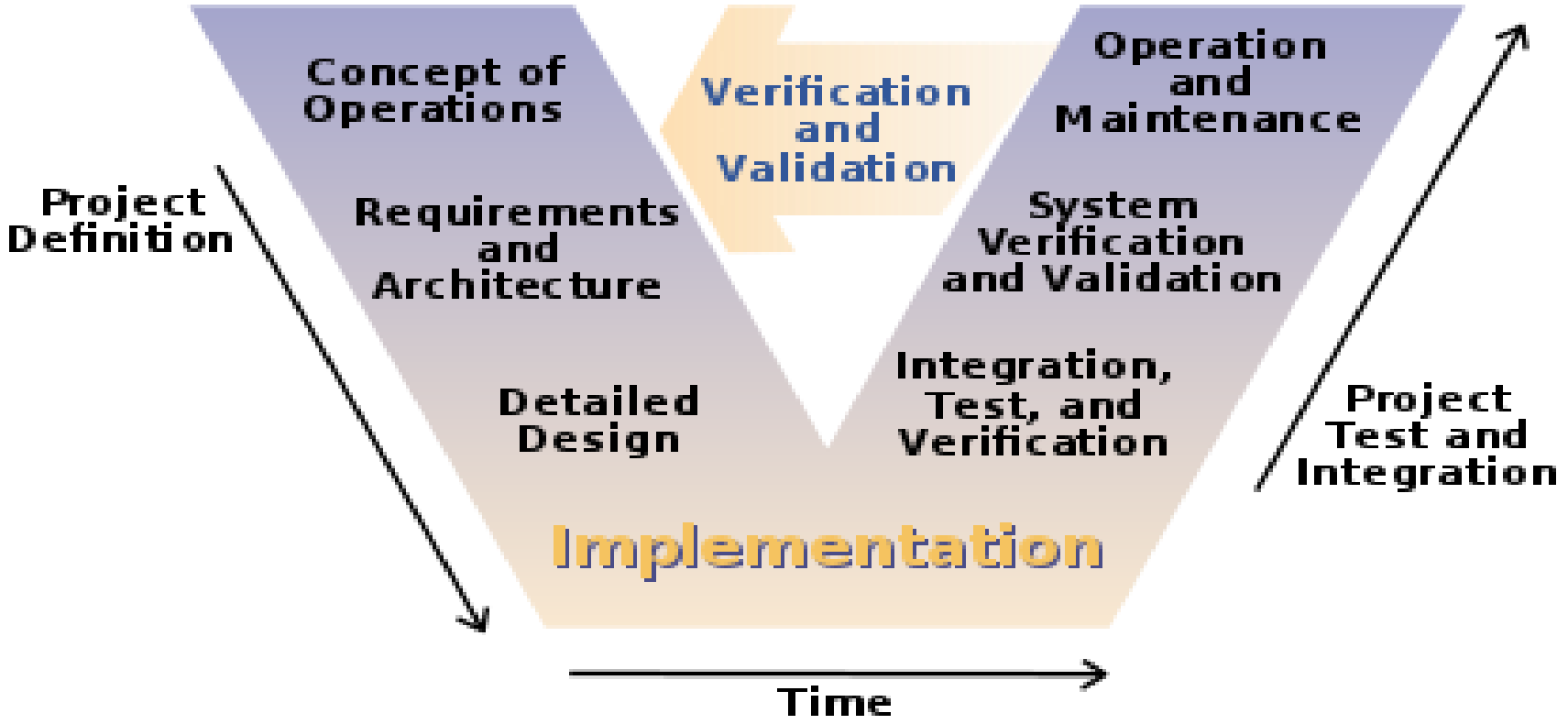
- Understand the concept
- Understand the user needs
- Understand the system context
- Define an architecture that achieves this

In addition:

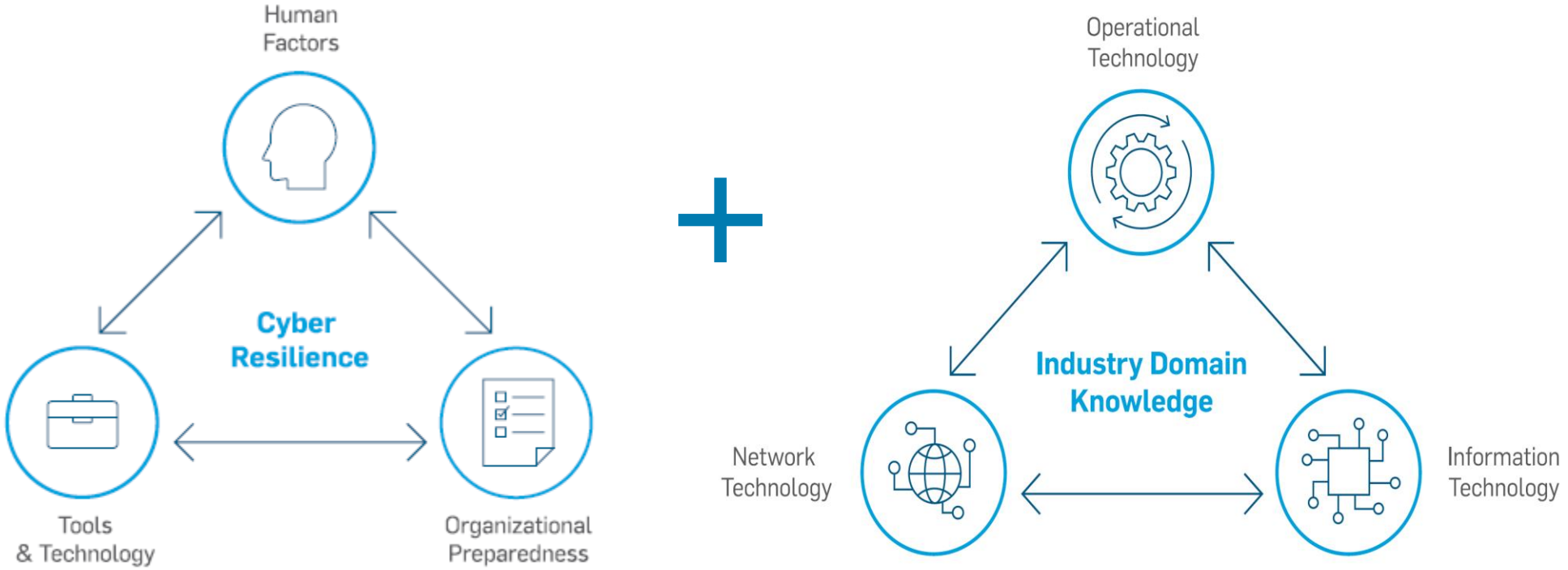
- Plan for negative tests
- Design for failure
- Model multiple threat vectors



Systems Thinking



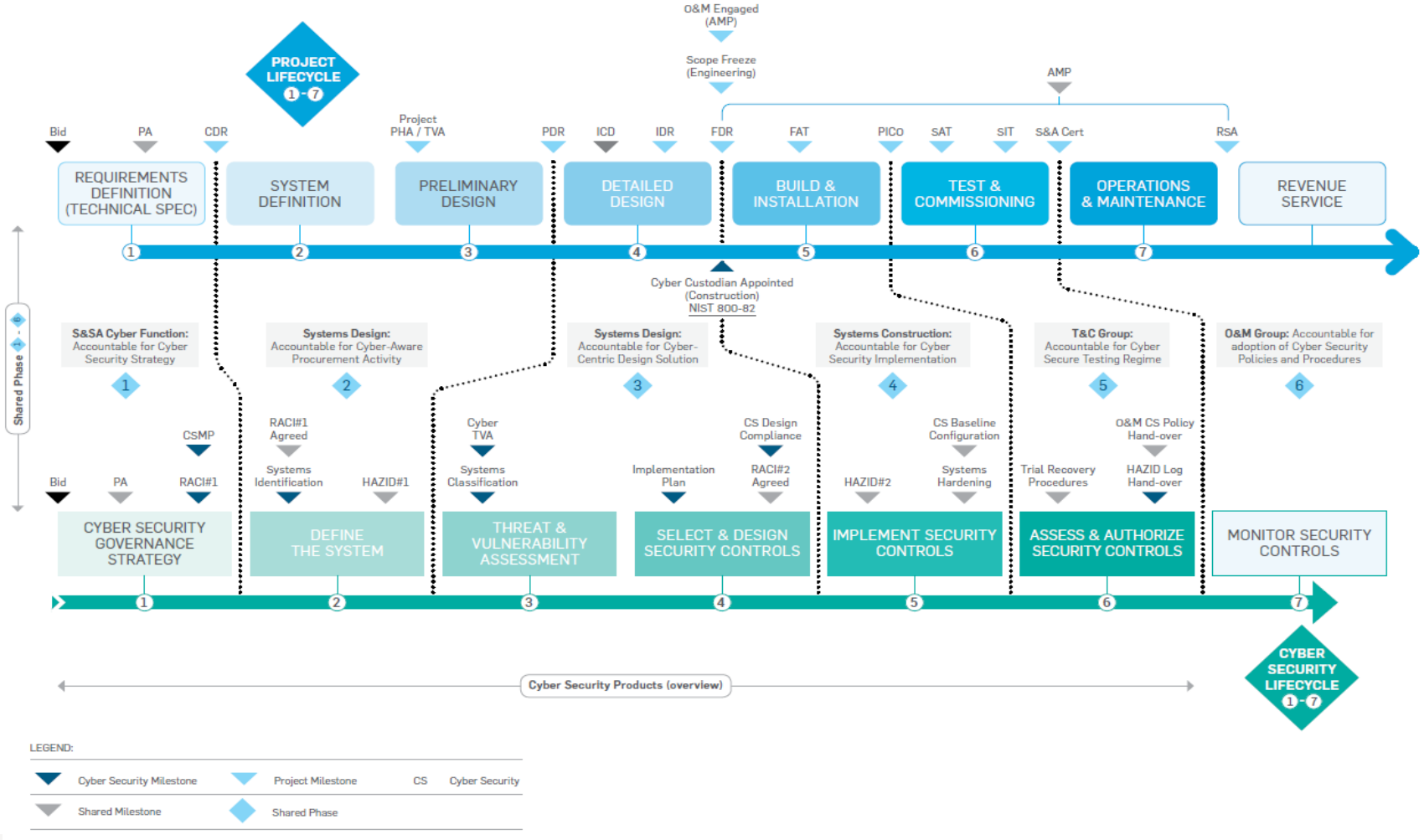
Using Systems Integration



SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Project Lifecycle and Cyber Life Cycle



SNC·LAVALIN

ATKINS
Member of the SNC-Lavalin Group

Summary

Cyber Security and Cyber Resilience are often after thoughts in complex multidisciplinary projects. Systems Integration, whilst often focussing on how a system should work, can be used to understand how a system may not work. It is therefore in the best interests of all major projects to actively engage these specialisms and combine their relative strengths to reduce costs, the risk of later rework and schedule delays and the overall risk to the system.

In order to deliver the most cost effective Cyber Security and Resilience, the earlier the engagement from the project

In some cases, the cost required to rectify or deal with a Cyber incident are significantly higher than they would have been if design considerations were incorporated at earlier project stages.

Our values are the essence of our company's identity. They represent how we act, speak and behave together, and how we engage with our clients and stakeholders.

SAFETY

We put safety at the heart of everything we do, to safeguard people, assets and the environment.

INTEGRITY

We do the right thing, no matter what, and are accountable for our actions.

COLLABORATION

We work together and embrace each other's unique contribution to deliver amazing results for all.

INNOVATION

We redefine engineering by thinking boldly, proudly and differently.