OPERATIONAL TECHNOLOGY (OT) OVERVIEW

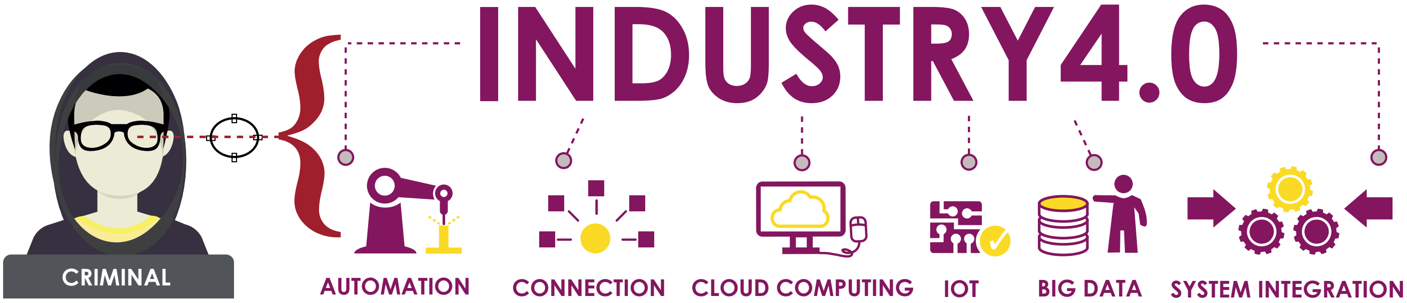
Many organisations are consolidating their approach to the deployment of technology across the enterprise. Chief Information Security Officers (CISO's) from all industries are constantly being pressured by directives from the board to 'do more with less'. In addition, Operational Technology (OT) environments that were once the preserve of engineering teams are now becoming the responsibility of the IT teams under these directives to promote operational efficiencies and lower operating costs.

OT SECURITY DEFINED

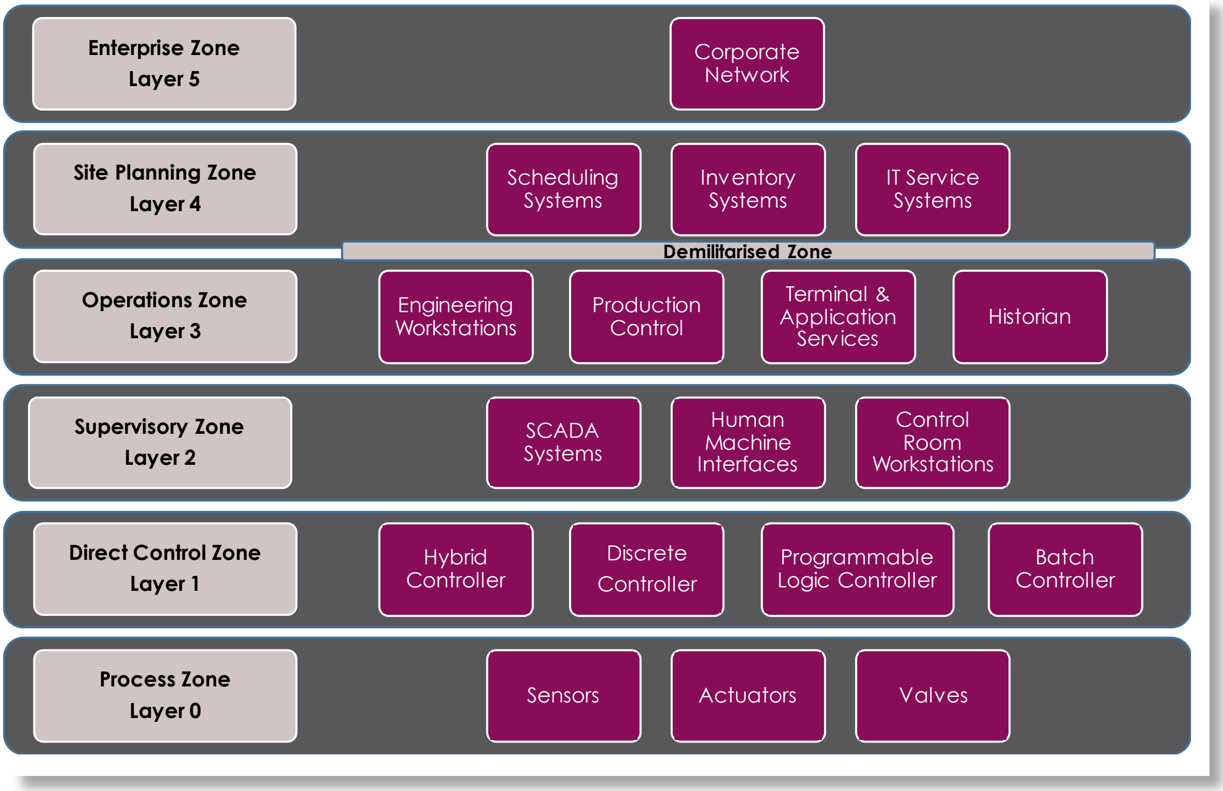
The term Operational Technology is used widely to define IT hardware and software that's dedicated to controlling processes through direct monitoring and or control of physical devices such as valves, pumps, switch gear etc. OT can be found in many of today's industries from the control of water treatment plants, through the energy sector where OT is utilised to control energy generation and power distribution; to manufacturing production lines and the baggage handling systems in many of today's modern airports.

Operational Technologies were introduced in the late 1950s and, historically, have been deployed in an isolated manner to address control and monitoring across a physically separate environment to that of the IT environment. These OT environments utilise dedicated servers / workstations that interface with the various devices to carry out the monitoring and control functions autonomously.

OPERATIONAL TECHNOLOGY IN THE CROSS HAIRS OF CYBER CRIMINALS



Operational technology is currently undergoing its 4th revolution. From the first revolution utilising steam powered mills to the programmable productions lines of today; Each revolution has sought to increase operational efficiency and lower operating costs. The latest revolution is converging IT and OT systems onto a single enterprise wise network creating the industrial Internet of Things (IIoT). This initiative fosters greater operational visibility, efficiency and subsequently lower manufacturing costs. The challenge of convergence is that it introduces some security concerns that need to be addressed to ensure that the organisation remain protected from cyber threats including espionage, data tooling corruption and exfiltration.



Enterprise Zone Layer 5: Corporate Network

Site Planning Zone Layer 4: Scheduling Systems, Inventory Systems, IT Service Systems

Demilitarised Zone

Operations Zone Layer 3: Engineering Workstations, Production Control, Terminal & Application Services, Historian

Supervisory Zone Layer 2: SCADA Systems, Human Machine Interfaces, Control Room Workstations

Direct Control Zone Layer 1: Hybrid Controller, Discrete Controller, Programmable Logic Controller, Batch Controller

Process Zone Layer 0: Sensors, Actuators, Valves

Figure 1: Operational Environment Overview

Figure 1 provides a high-level overview of a typical operational environment that has been converged with the corporate IT environment. Each layer of the diagram relates to a separate functional layer that is representative of a typical OT deployment. This deployment approach loosely aligns to the Perdue Reference Model (PRM) for enterprise architecture. The PRM provides a model for enterprise control, which end users, integrators and vendors can adopt in integrating applications at key layers within the enterprise.

- **Layer 0** - this is where you'll find the hardware that's controlled by the layer 1 componentry. This includes actuators, valves, motors and sensors.

- **Layer 1** - represents the direct control tier where you will find the intelligent devices such as programmable log controllers which will affect the change to the layer 0 hardware and sensing devices that will analyse the effect of the changes carried out on the lay 0 devices.

- **Layer 2 -** represents the supervisory tier where you will find systems supervising, monitoring and controlling the physical processes in real time. Typical devices at this layer include Human

Machine Interfaces (HMI), Supervisory Control And Data Acquisition (SCADA) and Distributed Control Systems (DCS) which oversee the controllers within layer 1.

- **Layer 3** - represents the operations layer, where many of the OT solutions are typically managed, measured and overseen. Managing production work flow to produce the desired products. Batch management; manufacturing execution/operations management systems (MES/MOMS); laboratory, maintenance and plant performance management systems; data historians and related middle-ware. Think of this tier as being a centralised networks operations centre. From this tier a site wide view of operations can be controlled via messaging through the layer 2 components.

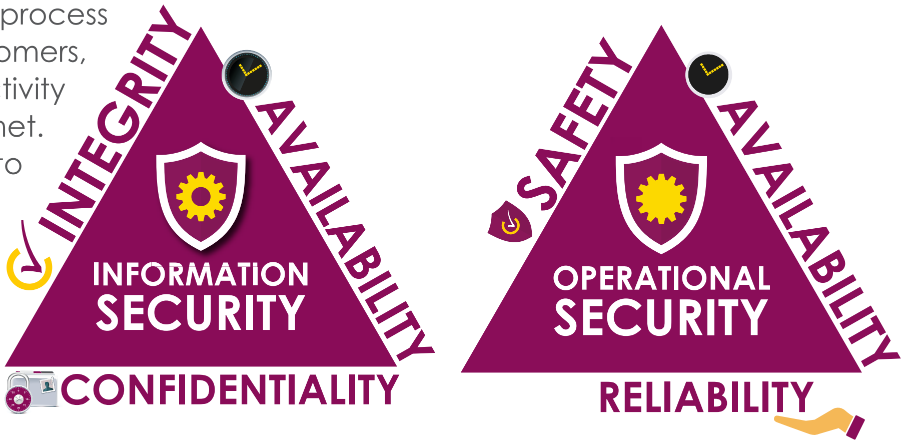
- **Layer 4** - represents the site layer of the model. Its at this point that the business- related activities of the manufacturing operation are managed. ERP is the primary system; establishes the basic plant production schedule, material use, shipping and inventory levels Geographically dispersed operations can be reported on centrally and updates made to control and affect systems globally.

- **Layer 5** - represents the traditional corporate IT environment. This connectivity afforded provides the ability to centralise operations and visualise an enterprise wide, end to end, view of the operation.

WHY IS OT SECURITY IMPORTANT?

Over recent years Operational Technology (OT) has become an easy high impact target for cyber criminals looking to affect normal operations, damage reputation or, most concerningly cause harm to human life. The water, nuclear energy, oil & gas, aviation services and financial industries being considered the most vulnerable as disruptions of their operations are anticipated to have the greatest and most immediate national impacts.

Many businesses strive for improved OT process efficiency and reliability for their customers, which often results in increased connectivity to enterprise technologies and the Internet. This convergence has the potential to increase system vulnerabilities, but can be addressed by adopting sound risk management principles, which are the same regardless of the underlying system type. Advancements in technology coupled with the desire for organisations to operate with a more efficient, flexible and expedient operating model has created what could be considered as a cyber threat playground for attackers.



Recognising the threat to national security as many OT environments form part of the nationals Critical National Infrastructure (CNI), The National Cyber Security Centre (NCSC) published a number of documents focusing on securing industrial control systems.

When considering the security of OT environments, the view changes from what we typically see within the IT world. Security for IT environments typically centres around the fundamentals of information Confidentiality, Integrity & Availability. Given that nature of OT environments and the critical functions they perform, OT priorities are considered to be safety, reliability and availability. Should a failure or malfunction of an OT component occur, it has the potential to have a catastrophic impact, especially if part of a CNI system.

Securing the OT environment from cyber threat is therefore a complex undertaking. It's made more complex due to many legacy issues as well. OT environments have a long lifecycle once deployed. In many instances this can be 10, 15 or even 20 years plus. As a result, deployments are installed with a 'spares forward' approach that ensures replacement parts are provided from day one of the installation, covering the solution should any component go end of life during its operational time period.

WHAT HAS THIS GOT DO WITH CYBER THREAT?

Converged IT/OT environments might utilise the same physical interfaces and connectivity, but from there the similarities appear to end. Many OT deployments that are in operation today are based on technologies from yesterday, looking specifically at security controls for a moment, many of the OT devices were not designed to be connected to the Internet or WAN for that matter. It's not unusual to find an OT deployment that's SCADA system is operating on Windows XP, NT4 or event DOS. These legacy operating systems are no longer maintained by the vendor and many well documented exploits and vulnerabilities remain unpatched across these systems. As a result, the security controls are at best very weak and in many cases hard coded into the OT fabric and thus not easily changed. For this reason, many OT vendors do not recommend the adoption of a converged legacy IT/OT environment.

Think of this like having the default admin password enabled on your home router. Opening this level of security up to an uncontrolled network could have catastrophic consequences.

If we assume that the OT equipment was capable of robust authentication we still have an issue relating to risk and understanding the impact of changes made across the OT environments. An example of this would be the locking down of an IT environment following identification of a breach. Within an IT environment, one of the initial steps you may take to limit exposure would be to lock down the environment or quarantine the affected asset as you'd seek to maintain the confidentiality and integrity of the system whilst only affecting availability. Within a typical OT environment locking down in this way may have a detrimental impact. For example, if you were to quarantine an endpoint that controlled power distribution, the loss of power that resulted will certainly cause disruption with may impact life.

INSECURE POOR PASSWORD PRACTICES LEAVE OT OPEN TO ATTACK

In summary, from an operations perspective the convergence delivers the efficiency, visualisation and flexibility initially desired. The problem is that it also entertains a number of risks that need to be understood and addressed to ensure smooth safe prolonged operation of the OT environments:

SECURITY CONTROLS

- Traditional OT deployments have a very limited security posture. In many deployments basic authentication is hard coded into the communicating components and cannot be adjusted.

These credentials can be easily discovered by searching across the Internet. This wasn't considered a risk previously as the OT environments were physically separate internally facing systems

UNDERSTANDING OF RISK

- OT environments have a physical function, it maybe controlling a valve, monitoring system temperature, switching power distribution. Each of these functions is critical to the OT system. Should any of these be adjusted without an understanding of the impact, OT administrators may not be aware of the impact of broadcasting.

EXPANDING CYBER THREAT LANDSCAPE

- Legacy solutions operating upon end of life operating systems pose a potential risk as documented vulnerabilities within the underlying OS could be exploited following convergence through a credentials-based attack and go undetected by monitoring solutions.

VISIBILITY

- OT environments typically have limited tool sets dedicated to security-based monitoring. For devices that have a log generation capability (OS applications etc.) they may no longer be supported log collection configurations by monitoring solutions of today.

Cyberseer provide an advanced threat detection and response service that helps provide successful defence against advanced actors in real time protecting both the IT and OT assets across the enterprise. Cyberseer utilise the latest next generation behavioural analytics and machine learning technologies and industry experts in Cyber Threat to deliver a 24/7 advanced threat detection service.

Behind this process lies a vast extent of human expertise and continued exploratory work to identify, investigate and analyse unusual behaviour that may be indicative of threats in real time as they occur. For every incident detected, Cyberseer Analysts draw on their expertise, external sources of intelligence and the context of your network before presenting you with an informed and considered explanation of the threats you face.

Cyberseer recognise that no two OT environments are identical, be it geographically dispersed operations, multiple iterations of identical components on a production line, shared accounts used for daily operation etc. Each Cyberseer service therefore need to accommodate and address the impact of these changes and amendments to the typical PRM architectural template. In support of this, Cyberseer will work with the Customer to understand the OT environment geography, model of operation and other factors. Once this process is complete, service design and technology options will be discussed aligned to the monitoring requirements.

Talk to us about customer use cases.

Demo both machine learning technology and the Cyberseer service.

☎ CONTACT US +44 (0)203 823 9030

If you would like to find out more about how the Cyberseer team can make difference within your organisation with regards to advanced threat detection, contact us today: **info@cyberseer.net** | **www.cyberseer.net**