NCSC Design Principles and Operational Technology

A fictional case study exploring the application of our secure design principles.

If you are responsible for the design or maintenance of an Operational Technology (OT) network, this study will help you to navigate the cyber security issues you will encounter as you design your cyber-physical system.

Last year we published our new cyber security design principles. Based on the NCSC's experience of architectural review and handling incidents across UK Government and Critical National Infrastructure (CNI) systems, these principles are intended to help architects and designers produce secure and resilient systems.

The principles cater for both IT and OT systems but it can be difficult sometimes to see exactly how a principle should be applied in any given case. So in this example, we're going to walk through the design process for an OT system, guided all the way by the secure system design principles.

Meet 'Admin Corp'

Let's imagine we're following a fictional organisation who are responsible for making decisions about the cyber security of a CNI processing plant.

Admin Corp runs a plant that produces Adminox, a highly volatile, refined form of administrative paperwork that is *essential to every organisation in the country*. It is created from volatile raw products using a continuous chemical process.

As an essential service, Admin Corp must comply with the EU NIS Directive. This means that Admin Corp's network, information systems and technology needed for the production of Adminox must be protected from cyber attack.

Also, because Admin Corp are regulated for safety by the UK Health and Safety Executive, they must take steps to ensure the continued safety of the Adminox production process.

Admin Corp - system requirements

The process for producing Adminox involves a number of steps, with the final product stored under pressure in a tank. Clearly, no one would benefit from the unconstrained release of this Adminox, with the potential for additional red-tape clogging up local services for years.

Admin Corp's system therefore has *two critical non-functional requirements*:

- As a responsible and safety regulated company, they need to keep the local environment safe from release of Adminox.
- Maintaining the availability of the product for customers in order to continue as a profitable company.

Applying the principles

The design principles should be applicable whether there is an existing architecture which requires re-design or a completely green-field site. In Admin Corp's case there is an existing architecture which they wish to improve.

Let's walk through each of the NCSC design principles and see how they can be applied to achieve the non-functional requirements:

---

1. Establish the context before designing a system

"Determine all the elements which compose your system, so your defensive measures will have no blind spots."

The most important first step here is to gain a complete, end-to-end understanding of system operation, which parts are critical and to identify the organisation's approach to undesirable consequences.

Implementation of this principle is likely to require involvement from all parts of the business: information technology teams, cyber security engineers, process operators, process control specialists and functional safety engineers (amongst others!),

Attack trees
Admin Corp want to understand the threat model for the Adminox processing system, so will gather relevant experts to build attack trees. These will illustrate the path an attacker would need to take to achieve a specific impact on either safety or availability. Note that an impact may only become noticeable when, for example, a disabled safety system is called upon. These attack trees will be used to inform design decisions later on.

Network zoning
As a fundamental part of this design, Admin Corp create a series of zones to group systems from which similar impact would occur if an attacker was to compromise them.

Separate zones are built for Business, Process and Safety functions. The premise being that if an attacker gains access to the Business zone, then the worst impact they could have is disruption to the running of the company, communication with customers etc.

Penetrate the Process zone, where the Process Control System (PCS) lives and the attacker can disrupt operations, causing a product availability issue.

Finally, if the attacker gains access to the Safety zone, then they may be able to adjust safety parameters to cause a destructive physical effect.

In our example, Admin Corp have a fairly simple zone configuration, but for larger systems, network zone design decisions are likely to be influenced by product design, geography and physical protection of the infrastructure (amongst other factors).

The Purdue model may act as a helpful reference model for this part of the design process.

Critical Zone Boundaries
Having created their attack tree and network zones, Admin Corp then walk through them, identifying the key points in the architecture where it might be possible to detect or prevent an attacker from achieving their goals - focusing in particular on the zone boundaries.

At each of these points, later in the design process, Admin Corp will reduce the attack surface by deploying countermeasures. In this way, even if an attacker reaches that part of the system they are going to be highly constrained and likely detected in their attempts.

As an example, think back to the 2015 attacks against the energy networks in Ukraine. Here, according to open-source reports, the attacker's actions weren't visible to the operator until the point at which they were moving the mouse around on the screen of the computer that ran the control system.

Ideally, the attacker's actions should have been spotted or prevented before this point. Identifying and protecting key network choke-points will help with this.

Supply chain security

Also at this point, although beyond the scope of this blog, it's important for Admin Corp to consider supply chain security. Specifically, Admin Corp will be considering how to gain assurance that new process logic, configurations, software, patches and other changes to the system do not impact on the key non-functional requirements.

Network design and documentation

Having established some of the fundamental aspects of the system, Admin Corp will then generate, communicate and agree upon a simple diagram of the plant, that depicts an end-to-end understanding of the physical process and logical network design. This will include the Business, Process and Safety zones and the boundaries between them.

Clearly documented on this diagram are the consequences the organisation has decided they are not willing to accept and the mitigations which have been deployed to prevent those consequences occurring.

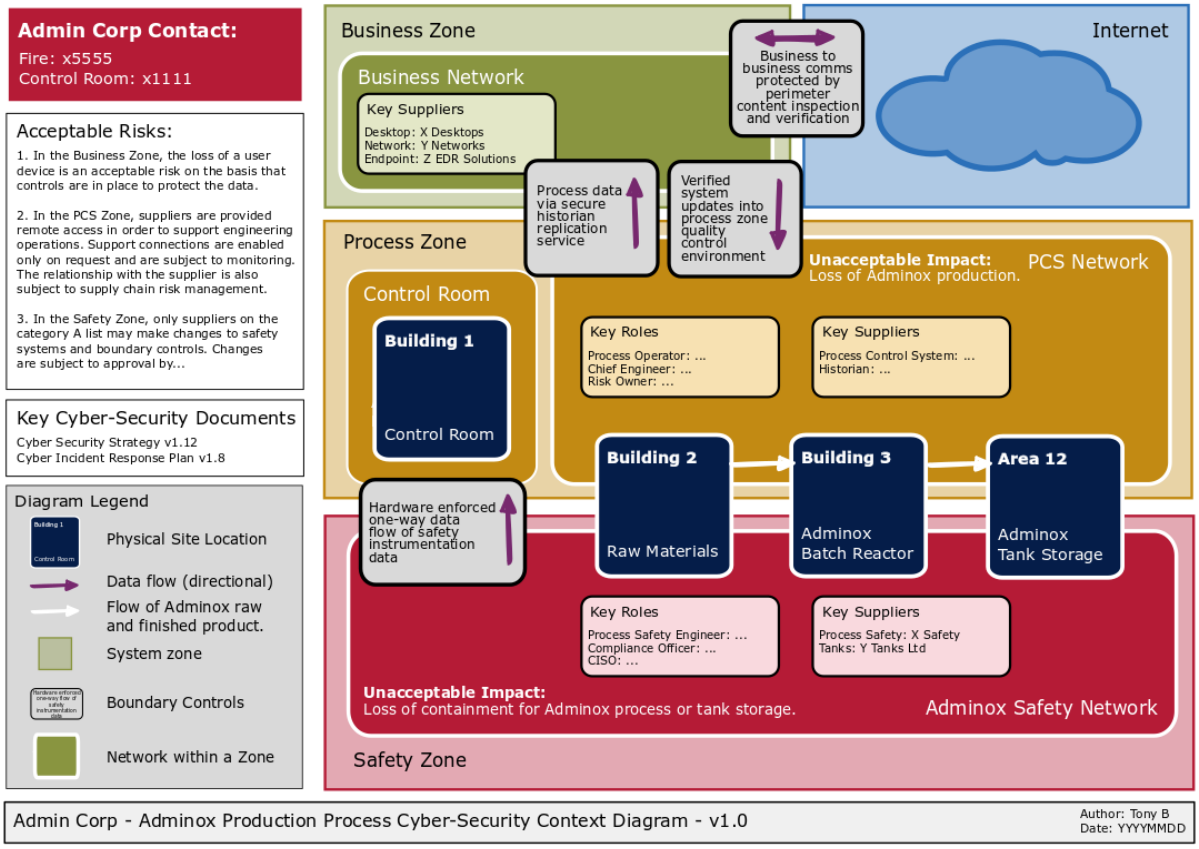
Also depicted are the roles responsible for maintaining the operation of the system, both from a process perspective and a cyber security perspective (include the role that suppliers play). Later on, Admin Corp will use this to ensure that suitably qualified and experienced people are assigned to relevant roles and ensure that there is no ambiguity about responsibilities.

The diagram will enable good decision making by ensuring critical knowledge is widely understood. However, of equal importance is that it will also help develop a shared risk proposition with suppliers who may be involved in the maintenance of the plant or needing to conduct incident response in the event of a cyber attack.

Some organisations may choose to use existing risk models such as Bow-tie to illustrate the mapping of cyber security controls to undesirable impacts and consequences.

A simple network diagram

The Adminox system diagram could look like this:



Having got to this point, Admin Corp now use the NCSC guidance on governance to set-out clearly how security risks to the Adminox production process are governed.

---

2. Make compromise difficult

"An attacker can only target the parts of a system they can reach. Make your system as difficult to penetrate as possible."

Having understood the context and armed with the diagram, Admin Corp will start making compromise difficult for the attacker.

Considering the original requirements, each of the network zones will require incrementally higher levels of confidence that the boundaries separating them from the layer below will stop an attacker.

Admin Corp would like to have greatest "trust" that the Safety zone has not been compromised, followed by the Process zone and finally the Business zone.

The key to making compromise of these boundaries difficult is to implement the following practices:

Do not trust external input
Browsing the Internet from the control room: Any input data coming from a lower trust zone could result in the exploitation of the system processing it. This means it's important to consider carefully the types of data you're bringing into and processing in the higher trust zone.

In the Admin Corp example, the operators with computers in the Process zone require access to the Internet and email in order that they can manage the process effectively. However, giving these system operator terminals in the Process zone direct access to content downloaded from the Internet would be an example of a "browse-up" anti-pattern, which could result in compromise of the Process zone.

To prevent this, Admin Corp will develop a secure browsing system based on a Virtual Desktop Infrastructure (VDI) solution. This system effectively creates a virtualised window up into the Business zone which is created and destroyed as users require it. If malicious content is sent to the VDI system, it will be contained and eradicated from there before it is possible for the attacker to affect the process. This is an example of a "browse-down" pattern, where riskier activities are isolated using a separate processing context.

Admin Corp also realise that their process and safety engineers have the same requirement for their engineering laptops (to browse the Internet and access email). To mitigate the risk of compromising the Process zone, they extend use of the VDI environment to these users too. Through policy and technical controls, the engineering laptops are only permitted to access the Process and Safety zones (via a dedicated Process zone VPN gateway discussed in more detail later).

Enforce one way flow
Visibility of the safety system: For regulatory reasons, Admin Corp want to have visibility of the safety system so they can monitor plant safety in real-time.

Admin Corp's executive board have decided that - due to the potential consequences - any electronic connectivity between the Safety and Process zones must only move data from the Safety zone from the Safety system (a one-way flow).

Admin Corp will use hardware known as a data diode to enforce one-way flow. This will prevent attackers from conducting online interactions with the safety systems and stop other malware in the Process zone impacting on the Safety zone.

Reduce the attack surface
Considering each of the boundary systems between the different zones of the network in turn, Admin Corp will look at the attack surface presented to an attacker operating in the lower 'trust' zone and reduce it by:

- Switching off unnecessary system and network services
- Implementing firewall rules which deny everything except for agreed critical network services
- Prioritise pushing sensor data from the higher trust zone to the lower trust zone and conducting complex operations such as data analytics in the low trust zone. They will prefer tried and tested approaches to ensure simple and well understood mechanisms are put in place to push data out of the high trust zone
- Avoiding exposure of services in high trust zones to access from the low trust zone. This is important because, exploitation of these cross-border services could lead to the attacker gaining access to the high-trust zone. However, in some cases, cross-border access will be unavoidable. For these cases, Admin Corp develop and test strong authentication mechanism to control access to any services exposed across the boundaries. For some use-cases it may also be appropriate to consider implementing the NCSC's pattern for safely importing data.
- Hardening all boundary hosts against attack by using modern operating systems and configuring contemporary mitigation measures to make it much harder for lateral movement to be successful.

Gain confidence in crucial security controls
The Admin Corp operations team are unhappy with the idea of a red-team test against their live systems. They worry about the potential this has for impacting operations.

This is a reasonable position to take, so they scope a red-team test very carefully, with the objective of penetrating the non-critical boundary systems within the Process zone (such as a historian or data-transfer system).

If a simulated attacker can successfully reach those systems without being stopped or detected, then it will be necessary to do more work to harden the attack surface.

Additionally, given the potential for safety consequences, Admin Corp create a lab environment in which the core systems and boundary between the Process and Safety zones are replicated. Lab testing provides a way to gain confidence that their data diode is operating effectively. This replicated environment allows effective red-teaming to be conducted safely.

In a further effort to obtain assurance without impacting production, Admin Corp also run a table top red team activity (paper-only) and architectural review with skilled security architects.

---

3. Make disruption difficult

"Design a system that is resilient to denial of service attacks and usage spikes"

To ensure the resilience of an OT system with high availability requirements, you will need to consider the design from a number of different perspectives. Design decisions will need to take into account physical, environmental, geographical and technical factors.

Overall system resilience can be achieved in many ways. For instance, by having multiple paths to a single destination, deploying redundant systems, or using geographically separated distribution networks.

These design decisions can lead to a good level of resilience - one that will cope with system failures or environmental incidents such as weather events. However, in

some cases, design decisions can have an adverse impact on cyber security resilience. For instance, if multiple redundant servers are deployed, running the same version of vulnerable software, this would not be resilient from a cyber security perspective. An attacker would only require a single vulnerability to disrupt production. So, an attempt to reduce the likelihood of system failure could result in poor cyber security resilience.

The designers of the Admin Corp process are therefore mindful of the potential for a single vulnerability to impact their system. Through their work to develop an attack tree, they identify that the Process Control System (PCS) has a number of system components that are deployed in a redundant configuration, intended to maintain availability of the process. For compatibility reasons, they are unable to change the system design to include a different manufacturer's components. Instead, they work with their supplier to ensure that robust cyber security controls are placed around the components, thereby making disruption difficult.

---

4. Making compromise detection easier

"Design your system so you can spot suspicious activity as it happens and take necessary action"

Having set out the system context and defined network zones, Admin Corp now needs the ability to detect when an attacker is operating in their OT environment.

Collecting logs
Admin Corp will be able to detect intrusions by collecting all relevant security events and logs. This is particularly important for the systems that sit on the edge of zones and communicate with lower trust systems.

Not all sensors, actuators and field equipment produce security events or logs, so it's important to focus on the systems in the path of the attacker which *do* produce events and logs.

Previous attack tree modelling work will help Admin Corp determine where best to focus their efforts, but they also choose to develop even more detailed attack hypotheses, using expert advice find the most valuable data collection points in the architecture.

Admin Corp decide to use the NCSC's Logging Made Easy for hosts in their Business Zone, while they establish a business case for investment in a more expansive Security Operations Centre.

Detecting malware
A key objective in collecting logs is to detect malware command and control communications.

A malware infection may be intentional or unintentional. Whichever the cause, early detection of the malware command and control activity is likely to reduce the potential impact. This is important because, even if the malware is unable to communicate with its controlling system it could still cause damage. For example, data deletion malware does not need to phone home in order to do damage.

Collection and analysis of domain name requests and attempted connections to Internet systems from OT environments are important steps towards detecting malicious activity.

Keep the attacker in the dark
When monitoring for command and control activity, it's important to ensure that an attacker *does not realise that they have been detected* - or they may change their approach and become harder to detect.

This is achieved by ensuring that monitoring is independent of the system being monitored. Or in other words, use optical network taps and security controls to prevent an attacker gaining access to the monitoring environment. This approach will also make it difficult for attackers to detect security rules through external testing and as a consequence reduce the likelihood that the attacker will achieve their goals.

Simple communication
Detection of an attacker's activities is easier if there are simple communication flows between components.

In Admin Corp's design, they deploy a single, multi-factor authenticated, VPN gateway to provide access to the OT environment. Having gained access through this gateway, a bastion host constrains user activity to agreed policies. After this, network and host detection rules allow security analysts to understand what is normal and detect abnormal states or behaviours.

This gateway allows Admin Corp to provision and control access for remote engineers, integrators and suppliers, all of whom are using systems that Admin Corp trusts to the same degree as the Process Zone.

Access to the Process Control System (PCS)
Admin Corp's Process Control System (PCS) is the brains of their production process. It is a vendor-provided solution that takes inputs from sensors across the plant and reflects that state on Human Machine Interfaces (HMIs). It then uses pre-configured logic to control the process and allows the operators to interact via the HMIs in order to respond to alarms, carry out maintenance and ensure the continued operation of the plant.

Admin Corp also uses a historian to record data from the process, which can be used report on process efficiency, enable maintenance and conduct other engineering operations.

In Admin Corp's case there are a number of use-cases for access to the PCS

1. Read-only PCS data for business analysts and regulatory compliance officers (desktops connected to the Business zone network).
2. Fully functional PCS screens for control room operators (desktops connected to the Process zone network).
3. Direct control of valves and actuators affecting the process of generating the *Adminox* product (in the Process zone).

It may be tempting to consider the Human Machine Interface (HMI) component of the PCS an adequate boundary between different zones of the system. Indeed, in some cases, this may be the pattern endorsed by the manufacturer.

Given the requirement for read-only screens in the Business zone, it might be tempting to make holes in the firewall to allow hosts in the Business zone to connect to the PCS. By doing this though, the number of opportunities to detect the attacker before they can impact the availability of the PCS is reduced.

If Admin Corp were to expose the PCS through the firewall to the Business zone network, the attacker may need just a single exploit against the PCS to achieve their

goals. This is something that, as a NIS regulated operator, Admin Corp will wish to take steps to prevent, in order to meet Cyber Assessment Framework objective B4.

Detecting attacks against the PCS
Instead of making holes in the firewall, the Adminox system designers and risk owners have agreed to create a mechanism by which read-only access to the PCS data is provided to the business network using known and trusted technologies. By deploying historian capabilities into the network, Admin Corp can collect the process data and make it available for analysis.

However, the primary historian will be deployed into the PCS environment, so for Admin Corp to maintain separation between the zones, they install a second replica of the historian in the Business zone. This replica system is sent data using securely configured database replication services from the PCS historian instance and then monitored carefully for compromise.

---

5. Reducing the impact of compromise

"If an attacker succeeds in gaining a foothold, they will then move to exploit your system. Make this as difficult as possible"

By using a zoned network approach and implementing effective monitoring, Admin Corp has made it much harder for an attacker who has gained access to the Business zone to traverse into the Process and Safety Zones.

However, they also need to take steps to reduce the impact of compromise in the case that an attacker is successful in compromising any one of the zones.

Only the essentials
The first step towards limiting the implications of compromise is to remove all unnecessary functionality from key boundary systems in the attacker's path. This will reduce the likelihood that an attacker can further their activity in the network.

Administration
The design principles tell us to "beware of creating a 'management bypass." With this in mind, Admin Corp will also take a careful look at how they manage the systems which control authentication for each of the zones.

The NCSC regularly sees operators choosing to use the same Active Directory for both the business and process networks, or rely on network or systems management functions that are carried out from the business network.

The result of this is that, typically, an attacker simply has to compromise Active Directory or management systems in the business network in order to have full control of the process network. This is an example of the "Management bypass" anti-pattern.

As Admin Corp have decided that the Process zone is a higher trust zone than the Business zone, they decide to have an entirely separate Active Directory within the Process zone, which has no trust relationships in place with the Business zone.

They also decide that all network and system administration within the Process zone must be conducted from a hardened systems enclave within the Process zone itself.

Allowing for a smooth recovery
Acknowledging that there is likely to be a compromise at some point, it is important to make it easy to recover following a compromise.

For Admin Corp, this means maintaining a set of offline "gold images" for systems which would allow administrators to quickly recover to a known-good state, in the case of a destructive attack.

It's important to note that it's not only an attacker with destructive intent who might do this, but far more commonly, ransomware, which could impact a system in this way.

For Admin Corp, the ladder logic and configuration of the process controllers is essential and so processes will be developed to regularly backup programs and configurations, storing them offline too.

Cost analysis
Having conducted their attack tree analysis and to reduce overall costs, Admin Corp choose to take a surgical approach, by backing up only the systems that would have an impact on operations.

Separation of duties

For some systems, it may also be appropriate to ensure that the design supports *'separation of duties'.*

In Admin Corp's case, the process of making changes to any systems within the Safety Zone are subject to strict separation of duties, not just to meet any regulatory requirements for safety, but also to reduce the impact of a cyber attack.

Proposed changes to the network design, or configuration, will be peer-reviewed and authorised by the Admin Corp Change Board, which is composed of individuals with functional safety, operations and security expertise. Final change execution will be implemented by a separate team of suitably experienced engineers.

Protecting documentation
Finally, the NCSC knows from it's experience of red-teaming CNI systems that an attacker who has access to up-to-date design documentation, P&ID and schematics is likely to achieve their objectives faster than one who doesn't.

So, Admin Corp must carefully consider how to protect key design documents. This is particularly important for those documents that would be critical to an attacker achieving the consequences which Admin Corp are particularly intent on preventing, such as documentation of the safety system. It is possible to do this by avoiding unnecessary caches of documents and limiting access to certain key design documents on a need to know basis.

Next steps

Having achieved these steps, Admin Corp believe they have appropriate risk mitigation in place as part of their system design to defend against both deliberate acts of cyber intrusion as well as incidental malware infections that might have an impact on the production process.

Their next steps are to ensure they have iterative improvement processes in place to initiate improvement actions from any events which threaten to impact Admin Corp's availability and safety requirements.

As an operator of Critical National Infrastructure, Admin Corp ensure they continue to manage the Adminox process safely and effectively by joining the NCSC's CISP

platform and maintaining a relationship with the NCSC Private Sector CNI Engagement Team.