Cyber Security Management of Industrial Automation and Control Systems (IACS)

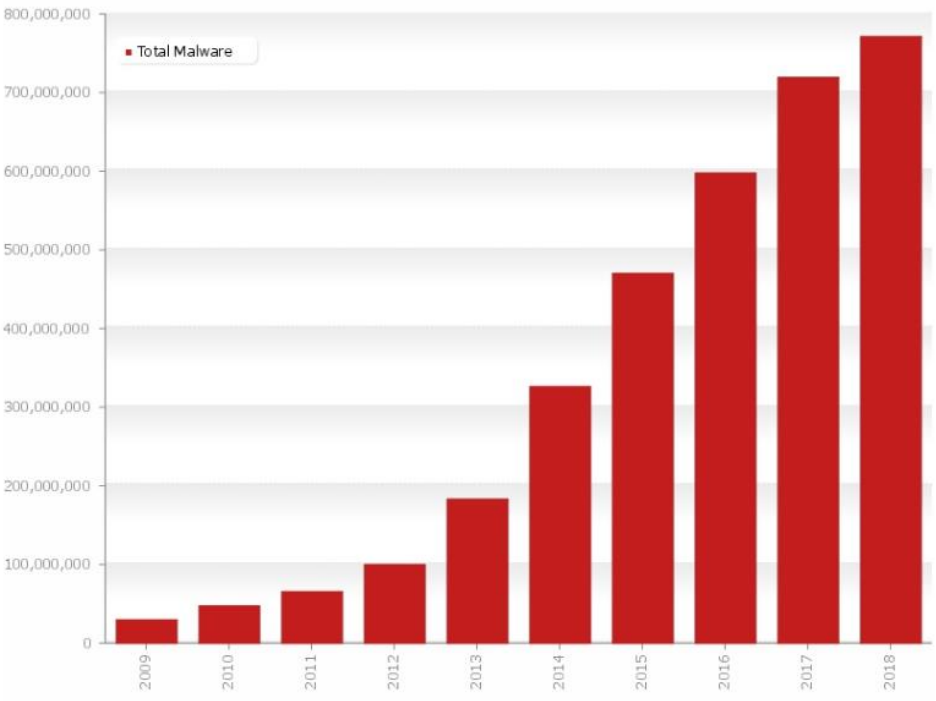
Cyber Security Management of IACS

The IACS (Industrial Automation and Control Systems) is defined as a collection of networks, control systems, SCADA systems and other systems deemed to be vulnerable to cyber-attack.

All computer based systems are vulnerable to attack and with the increase of interconnectivity and complexity of these systems the amount and sophistication of attacks has also increased.

Prominent attacks have included; the theft of the NSA hacking tools and subsequent release on WikiLeaks with the codename of "Vault7" in 2017, the breach of UBER's data security in 2016 that affected over 50 million customers, and Ransomware attacks such as *Petya* and *Wannacry* that held thousands of companies data to ransom in 2016 and 2017.

Malware (malicious software) is on the increase. It has been reported that there are currently 250,000 Malware threats created every day.



source: AV-Test.org MAY 2018

As can be seen by the graph above, the amount of Malware has increased exponentially over the last ten years. Concerning as this is, tools for countering these threats have also become more advanced and software such as NORSE can even track attacks in real time.

As cyber security tools advance to meet new threats, and virus checkers update their databases, more threats are created and new viruses are unleashed in a seemingly endless arms race.

What are the Threats to Operational Technology?

Operation Technology, or “OT”, can be defined as systems designed for the controlling and monitoring of physical devices in real-time.

OT systems are vulnerable to all forms of cyber security threat, but the most recent and dramatic have been Ransomware attacks.

The nature of most Ransomware is to spread as wide a net as possible and attack companies and organisations indiscriminately. They are also the most common, accounting for 60% of all cyber-attacks.

In the event of an attack, a company that opts to pay the ransom has statistically only a 50% chance of getting their data back, making it very likely that once the attack is underway it is already too late to do anything about it.

Historically, malware has also been used to target specific locations for specific nefarious purposes, such as the Ukrainian power grid, an Iranian nuclear plant (*Stuxnet*), and a German steel mill.

Whether targeted or indiscriminate, the frequency of attacks is increasing. It has increased by 82% in 2017 in the energy sector alone.

How to protect Operational Technology

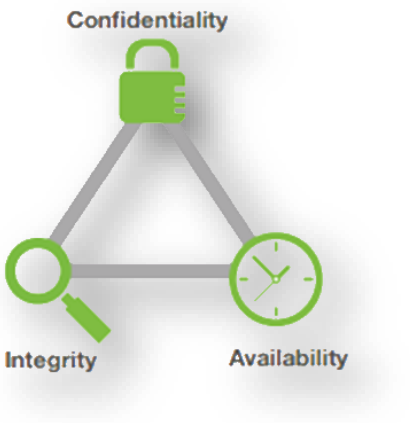
To counter the threats to Operational Technology, institutions such as the International Electro-technical Commission (**IEC**) have created compliance standards such as **IEC 62443**, **IEC 61511** and HSE OG 0086.

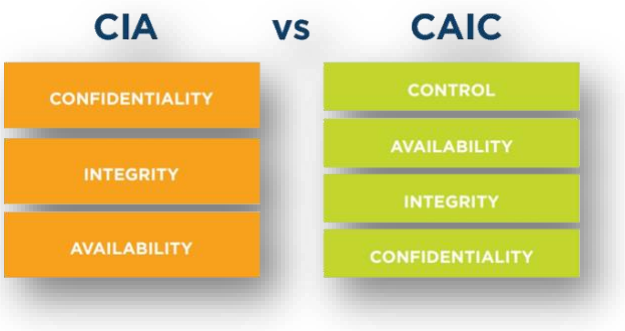
These standards help define and understand the creation of a Cyber Security Management System (**CSMS**), the difference between Information Technology (**IT**) and Operation Technology (**OT**), and how to prevent or lessen the risk of cyber-attacks by planning, implementing procedures and creating polices and processes.

The difference between IT and OT

Information Technology's priority is information. Processing it, communicating it and securing it from unwanted access and interference.

This can be defined as the “CIA Triad”. Each side of the triad triangle is one of the three important factors - Confidentiality, Integrity and Availability.





Operational Technology's priority is Operational Availability. After that the next most important factors are Integrity and Confidentiality.

The “CIA vs CAIC” model also adds Control as top priority to the CAIC stack and Safety is considered to be an integral part of Control

OT Challenges

Operational Technology has a unique set of limitations, risks and challenges.

Obsolescence is a key issue, as all old equipment was designed before modern threats were understood and many are running on old operating systems that have multiple vulnerabilities and no current patches.

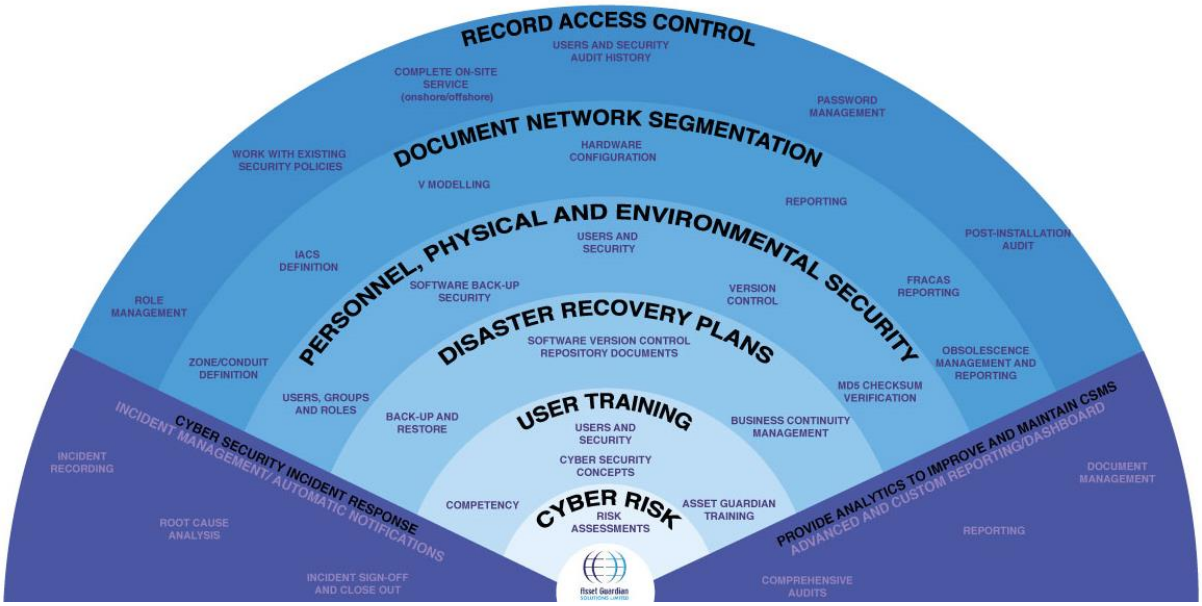
Patches may not be available, or may be unsuitable for the current operational requirements of the equipment in use. Testing and approving patches for operation can be a slow process.

Also, Virus Scanners, a vital component of cyber security in IT cannot always be used in an OT environment where its use may interfere with operations and reduce system availability.

Cyber Security Management System

With an understanding of what the threats are to the IACS, the information and tools available to counter these threats and a clear understanding of the challenges that are faced, a system of management can be implemented for cyber security.

Adherence to the IEC-62443 standard requires the creation and use of a CSMS (Cyber Security Management System). The CSMS should be designed in such a way as to protect the entire IACS.



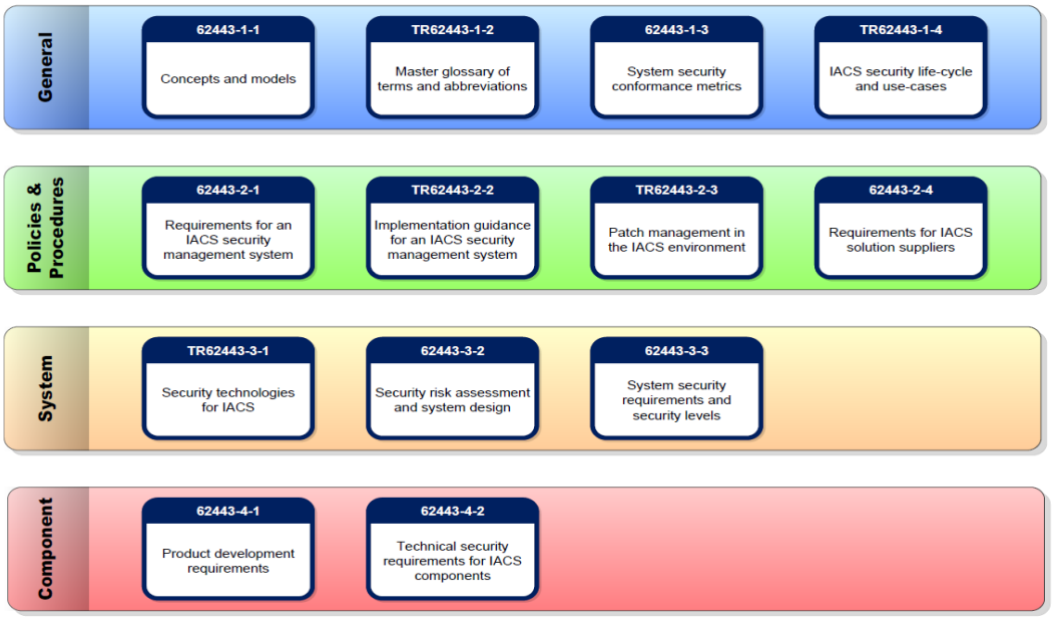
The CSMS forms the core of an overall cyber security plan. It should be used to identify and assess risk, plan user training, as part of disaster recovery plans and for incident reporting, response and recording.

As the diagram above shows, the management systems consists of many elements, element groups and categories, organised in such a way as to structure and manage all cyber security activities in accordance with a company's specific culture and needs.

IEC 62443

ISA/IEC-62443 (formerly ISA-99) is the standard applied specifically to the Controls and Automation industry. It comprises standards, reports and procedures pertaining to cyber security in an *IACS* (Industrial Automation and Control Systems).

The guidance presented in the standard is targeted at everyone involved in the application of the CSMS on the IACS. The standard applies from the first stages of design and implementation through to the integration of the systems, and day-to-day use, management and maintenance.



Source: IEC-62443

What Can I Do?

You may now be wondering, knowing about the CSMS and how it relates to IEC-62443, what can I do to make my facility cyber secure?

Remember that everything cannot be done at once, but at the same time you cannot simply work through the systems one at a time in an arbitrary manner. Actions to be taken must first be analysed and prioritised. This is done through the risk assessment processes which aims to identify the vulnerability of each system and the consequences if that system comes under attack.

Once the risk assessments are complete, ensure that all the systems are stable, secure the highest risk systems first and then continue on, working through the priorities established in the risk assessments.

How Do I Do It?

Asset Guardian employs a phased approach, geared towards compliance with IEC-62443 and the creation of a CSMS. The completion of each phase feeds its findings and resolutions into the next until the process is complete. The CSMS, once in use, is then continually reviewed and if need be, revised, in compliance with this phased approach.

Audit and Assess

Audit:

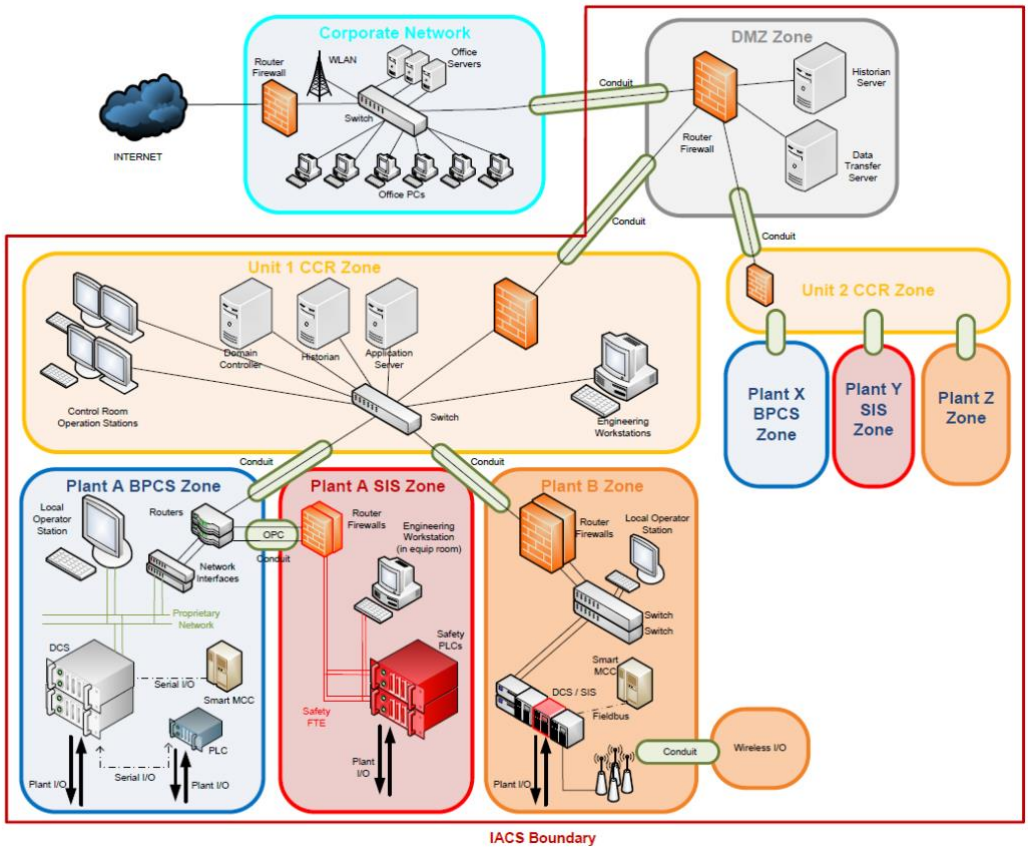
Plan all activities, identify all systems that form the IACS area.

Create polices, processes and procedures to carry out the planned activities.

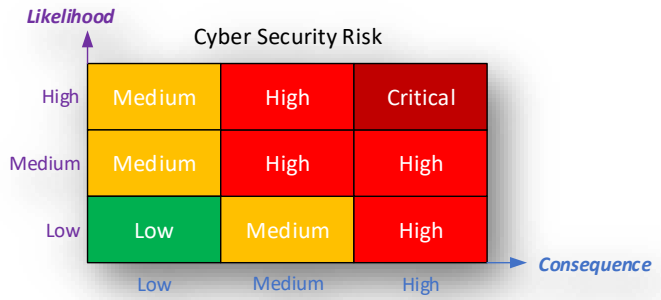
Generate a Simple Network Diagram that defines Zones (including separate Safety Instrumented Systems (SIS) zones), Conduits and general layout, and shows the protections that have been put in place.

Compile an Asset Register that links Assets to Zones. Assess the risks to all systems and prioritise the actions to be taken.

An example Simple Network Diagram is shown below:



In this diagram DMZ means “De-militarised Zone”, CCR means “Central Control Room”, BPCS means “Basic Process Control System”, SIS means Safety Instrumented Systems and PLC means “Programmable Logic Controller”



Assess:

All equipment to be identified and recorded.

Identify installed software, firmware, operating systems and all other systems vulnerable to attack. Identify which zone or zones they inhabit and what endpoint protections are currently in place.

If there is a current risk assessment system, review how it may be integrated into the incoming CSMS as it is developed.

Risk Assessments are the process by which negative events are identified, analysed and judged. Assess cyber security risk from the risk matrix defined in IEC-62443 and use the results to prioritise actions.

During the Risk Assessment process, overall and also on a system by system basis, consideration should be given to the likelihood of cyber incident and the consequences of the cyber incident (CAIC).

Stabilise and Secure

Consider countermeasures against the identified risks. Look at the Zones that need to be stabilised first.

Consider all factors and recommended solutions that target the identified risks. For instance, perimeter security might be addressed by network isolation and remote access managed by a secure authorisation scheme. Even physical security, swipe cards and keypads may be used to secure access to specific sites and zones.

Then look at the asset register that was generated in the first phase to begin the process of fully securing the IACS area. Consider endpoint protection, whitelisting, the issues around patching, how best to manage authentication and authorisation, awareness training, the movement of assets between zones and all other factors identified earlier on in the process.

Attack Vectors

Each form of cyber-attack has an associated counter measure and these should be considered during the CSMS process.

Attack vectors include: Malware (software similar to viruses that may interfere or slow down running software), SQL injection (attempting to harm a database by hiding code in the data), Cross Site Scripting (injecting client-side scripts into web pages), Distributed Denial of Service attacks (flooding systems with bandwidth slowing requests), Man in the middle attacks (intercepting secure communication), Phishing, Pretexting and Credential reuse (all forms of social engineering attack).

The number one attack vector has always been the human element.

Human Component

The human component in any security system is handled by a process of authorisation and authentication, i.e. only certain people have access to certain sites or zones and their identity is confirmed on all attempts to gain access.

Awareness training also helps to reduce the human elements of cyber security and while the industry standards cover this in depth, the training at a minimum should cover the types of threat, and the processes and procedures that are in place. This training should be made available to everyone with access to the IACS, including staff, contractors, vendors and everyone with remote access.

Manage and Maintain

A CSMS is of no use unless it is kept up to date. A system of Change Management is required to monitor changes to the IACS and the asset register should represent as closely as possible the current systems.

Obsolescence Management is a key issue in all systems and should interface with the Asset Register in monitoring the lifespan of all equipment. Cyber Risks feed into Obsolescence Management when considering strategies for upgrades, patching and replacements.

The ongoing process of Patch Management should also be controlled by the CSMS, so that tests, roll outs and issues can be managed and recorded in the Asset Register.

Incidents of cyber-attack should also be tracked and managed as part of the CSMS. Considerations such as e-mail notification, resolution tracking and lessons learned should be taken into account, with a focus on the prevention of attack reoccurrence.

Disaster Resilience

Disaster Resilience can be considered the most important function of a CSMS. No system can be 100% secure and one of the reasons why is that the human component can never be removed.

A measure of Disaster Resilience is how quickly and completely a system can recover from disaster. Disaster Recovery is a subset of an overall Business Continuity Plan. Primarily it is the management of data such that it is recoverable in the event of a disaster.

Disaster Recovery plans and procedures that form part of the overall CSMS should be in place in the event of system or data loss. Full configuration information should be maintained, as well as secure and isolated backups of all software and firmware. Proper security control and authorisations should be in place to aid in speedy disaster recovery.

Safe Secure Backups

Software and firmware backups should be maintained outside of the network zone that the live software resides, to prevent cross infection. Proper change control should be managed by a planned process, backups should be as up to date as possible and maintained under full version control.

Software backups are only useful if they are still valid when they are required, so file integrity checking should be a regular activity to ensure that backups can still be restored. File checksums can be used for this and backups should always be protected from viruses and ransomware. Access to the backups should only be available to authorised users.

Review and Revise

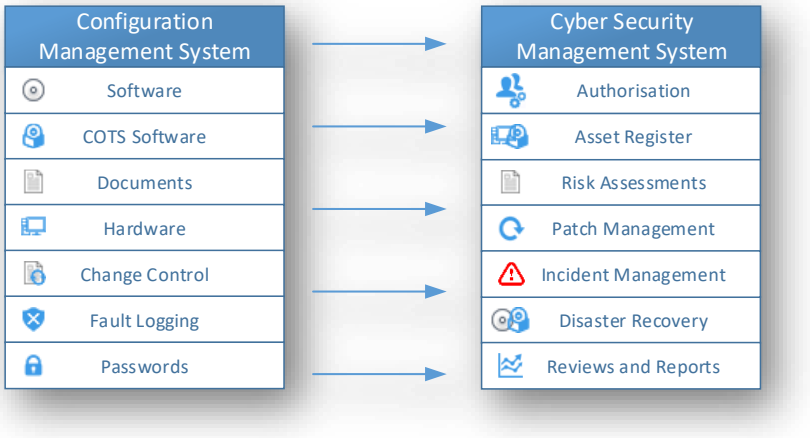
The final phase requires that, as well as managing and maintaining the IACS through the CSMS, the CSMS must itself be monitored for effectiveness. Changes to the CSMS should be carried out in a well-managed and regulated manner.

Processes and procedures should be regularly reviewed and updated when required. The CSMS should also be kept up to date in regards to new and emerging technologies and the ever expanding and evolving variety of cyber-threats.

The need for refresher training for the users of the CSMS should be regularly reviewed and new training developed and offered to users if required.

Integrated Solution

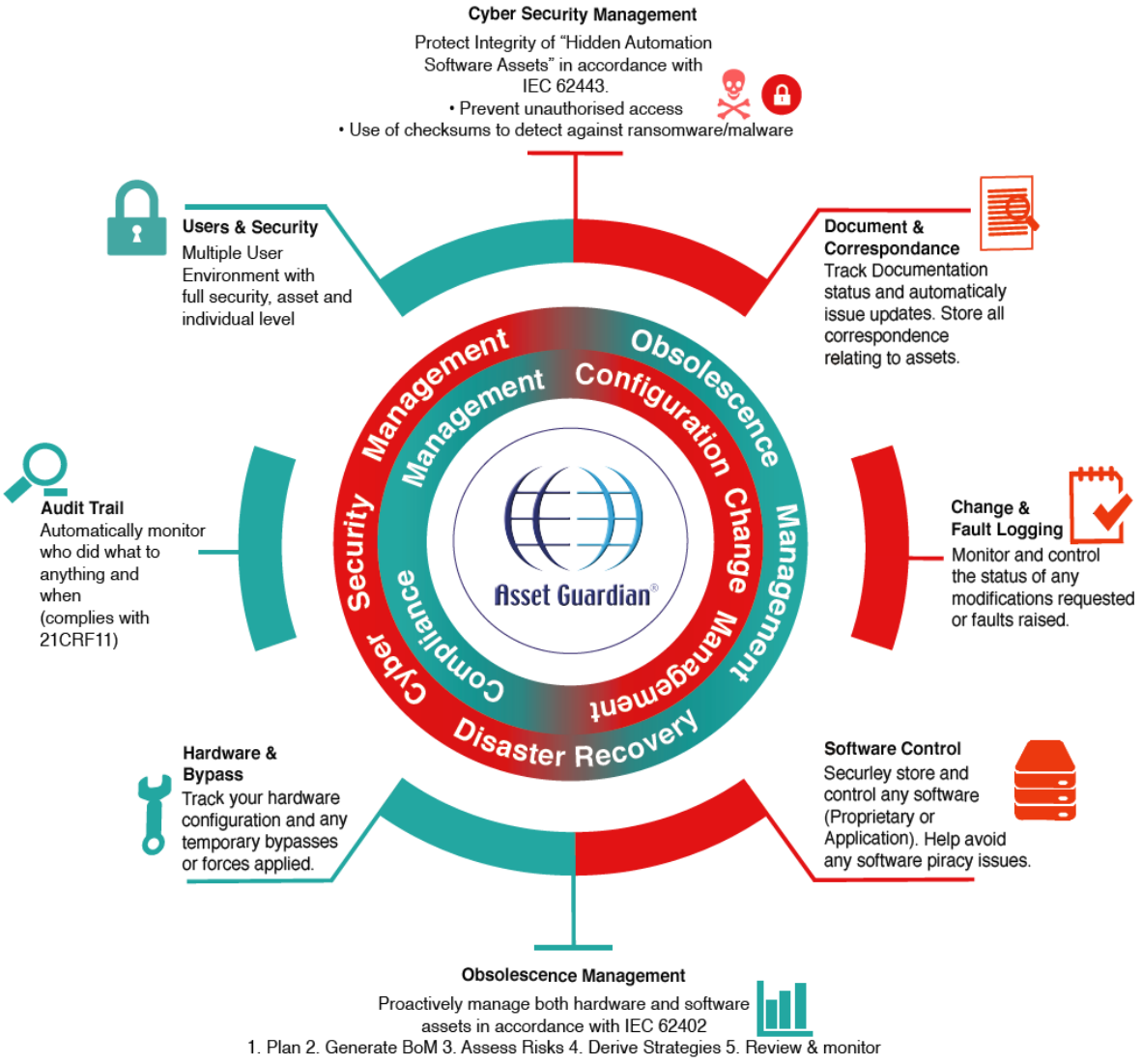
The four phases of designing, implementing, managing and reviewing the CSMS can be integrated into an existing Configuration Management System (CMS). Elements of an overall CMS may be mapped onto functions that are required as part of the CSMS as show below:



Asset Guardian

Asset Guardian offers all the features of a Configuration, Compliance and Obsolescence Management System, but also sections specifically designed for Cyber Security Management.

The diagram below shows how Asset Guardian has been designed to meet the cyber-security requirements as defined in the IEC-62443 standard.



Conclusions

Cyber threats to the IACS are on the increase leading to the requirement for increasingly sophisticated counter-measures. The challenges of protecting the IACS are different from those of more standard IT network architectures, but there are standards tailored towards the need for cyber-security in an OT environment.

These standards require that an IACS is protected by a set of principles, processes, procedures and tools collectively known as a CSMS.

Implementing, managing and using a CSMS may be done in four phases; Audit & Assess, Stabilise & Secure, Manage & Maintain, and Review & Revise.

Cyber-attacks come in many forms, and while recent ransomware attacks have been more newsworthy and spectacular, more common and insidious forms of attack such as phishing and pretexting are just as dangerous. These can be countered through rigorous authorisation and authentication systems and through user awareness training.

Another key defence against cyber-attack is the use of a Disaster Resilience and Recovery plan, and a key part of the recovery plan is to ensure that verified backups are stored regularly in a secure location isolated from the live system.

The use of an integrated solution is recommended for organisations that face cyber security threats as these threats rarely occur in isolation. A solution that also records and tracks all other aspects of the IACS, such as configuration and obsolescence management will ensure not only compliance to industry standards, but aid in disaster recovery, user management, auditing and many other activities associated with the countering of cyber-security threats.