INDUSTRIAL CONTROL SYSTEMS
Community of Interest

Managing Industrial Control System / Operational Technology information and data securely

Introduction

NCSC has generalised guidance on protecting data/information that is held digitally - this guidance covers both data/information in transit, at rest and exporting data to other systems, while this article is part of a series of Industrial Control System (ICS)/Operational Technology (OT) specific guidance articles, this one looks at anti-patterns relating to managing data and information noted in ICS/OT environments, and how to address them.

Important Note: *While the ICS COI is supported by the NCSC, and NCSC staff are involved in a range of its activities, no formal review of this guidance article has been undertaken by the NCSC. The ICS COI and its members strive to produce relevant ICS/OT specific cyber security guidance to supplement principle based cyber security guidance published by NCSC and have taken care to reference this guidance where applicable. This guidance article will be reviewed every 18 months to ensure that it has not been superseded by guidance published by NCSC, relevance and that any references are still accurate. The ICS COI and its activities are purely voluntary, with guidance articles produced that are deemed needed by UK Operators and their supportive industry partners. The fact that this guidance article has been published by the ICS COI has no relevance to the priority and focus of guidance published by NCSC*

This guidance is written for those responsible for securing ICS/OT environments, and the data/information held that relates to the assets within them. Primarily this is for UK Critical National Infrastructure (CNI) operators, but this guidance can be used by all organisations running ICS/OT environments, in addition to suppliers, system integrators and managed service providers supporting ICS/OT environments.

ICS/OT related information can be held digitally in a plethora of forms such as:

- human readable documents,
- spreadsheets,
- schema-compliant data files,
- heavily structured, relationship-rich datasets,
- various database or file types.

NCSC defines that there are four main groupings of ICS/OT data:

- **Design data -** defines the architecture, specifications and/or functionality of an ICS/OT system. Examples include network diagrams, asset/data inventories, configuration files and process flow diagrams.
- **Access data -** encompasses information that is essential for the authentication and authorization of users and systems within the ICS/OT environment. This includes user credentials, details of personnel, encryption keys, access control lists and access logs.
- **Operational data -** refers to the information involved in the real-time control of an ICS/OT system. This includes the unrefined data generated by ICS/OT devices/software, as well as the information ingested. Examples include sensor readings, system logs and alerts. Operational data also captures historical and predicted reporting on component and/or system performance.
- **Risk and safety relevant data** - encapsulates information on weaknesses in the system design, its components and the potential consequences of risks if they were to occur (including safety impacts). Examples include HAZOP assessments and CVE databases.

A long-term trend is the desire to enable this data/information to be used productively within and between organisations and ICS/OT operators. The challenge is to do this without undermining the security of the operators/organisation and ICS/OT environments that seek the benefits of increased connectivity and data/information exchange.

Large data breaches can be financially and reputationally damaging to any organisation but there are additional risks posed by data/information loss for those owning and operating ICS/OT systems (including CNI systems). These risks include the impacts resulting from any subsequent operational outage or disruption (this can include operational and public safety consequences) and given the slow-changing nature of the physical assets that collectively form the ICS/OT environments (including the huge costs involved in making changes), any data/information exposed around the ICS/OT environment is likely to have applicability over a longer time scale than is normally observed within IT systems.

Additional considerations within ICS/OT environments where the safety of a system may be a key consideration that security treatments should not conflict with or where there can be immediate threats to the operation of hazardous or critical ICS/OT systems if their data/information systems are interfered with. Moreover, the data/information that requires protection in integrated information environments can be a mix of design data, implementation data and performance data

that can contain near-real-time performance data, the location of critical physical assets, their operational status and details of personnel.

Within ICS/OT environments there is heavy reliance on a wide range of data/information types, represented in a range of both legacy and more modern formats, with the imperative to ensure that engineering, operation and maintenance activities are biased towards system availability. Poor information management can inhibit operational effectiveness and information security simultaneously.

Anti Patterns

Working across several CNI sectors including transport and energy, examples of “bad practices” or “anti-patterns” have been identified. The concept of a ‘bad practice’ or ‘anti-pattern’ refers to a barrier to achieving a secure outcome. Although the NCSC no longer promotes the anti-pattern approach to guidance, it defined that an anti-pattern represents any repeated (but ineffective) solution to a common problem. This has been expanded in this guidance to include poor practices that are applied which negatively impact the cyber security posture for an organisation. The ICS COI uses this approach as it is still a useful tool for framing this space in ICS/OT environments.

Anti-patterns are ineffective implementations that should be avoided, especially in operational settings. This guidance summarises these to elaborate on the existing anti-pattern advice offered by NCSC to provide further guidance relevant to ICS/OT environments.

Seven anti-patterns are described in this document are those that are commonly seen and especially harmful within ICS/OT environments (however, they may also apply to traditional enterprise IT environments):

1. **Staff and contractor low awareness of the consequences of poor information sharing**
2. **Poorly controlled sharing of design and configuration documents**
3. **Openly accessible links to files and documents**
4. **Poor use of document and file management system security features**
5. **Assumptions that adopting database systems provides increased security.**
6. **No records of what documents and files are, or were, shared.**
7. **New-tech adoption without addressing the management of information hosted within or processed by it.**

This guidance assists and supports Cyber Security professionals working within ICS/OT environments to identify indicators of anti-patterns and potential weaknesses. It focuses on the technical aspects and appropriate compensating controls to promote good cyber hygiene processes.

Anti-pattern 1 - Staff and contractor low-awareness of the consequences of poor information sharing

Individuals working within and for organisations with ICS/OT environments, are generally unaware that the ICS/OT environment related data/information that they are creating, using or sharing has any bearing on the commercial or operational security of systems that they are involved with. This can mean that the most 'convenient' approach is often taken to get the job done with little awareness of any possible consequences. Engineering activities, for example, can only succeed if there is sufficient sharing of information but doing this inappropriately can have consequences.

Examples of getting this wrong can include:

- Knowingly sharing specific ICS/OT related documents (e.g. design schematics, configuration information, CAD files, scans of designs, etc) to parties that are only partially trusted or are unaware of any trust expectations on them.
- A culture that views security measures as an encumbrance or something to avoid.
- Over-sharing ICS/OT related data with a supplier and relying on them to find what they need to modify a design, change the configuration of something they are working on or make a delivery.
- Assuming that suppliers will know what is needed because they 'already have a lot of our data'.
- Relying on those working on ICS/OT related projects, supply activities or support to work out for themselves what the security implications are of sharing and using data.

How to identify this anti-pattern - Speak to employees and suppliers to find out what their attitudes are towards the use of information in their activities. Attitudes towards security are often easy to discover and can be a revelation to those in organisations who ought to know better. If individuals think it is someone else's job to take care of information security so that they don't have to then there is a sign that information may not be as secure as the organisation would like to believe. Technical security measures and corporate policies only go so far.

A better approach - Ensure that information security risk management is a board-level responsibility, with effective governance in place, clear messaging throughout the organisation and an effective approach to continual improvement of information security practices. For roles that are likely to result in access to significant documents or information systems within or relating to the ICS/OT environment, ensure that there is good management and make use of training, vetting and monitoring to minimise risks. Raise awareness of the need for improved approaches to sharing ICS/OT environment related data internally and with suppliers. Effective ongoing management is needed as information security issues can hit even those organisations that think they are 'good'.

Key reference sources:

- NPSA - Passport to Good Security
- NPSA - Security-Minded approach to Information Management

- NPSA - Security-Minded approach to Digital Engineering
- NCSC - CAF Principle A Management Governance

Anti Pattern 2 - Poorly controlled sharing of design and configuration documents

Frequent emailing of large files or any organisationally sensitive information relating to ICS/OT environments goes unnoticed. If the company email limits prevent the sending of large amounts of information, individuals resort to their own preferred methods perhaps by using 'free' online file sharing utilities or video / collaboration applications that support document uploads within the channel. If an ICS/OT environment related supplier or partner organisation states that they need information, then there is a willingness to supply it without checking what the purpose is or what the expectation is around how it should be treated.

If challenged, each instance of corner cutting like this is excused as being of little significance "given the size of the organisation or system". However, a cautionary maxim like this should illustrate the risk: Loss of a little data can be the loss of a lot of information.

Improper use of some internal document and other file sharing systems can result in a scattering of multiple copies of ICS/OT environment related documents across many locations (both within the ICS/OT environment and externally in the likes of the corporate IT environment), despite them being held securely in a cloud-based document management or file server solution. If the controls for managing versions and security controls are too complex, then out-of-system methods can become commonplace such as saving files locally or resorting to the techniques above even for sharing documents internally.

How to identify this anti-pattern - little use of identity management and role-based access control methods within ICS/OT environments, the corporate IT environment, and between organisations. Direct access to corporate file servers by many employees, relying on desktop applications and/or file naming conventions to implement configuration and version measures. The number of large emails, and the type of attachments, may be an indicator of this (both internally and externally). Employees may be willing to state that this is commonplace and may also usefully explain why alternative approaches are not suitable (they may not be, a sign that there is room for improvement).

A better approach - Recognise the need for sharing data but implement measures to allow it to happen in an appropriate manner (see the recommendations in the following sections). If poor practices are endemic, communicate clearly what good practices are and, perhaps, consider technical measures to limit the use of inappropriate methods of sharing information. Implement defensive measures such as limits on file sizes that can be emailed and deny the use of some file types (e.g. compressed files). Organisations sharing electronic documents should consider converting them to a safer, different, file format (e.g. converting shared documents to PDF by an agreed process). Where document management systems or other file server applications are used consider additional risks that they may include alongside the benefits. In situations where trust is lower or the need for document access is intermittent consider using document viewers served by the client to supplier browser-sessions, enforcing restrictions on the ability to copy and save material locally.

Key reference sources:

- NPSA - Document release guidance
- NPSA - Publishing documents without compromising information security
- NCSC - Design Pattern: Safely Exporting Data

Anti Pattern 3 - Openly accessible links to files and documents

Online methods to share large numbers of documents and large volumes of data have proliferated, offering a lot of choice. This can range from 'free' services that individuals can sign up to with little awareness of their employer to online services that organisations can trial or subscribe to. One weakness that can go unnoticed is the convenience provided by the sharing of links (e.g. URLs), links that can be accessed by anyone with access to the link. This can enable significant amounts of ICS/OT environment data being exchanged unofficially. This can be compounded by those uploading the ICS/OT environment data not removing it from the service when the intended transfer has happened. This can result in the link being shared with, or obtained by, other parties at a later date with no visibility to the corporation. There are examples of material released publicly by well-intended organisations that contain embedded links to such openly accessible private data stores. The simple act of copying graphics, tables or text into documents for wider distribution can inadvertently leak sensitive information that can remain hidden in the document until found by a search engine and/or a potentially hostile actor. Short-cuts to get the job done can cost in the long run.

How to identify this anti-pattern - Lack of corporate processes and tools to enable document and file sharing to happen in a suitable manner. Where there are organisational activities that rely on significant exchange of documents then questions should be asked of the methods being used to achieve this. Other indicators may be connections to online services commonly used for file sharing (that aren't corporately approved) and no document release process that includes an information risk check.

A better approach - Ensure that there are effective document and file sharing methods provided for that fit with the organisations information security risk management policies. Consider polices that limit (or prevent) the use of unapproved file sharing methods. If sharing of documents with suppliers is required, then ensure that suitable measures of protecting the documents are clearly stated and agreed contractually. If documents are being prepared for wider distribution about projects that are commercially or nationally sensitive, ensure that there is a process to check the information risk prior to release.

Key references sources:

- NPSA - Document release guidance

Anti Pattern 4 - Poor use of document and file management system security features

A range of increasingly capable document and file management services have become available. Many of these are also architected around cloud provisioning and this can provide its own security benefits. In fact, NCSC recommend the use of cloud services to enable organisations to focus on the security of the data. Unfortunately, this can be easily overlooked. Organisations can find it hard to keep track of the policies and user activities relating to services that they are responsible for and can be unaware of access that their employees and suppliers have to other systems. Examples of this include Common Data Environment (CDE) required for use in large built asset systems during their design, build and, increasingly, operational lifecycle phases. On even modest projects there can be hundreds of users from tens of organisations. Other large document management systems can be built upon well-known cloud storage platforms with a rich array of sharing options and policy controls (including role-based access controls). Again, these are often overlooked with user access being increased over time and little monitoring of who is accessing what data, and why.

This can lead to a race to the bottom, with too many users being given persistent access to too much.

How to identify this anti-pattern - False confidence in adoption of online file sharing services that have the features to allow effective user access control and monitoring. Little evidence of good access controls being applied to users and infrequent (or zero) review of users' need to access the data. If logging and monitoring is available, little evidence of it being used to inform decisions about how effective any of the controls are and what the risk landscape looks like.

This is a management activity and is about getting it right. Over-zealous application can also backfire, with legitimate users being prevented access to data or organisations losing contact with data held within their own systems due to nobody suitable having permission to access it.

A better approach - The organisation has a mature approach to information management including a clear policy for identity and access management (including policy for allowing employees access to other parties' systems). Role based access is employed where organisational risk management requires it (ideally on all corporate systems), and it is reviewed as a matter of routine by those responsible for granting access.

Key reference sources:

- NPSA - COMMON DATA ENVIRONMENTS A guide for BIM Level 2
- NPSA - Introduction to PAS 1192-5:2015 A specification for security-minded building information modelling, digital built environments and smart asset management
- UK BIM Framework - Guidance Part C Facilitating the common data environment (workflow and technical solutions)
- NCSC - CAF principle B2 - Identity and Access Control

- Google - Share drives overview
- Microsoft - Policy recommendations for securing SharePoint sites and files

Anti Pattern 5 - Assumptions that adopting database systems provides increased security.

ICS/OT environments can require very large numbers of detailed design and other engineering and operational documents. Managing large numbers of ICS/OT environment related documents and other files can be eased by using centralised document management systems, based around scalable object stores and can employ labelling schemes. Users can become familiar with the folder structure, file naming convention and labels, with the ability to use search features to discover documents they need. However, an aggregated collection of valuable ICS/OT environment related documents can present opportunity to attackers. In the first instance, obtaining documents of interest can be far easier if they are available from one location – if access can be obtained. The assumption of increased security can result in legitimate users storing, and even sharing, unusually sensitive material without assessing the risk. Examples include sensitive intellectual property, proprietary designs, ICS/OT configuration information and even passwords. Secondly, poor cyber security measures including inadequate backup methods can leave such document stores open to ransomware attacks.

How to identify this anti-pattern - Use of centralised document and other file storage applications that are lacking mature security risk mitigation measures is a clear sign of this antipattern. Even if good identity management, role-based access and storage, potentially even file-based, encryption is used risks can remain such as that posed by ransomware.

A better approach - Adopting a cross-cutting information security risk management approach throughout the lifecycle of the systems to which the electronic documents and files are needed can identify these issues in time to mitigate them.

Key reference sources:

- NCSC - Supply chain security guidance - Third party data stores

Anti Pattern 6 – No records of what documents and files are, or were, shared.

As the range of methods to enable file sharing has increased, so has the challenge of being able to keep track of what ICS/OT environment related data/information have been accessed or shared, and by/with whom. Although the range of technical measures that could be applied too this challenge have also increased the challenge is hard to address by them alone. Many organisations don't know where their documents and other files are stored, relying on employees' knowledge and best-endeavours to store, find and use the documents they and their colleagues require. Any inventory of physical and electronic assets is piecemeal, out of date and not evaluated periodically. Any records of access to, copying or sharing of documents are of poor quality and are never used to evaluate poor practices or detect non-compliant activities.

If you don't know what happened to your data, you will find it hard to justify that you have taken sufficient care of it.

How to identify this anti-pattern - It can be straightforward to identify the two most common elements of this anti-pattern. Firstly, has the organisation identified their requirement to have records of access to and sharing of documents and files, and ensured that these requirements are met? If not, there is a weak basis for any records collection. Secondly, were there are records collected, are they used to identify potentially unauthorised or risky information management practices? If either of these are not done there is an immature approach to monitoring that should be addressed.

A better approach - Corporate document management information requirements, including records management requirements, are identified and documented in advance of implementing (or upgrading) document management systems. The creation of records is done to meet the lifecycle management processes of corporate documents, with the records being used to inform compliance monitoring and other risk management activities (including supply-chain and insider-threat risk management). A mature organisation will be able to know, from its records, what information was accessed or shared and with whom throughout the lifecycle of those documents.

Key references sources:

- NCSC - CAF Principle A Management Governance
- NCSC - CAF Principle A3 Asset Management
- NCSC - CAF Principle B3 Data security
- NCSC - CAF Principle C1 Security Monitoring

Anti Pattern 7 - New-tech adoption without addressing the management of information hosted within or processed by it.

The growth of services offering off-premises hosting of business-critical, or support, functions based on consuming or storing the client's data can result in organisations not being sufficiently aware of what is happening to their data. For ICS/OT environments, this can include Industrial Internet of Things (IIoT) monitoring, operational data analytics, process optimisation and can involve streaming or file-based transfers to systems that the client doesn't own. Some services may involve machine learning, adding further complexity for the client to take stock of. The client can be unaware of the security implications of different service offerings and, for example, may select a service based on the lowest cost of competing solutions that appear to offer the same functionality. Moreover, many services can look attractive, but the small print will typically make it clear to the client that it is the client's responsibility to manage their own data within the system. Key aspects such as data quality, information lifecycle management and managing within a wider enterprise are left to the client. While this is understandable from a responsibility and accountability perspective, as the supplier can't reasonably take them on, it is too easy for clients to assume that risks that they should be actively addressing have been lowered by outsourcing services. This can be compounded if the client has little experience and awareness of the technologies being offered resulting in loss of corporate oversight of it.

How to identify this anti-pattern - An enthusiasm for Digital Transformation without considering information security when pursuing and adopting new solutions. Outsourcing of ICS/OT environment related data-based services that have traditionally been done internally without objectively assessing the security and resilience risks is a sign that there may be future security issues that have yet to be identified.

A better approach - Identify sources of unfamiliar or new security risks early and flag them to the business. Ensure that expert advice is sought that enables the benefits of adopting new technology-enabled services while also mitigating security risks. Trialling of a new service to assess its performance, including corporate information resilience and security risks, could be a good way of learning prior to adoption.

Key reference sources:

- NCSC - Cloud Security Principles

Summary

Managing the security of ICS/OT environment related electronic files and the security of the systems, processes and organisations that depend upon it is a lifecycle activity that, for infrastructure assets and systems, can extend to decades or more. Once lost, ICS/OT environment related data/information in documents and files can remain valuable to adversaries for as long as it is representative of the systems that it relates to. Good information security requires a mature, risk managed approach that recognises the need to share information with those who need it while preventing access to those who shouldn't get hold of it. Documents and other files are no exception. Information security risk management should start as early in the lifecycle activity of the infrastructure asset system (or project) and be maintained throughout.

This guidance has outlined that dealing with Information Security Management for documents and files as part of an integrated approach to Information Management. The outcome of doing so is a more cost-effective result that is compatible with an increasingly connected and integrated information environment that data-dependent sectors now demand; one that can preserve security where needed while enabling information exchange in a suitably controlled and managed manner.

Statement of Support

This guidance has been produced with support from members of the Industrial Control System Community of Interest (ICS-COI) for publication via the Research Institute for Trustworthy Inter-connected Cyber-Physical Systems (RITICS). This guidance is not intended to replace formal NCSC guidance where already available, and care has been taken to reference such existing guidance where applicable.

Document Details

This document is version 1.0 and was published on 23/09/2025. It will be reviewed every 18 months.