SECURE COMMUNICATIONS AND INFORMATION SYSTEMS

TRAP

Thales Risk Assessment Process
Executive Summary

Cyber security incidents and attacks can damage organisations' profits, reputation, competitive position and even its operational ability, yet many companies remain unaware of the risks such events pose to their organisations.

Within Industrial Automation and Control Systems (IACS), standard IT technologies, such as TCP/IP, Microsoft Windows and Web browsers are becoming more widely used. These standard IT technologies are replacing conventional proprietary technologies and enabling bespoke process control systems to be replaced with COTS products. Modern SCADA systems are becoming increasingly complex, digital and connected. The security of these systems represents a significant challenge within today’s industrial and service infrastructures.

With the increase in complexity and connectivity there is a potential for increased risk exposure. Therefore, within these environments, it is essential that organisations understand the risks that their systems are exposed to, and take action to mitigate the risks which their environments now face.

However, many of the national and international standards which offer guidance on industry best practice on cyber-security focus primarily on IT environments and are not ideally suited to implementation within OT infrastructures.

There are many different tools available to help organisations undertake cyber risk assessments on their systems, but none are completely suited to being used in a commercial IACS environment.

To provide a flexible yet objective approach, Thales has developed TRAP – the Thales Risk Assessment Process. It is a standards based, asset focused risk assessment process for Business Systems and Industrial Automation and Control systems.

It is not a subjective process; this means it can be repeated by different analysts and give exactly the same result. In addition, the process is designed to be tailored for different standards (IEC62443, ISO27000, GDPR) to fit the customer’s domain (Government, Energy, Oil, Nuclear, Commercial, etc).

It recognises that not all assets have the same business impact value to an organisation if compromised and so is based on categorising assets into one of 4 increasingly more complex classes and asking questions, based on relevant standards, about each asset to identify risks.

It can be used to produce Risk profiles for individual assets or complete facilities, individually and collectively, based on customer-specific business impact. Therefore following a TRAP review an organisation will be better placed to understand its risk exposure and target scarce resources to achieve risk reductions.

Contents

1. Executive Summary
2. Table of Contents
3. Glossary
4. The Origins of TRAP
5. Current Threat Environment
6. TRAP Methodology
7. The Risk Assessment Process
8. TRAP Unique Features
9. TRAP Reporting Options
10. Conclusion
11. Why choose Thales?
12. About Thales

“92% of remotely available Industrial Control Systems have vulnerabilities” – Kaspersky Lab, July 2016.
Thales has extensive experience of conducting risk assessments with customers operating across numerous industry sectors. These assessments have been carried out using a variety of different methodologies. However, it became apparent that existing methodologies often did not fully meet the specific requirements of our Industrial Control clients, either in terms of their system focus or the underpinning standards on which they are based.

Traditional methodologies tend to be derived from generic information security guidance, such as the ISO 27000 set of standards. Whilst the recommendations made in these standards are extremely relevant to Business Information Systems, they are not always as applicable within an IACS environment.

These Risk Assessment methodologies also address human behaviour-related threats to the system(s) being assessed. However, within IACS environments, Human-Computer Interaction (HCI) is often quite different from that within a traditional business system.

In order to provide a risk assessment that was better targeted to IACS environments, Thales developed TRAP, a four-stage risk assessment process specifically tailored to OT environments. TRAP was developed based on our extensive knowledge of Industrial Control System (ICS) used in CNI environments.

TRAP incorporates a system classification process, which assigns each asset to one of four categorisation levels. It then uses non-subjective, weighted questions to produce a set of cyber-security key performance indicators (KPIs) that clearly illustrates how each asset or facility compares to industry best practice, and identifies the areas which are most vulnerable to attacks.

TRAP can assess your systems compliance against any combination of standards that are appropriate to your organisation (such as IEC 62443, ISO 27002, etc.).
CURRENT THREAT ENVIRONMENT
The number and variety of cyber threats which Industrial Control Systems are being exposed to is increasing at an alarming rate. Whilst Cyber-attacks have previously occurred more frequently on traditional business systems, the incidences of such attacks on critical infrastructure in general, and Industrial Control Systems in particular are growing at an alarming rate. The impact of a cyber-attack taking place at any of these facilities could have serious health and environmental implications as well as adverse operational, financial and reputational impact on an organisation.

In IT business systems, cyber-security is measured in terms of confidentiality, integrity and availability. The most important of these are traditionally confidentiality followed by integrity. Within control systems the priority of these aspects is reversed and continuous availability of systems and functionality become their primary concern. The range of cyber-attacks targeted at IACS can have many and varied impacts, ranging from minor disruption and inconvenience right through to environmental catastrophes and major loss of life.

One of the main attack vectors for cyber-attacks against Industrial Control Systems is via the Internet, which many of these systems were never originally intended to be connected to.

Tools used to identify vulnerable systems are now readily available. SHODAN, for example, is a search engine similar to Google which indexes HTTP (web message) header information – allowing users to identify equipment generally used within industrial control environments.

Project SHINE (SHodan INtelligence Extraction) was created to extrapolate metadata from the SHODAN search engine. This project investigated how many SCADA/ control systems were directly accessible on the internet and it discovered that over 1 million SCADA / ICS systems were directly connected to the internet with unique IPs. This figure is growing by between 2000 – 8000 / day. It is quite possible that many of these devices will be insecure and exploitable.

The business impact of a cyber-attack on SCADA systems must be clearly understood by the organisation in order to plan and implement the range of physical, technical, personnel and environmental security controls that should be put in place. As with cyber-attacks on IT systems, those launched against OT systems come in various forms and can have a multitude of impacts, based on the operations of the target company.

For example, a cyber-attack on a steel plant in Germany caused considerable damage to the blast furnace, whereas an attack on the San Francisco Municipal Transportation Agency resulted in ransomware being planted on the fare collection system which allowed passengers to travel for free.

TRAP METHODOLOGY
The Thales Risk Assessment Process (TRAP), is a standards based, asset focussed risk assessment process for use on Industrial Automation and Control Systems (OT) and Business Systems (IT).

The TRAP methodology incorporates a system classification process, which assigns each asset within an organisations OT infrastructure into one of four categorisation levels, based on increasingly levels of complexity.

Classification of a system is based on multiple factors, including levels of functionality and connectivity as well as user classes and interaction. Threat Intelligence from National Security Authorities, Regulatory Bodies or Special Interest Groups can also be injected into the classification process, as can any risk mitigation already provided by parallel redundant systems. All of these elements are combined to give an indication of the likelihood of compromise for an asset or facility.

A comprehensive Business Impact Assessment is then carried out against each asset to determine how a compromise of the system under assessment would impact the organisation. Impact is categorised across multiple different elements of the business, each of which is completely tailored to an individual company. It can be entirely bespoke, or based on specific industry sectors. Each element is assessed in terms of its impact on Confidentiality, Integrity and multiple versions of Availability. Availability is treated differently from the other elements, as often IACS have time-dependant functions to perform, and this can affect the impact any loss of availability might cause over different time periods.

The likelihood of compromise and output from the Business Impact Assessment are combined to classify each asset into one of four cybersecurity classes.

TRAP utilises an in-house developed tool which takes as input any combination of different standards (IEC-62443, ISO-27000, etc.) dependant on the customers’ domain (Government, Energy, Oil, Nuclear, Commercial, etc.). It then converts the compliance requirements contained within these standards into four class-specific question sets which consist of non-subjective, weighted questions. These are then used to establish the current level of compliance each asset / facility has against the chosen standards set. This Gap Analysis also clearly illustrates how each asset or facility compares to industry best practice and regulatory requirements, and identifies the areas which are most vulnerable to attacks.
THE RISK ASSESSMENT PROCESS

The output from the Gap Analysis is then used to produce a Risk Assessment for each asset, as well as an aggregated report for each facility. This Risk Assessment will identify specific areas of risk down to individual control level.

From this, the analyst will generate a Risk Treatment Plan, which will include recommendations of risk mitigation activities that should be incorporated into the system. These recommendations will be based on industry-specific mitigation techniques, and be appropriate for the system(s) being evaluated.

TRAP UNIQUE FEATURES

There are other risk assessment processes available, however none of these have the potential to help your organisation like TRAP.

The following are the key differentiators for TRAP:

Threat Level

- The TRAP tool allows you to include information from your National Security Authority, Industry Bodies and relevant groups, which is then incorporated into the overall risk calculations.

Risk Appetite

- TRAP also allows individual companies to insert their own Risk Appetite factors for different security aspects (C, I & A) against each asset.
- Reports are generated which show overall risks, but also those which are above current Risk Appetite levels.

What-if scenario testing

- With one click, organisations can visualise what effect a change in the National Threat Level, Business Impact, or Risk Appetite would have on an already assessed system.

Weighted question sets

- TRAP assigns weights to each question in each question set, based on understanding of each industry sector, to prioritise the specific areas that need more focus than others.

Multiple standards included

- The TRAP process currently supports assessments against IEC 62443, ISO27000, ANSSI and SANS 20.
- A GDPR module is currently being developed.
- Any other standard(s) can be incorporated at a customer’s request.

TRAP REPORTING OPTIONS

The TRAP tool can be used to provide different reporting options to suit your organisation’s preferences, so that the results of the gap analysis can be displayed in graphical representations as follows:

Tabular

### CLASS 3 TABLE - AGGREGATED C, I & A

<table>
<thead>
<tr>
<th>CONTROL AREA</th>
<th>LOW</th>
<th>MEDIUM</th>
<th>HIGH</th>
<th>VERY HIGH</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Policy</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Organisation of Security</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Asset Management</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Human Resources Security</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Physical and Environmental Security</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Communications and Operations Management</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Access Control</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Systems Acquisition, Development and Maintenance</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Incident Management</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Business Continuity Management</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Compliance</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR1 - Identification and Authentication Control</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR2 - Use Control</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR3 - System Integrity</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR4 - Data Confidentiality</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR5 - Restricted Data Flow</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR6 - Timely Response to Events</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>FR7 - Resource Availability</td>
<td>3</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Risk Totals: 108

- LOW: 0%
- MEDIUM: 40.7%
- HIGH: 48.1%
- VERY HIGH: 0.0%

TRAP

Thales Risk Assessment Process
TRAP is a flexible and customisable process, supported by tools, designed to help organisations understand the risk exposure that they face and provide the results in a format that best suits the organisation.

In developing TRAP, Thales has built upon its knowledge and expertise to provide a process that is unique in the risk assessment arena. TRAP is scalable to suit simple systems, right up to very complex industrial environments. It can be applied not only to Industrial Automation and Control Systems, but also to Business IT environments. TRAP can also be used in any scenario where compliance against any forms of legislative or regulatory compliance needs to be measured.

WHY CHOOSE THALES?
Thales are able to provide operatives with both the process skills and the sector knowledge. Thales has a proven record in delivering risk assessment across both civil and military operations and in all business sectors. Thales is committed to helping organisations understand the threats to their business and is a major collaborator with the National Cyber Security Centre in the UK.

Thales provides Managed Security Services for Critical Infrastructure Operators and multinational organisations from its own network of Cyber Security Operations Centres. These facilities have the ability to monitor network infrastructures in real-time to detect potential attacks and can provide incident management capabilities following a breach, including full forensic investigation support.

Our security consultants can undertake scanning of existing infrastructures to detect potential threats and recommend appropriate controls that should be instigated to help mitigate or remove any identified vulnerabilities.

Comprehensive Cyber Security however is not just about technical solutions. Thales has extensive experience in developing Information Assurance and Governance programmes for world-leading organisations, and can provide training and awareness programmes tailored to individual customer’s needs.

ABOUT THALES
Whenever critical decisions need to be made, Thales has a role to play. World-class technologies and the combined expertise of 65,000 employees in 56 locally based country operations make Thales a key player in assuring the security of citizens, infrastructure and nations in all the markets we serve – aerospace, space, ground transportation, security and defence.

For more than 40 years, Thales has delivered state of the art physical and cyber security solutions to commercial, critical national infrastructure, government and military customers.

Thales will help you refocus your security spend to defend your organisation and prevent significant loss of revenue and reputation. Thales will ensure your competitive advantage is maintained by being able to demonstrate resilient and secure use of physical and cyber security.

For further information visit our website at www.thalesgroup.com/en/tcc-uk or email, thalescyberandconsulting@uk.thalesgroup.com