

# THALES CYBER AND CONSULTING

## Thales Risk Assessment Process (TRAP)



### KEY BENEFITS

- Objectively and quantifiably measure the risk profile of your ICS
- Compare your current cyber security posture against industry best practice
- Highlights specific and systemic vulnerabilities in the organization's systems and provides prioritised recommendations on ways to address them
- Provides a method to accurately monitor improvement in your cyber security
- Can be applied to all industries as question sets can be tailored to suit any environment

### INTRODUCTION

The cyber security of Industrial Automation and Control Systems represents a significant challenge within today's complex industrial and service infrastructures. It is essential to defend our current ICS environments against a cyber-attack. The ability to determine and understand what the threats and risks are that these systems could be exposed to is now critical.

### THALES RISK ASSESSMENT PROCESS (TRAP)

Thales has developed a bespoke methodology and accompanying tool to objectively assess current cyber security provision within Industrial Automation and Control Systems against a baseline standard(s) such as IEC 62443 and to identify areas where improvements are necessary to achieve an acceptable risk profile.

### OUR APPROACH

Data collected through a series of directed workshops identifies the current state of your ICS estate. Assets are then assessed on their functionality and connectivity models, and combined with threat information and business impacts to determine a risk factor for each asset. Each asset is then objectively and comprehensively assessed based on their risk factor to determine the controls which are currently deployed and how that compares to industry best practice. As a result any gaps or non-compliance to the standard will be identified.

### USE CASES

TRAP is specifically designed to be configurable for multiple industry sectors. It supports compliance with multiple International Standards and generates sector-specific question sets as part of the assessment process. It is particularly suited to organisations which run Industrial Control and SCADA systems in parallel with traditional IT systems, in sectors such as Energy, Transport and Nuclear.

The TRAP methodology can be applied to existing systems as well as upgrades to legacy environments and completely new installations.

### FUTURE DEVELOPMENT

The functionality provided by the TRAP tool is being continuously reviewed and enhanced to take account of the ever changing threat landscape. It uses applied learning gained from each deployment to feed best practice principles across industry sectors.

### BUSINESS MODEL

Thales will provide experienced consultants to work with your teams to perform TRAP assessments. Engagements will be fixed price according to the size of your environment and the extent of your estate. Contact us for further details, or to request a quotation.

## SUMMARY OF SERVICES

- Prioritised risk reports detailing areas where the introduction of mitigation controls would be most effective
- Functionality and Connectivity categorisation of assets and facilities
- Probability assessment based on industry-specific threat profiling
- Business Impact Assessment of compromise
- Gap Analysis against all relevant standards including IEC 62443
- Full Risk Assessment of your environment
- Methodology and Tool tailored by domain

## MARKETS AND CUSTOMERS

TRAP is applicable across the entire systems development lifecycle and in all domains where Industrial Automation and Control Systems are operated, such as Nuclear Power Plants and Reprocessing Facilities, Railway signalling systems, Oil Refineries and Pharmaceutical Production Plants.

Operators of CNI facilities are more frequently being targeted by cyber attacks and would benefit from the assessments provided by the TRAP tool.

TRAP helps customers objectively assess their compliance to industrial cyber security standards such as IEC 62443.

## CASE STUDY

TRAP has been successfully used within a major Nuclear facility in the UK. By using the TRAP methodology, the client was able to identify key areas of their ICS estate which could be susceptible to cyber attack and prioritise resources to mitigate those risks.

## WHY THALES?

- Extensive expertise in Cyber Security, both in Information and Operational Technologies
- Proven track record of delivery in Industrial Control sectors
- Unique approach to Industrial Cyber Security Risk Assessments