



Process Control System Security

A Trusted Approach to Process Control System Security for the Energy Industry

With Gartner predicting that, by 2015, at least one G20 nation's critical infrastructure will be disrupted and damaged by online sabotage, infrastructure managers are looking to establish an effective security regime that addresses threats and vulnerabilities in their industrial networks.

Following high profile attacks such as Stuxnet, Conficker and NightDragon, Process Control System Security (PCSS) is recognised as an increasingly business critical issue for energy and utility companies globally.

Solution

Concern has risen with the migration of Process Control System vendors to commercial off-the-shelf computing and communications platforms. The increasing interconnection of industrial control and traditional IT systems can undermine the integrity and security of vital control systems.

ProcessSecurity+ helps world-renowned energy organisations protect against safety issues, financial loss, non-compliance, HSE incidents and public relations issues that are all real, and potentially damaging. All of which are a consequence of a failure in PCSS. Amor's approach to ensuring PCSS is based upon a proven 5 stage methodology:

Features

- End-to-end project management of the Process Security process
- Aligned with emerging UK, USA and international standards
- Full assessment of PCSS maturity in an organisation
- Create/review security policy against industry best practice
- Identify, document and categorise the organisations' process control systems
- Perform and document methodical compliance and risk assessments, aligned with the security policy
- Identify and implement remedial actions to mitigate risks
- Definition and implementation, including training, of processes and procedures to ensure ongoing PCSS sustainment and compliance



STEP 1:

Maturity Assessment

Have we got a problem?

STEP 2:

Inventory

What have we got?

STEP 3:

System Assessment

Where are the gaps and risks and what do we do about them?

STEP 4:

Implementation

Close the gaps and mitigate the risks

STEP 5:

Sustainment

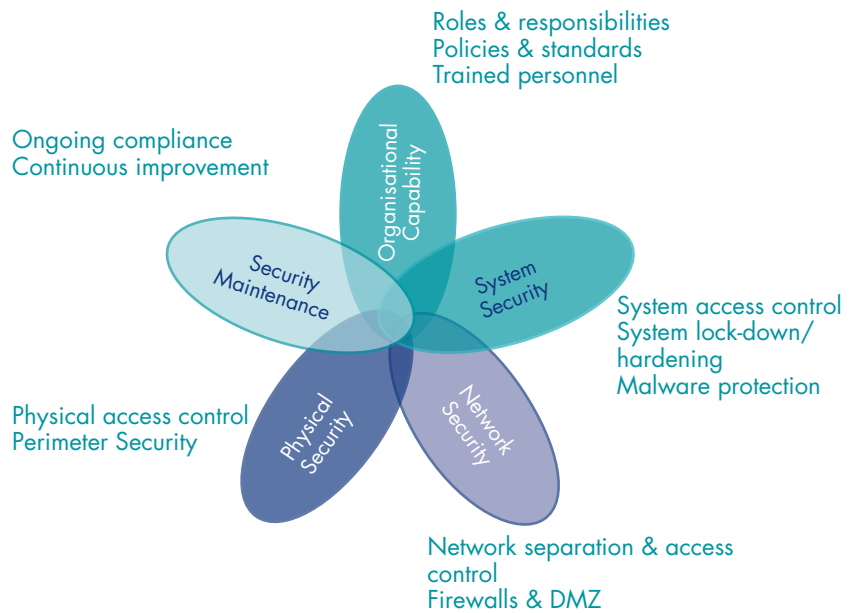
Establish processes to maintain security





Solution

The Kingsnorth power station shutdown, the Olympic pipeline explosion and the Natanz Nuclear Uranium Enrichment Plant Stuxnet attack are just three large security breaches that have made headlines in recent times. For the most part, these incidents are the result of unintentional staff errors that can be easily prevented by good security practices. However, a deliberate attack by disgruntled employees, or an attack from outside your organisation, is much harder to protect against. Without doubt, the precautions you are already taking to prevent unauthorised access to your business network will help, but the use of Amor Group's ProcessSecurity+ methodology should be considered to reinforce the strength of your system, with a focus on 5 key areas:



Track Record

Amor Group operates a Process Control System Security team unique in its focus on the Oil & Gas and Utilities markets. Our highly skilled and operationally focussed team have successfully mitigated the security risks inherent in the changing industrial process control landscapes on over 8000 items of equipment and 500 process control and monitoring systems, all of which have been in the Energy sector. Working with multiple organisations last year, our team was able to help our customers:

- Achieve 100% compliance with internal process control policies and industry best practice guidelines;
- Achieve zero reportable health, safety and environmental incidents triggered by security breaches of process control systems;
- Sustain brand equity through avoidance of negative press coverage emanating from process control related incidents;
- Avoid unplanned shutdown through avoidance of security breaches.

