But enabling connectivity and remote access on this scale introduces vulnerabilities.

CPNI have developed a framework and good practice guide for securing ICS. This comprises eight core elements that address the increasing use of standard IT technologies in ICS. You can use these as points of reference to help you develop and tailor ICS security, appropriate to the needs of your organisation.

Malicious code is getting onto our industrial networks in different ways.

Stuxnet was the first known autonomous threat to target and sabotage Industrial Control Systems to such an extent.

In 2003 the Slammer worm infected the security system of a nuclear power plant and Industrial Control Systems are being targeted.

How can you manage the risk?

CPNI have developed a framework and good practice guide for securing ICS. This comprises eight core elements that address the increasing use of standard IT technologies in ICS. You can use these as points of reference to help you develop and tailor ICS security, appropriate to the needs of your organisation.

REFERENCES