Risktec

RISKworld issue 27 spring 2015 pg 5 the newsletter of risktec solutions limited

Cyber Risk for the Rail Engineer

Cyber security issues have pervaded almost all aspects of life as daily data breaches and hacked websites testify. In the rail sector, where previously isolated control systems have become connected to the internet, we have seen a new challenge emerge for engineers tasked with ensuring system reliability, availability, maintainability, safety and now security (RAMSS).

There are very good reasons for connecting control systems to the internet. Operating costs can be kept lower and reliability and performance can be greatly improved by providing more timely information and instruction for maintenance. There is also a safety benefit from a reduction in human error.

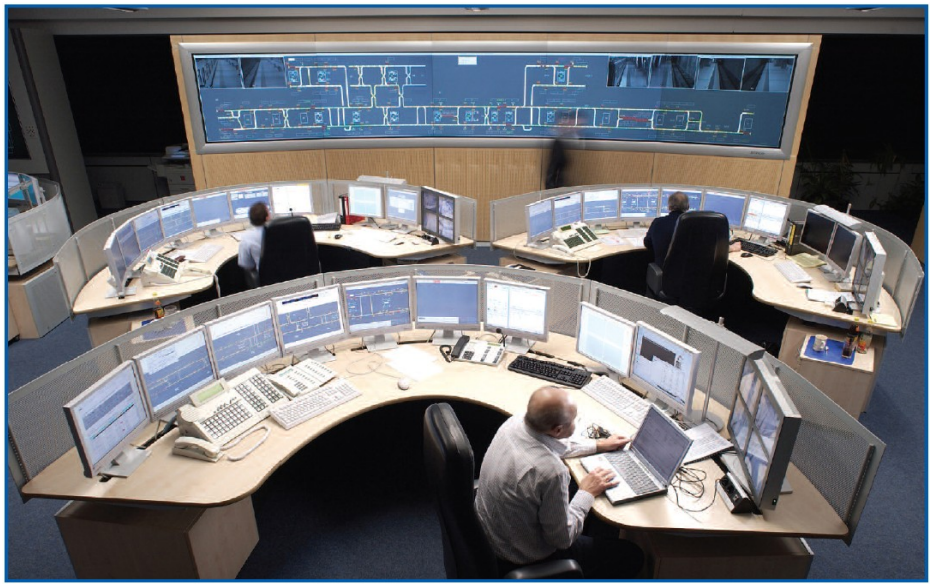
Unfortunately the commercial drive for internet protocol (IP) enabled systems has brought in security risks, with systems now being exposed to hackers across the internet. Hacking control systems is the new and growing pursuit of hobbyist hackers, those with malicious intent and nation states alike. As more and more IP enabled and connected, commoditised hardware is used, cyber related risk needs to be considered; it is now a given that any current or future rail system may use products vulnerable to cyber attack.

Box 1 - Managing Control System Cyber Risk

- Accept that cyber risk is now a part of everyday rail engineering activity
- Become cyber aware and take an interest in cyber related security issues
- Get a thorough understanding of the control systems in your domain and ensure that they have been cyber security risk-assessed and incorporated in the safety case
- Ensure control system vendors are able to provide evidence of a detailed third-party cyber security evaluation of their products

The reality of cyber risk

Probably the first time the public was made aware of control system hacking was in 2010 when the Stuxnet computer worm was widely reported to have infected nuclear facilities in Iran. A technician plugged a worm infected USB stick into a control system PC. This adversely impacted the site's centrifuges and their ability to enrich uranium. Over the past year other control systems have been hacked due to weak system passwords or simply because control system administration interfaces had no firewall or authentication mechanism in place.



Cyber risk and rail systems

Those responsible for infrastructure are taking cyber risk seriously: the UK Government's 2010 National Security Strategy rated cyber attacks a 'Tier One' threat alongside terrorism, war and pandemic disease. Rail engineers need to take an equally serious approach to cyber risk.

In the UK, with the move to unified control systems and regional operational centres, the impact of a successful cyber attack can have national implications. How might cyber security affect other systems such as power, passenger information, asset condition monitoring, train door control, ticketing barriers and escalators for example?

Managing system risk

RAMSS rail engineers have a key part to play in managing cyber security risk, see Box 1. They need to ensure that the advantages delivered by new technology and networks are not outweighed by cyber risk. Engineers should know enough about cyber security issues to ask pertinent questions of system suppliers and implementers, and in turn seek expert advice if they have any doubt over the safety and reliability of a system.

As such, cyber security is becoming an ever increasing requirement for inclusion in engineering safety cases. A safety justification for a technical system should consider the impact of cyber security risk and demonstrate that safeguards are in place to control this to an acceptable level. Safety cases lacking in this area are incomplete.

Conclusion

With many rail networks across the world undergoing a transformation by introducing IP enabled systems, cyber risk has become a reality. Control systems across these rail networks are potentially exposed to cyber attack. To counter this, RAMSS rail engineers need to ensure that such systems are security risk-assessed and any weaknesses are mitigated proportionately, alongside other traditional risks. After all, who wants to be headline news in the next hacking scandal?

UK Principal Office
Wilderspool Park
Greenall's Avenue
Warrington WA4 6HL
United Kingdom
Tel +44 (0)1925 611200
Fax +44 (0)1925 611232

Europe
Aberdeen
Alderley Edge
Ashford
Bristol
Crawley
Derby
Edinburgh
Glasgow
London
The Hague

Middle East
Abu Dhabi
Dubai
Muscat

North America
Calgary
Houston (South East)
Houston (Energy Corridor)

For further information, including office contact details, visit:
www.risktec.com
or email:
enquiries@risktec.com

Risktec
TÜV Rheinland Group®