# Transport- Securing the Railway Environment
# Case Study – Rail Corridor Security Specifications & Risk Assessment

## The Client

A consortium lead by a bi-lateral railway authority and a major international petroleum company.

## Client Profile

The railway operates a corridor over 905 km of single and double track; with a carrying capacity of 15 Million Tones of freight and 3 Million passengers per year. Over half of the freight transported is made up of oil and oil products.

The rail corridor is an energy and economic regional powerhouse as part of an oil transportation network, shipping oil to Western Europe and beyond.

The railway is under going substantial infrastructure modernisation and new build construction to expand operating efficiency and capacity. A vital pre requisite for future aspirations is the secure transport of oil inventory and passengers.

.

CYBERRISK.COM
SECURITY - ASSURANCE - FORENSICS - ENABLING

## The Challenge

To undertake a comprehensive security review, strategic security risk assessment and provide advice on functional requirements and applying appropriate standards; for cyber, physical and operational security. Particular emphasis was placed on addressing threats from terrorism, organised crime, criminality, sabotage and nation state attack.

## Response

Cyberrisk.com undertook a security threat, vulnerability and risk assessment creating a central risk register with risk mitigation strategies. Specific detailed advice was given under the themes of cyber security and resilience, physical and electronic protective security, Counter Terrorism protective security and Crime prevention through environmental design.

The cyber security assessment focused on SCADA and signalling systems and managing cyber risks of the network control systems. In terms of physical counter terrorism protection, specific advise was given on Hostile vehicle Mitigation (HVM), blast effects and blast protection, ballistics / weapons protection and integrated security. As well as providing functional specifications for CCTV and access control.

## Result

- ► Implementation of a Cyber Security and cyber risk management framework (covering ICT, SCADA systems, Signalling and Network Control Centre)

- ► Deployment of Integrated perimeter security systems for staging yards and critical assets and infrastructure, consisting of security fencing, CCTV & lighting, perimeter intrusion detection systems (PIDS), C3i command and control, card access control and alarms, security/electronic tagging of oil tanker wagons.

- ► Adoption of industry best practice standards, such as ANSI/ISA-99.02.01-2009, Security for industrial control systems, ISO 31000 Risk Management, ISO 27000 Information security management.

- ► Improved standard operating procedures (SOP's) and security training.

- ► Reduced vulnerability of critical assets to threats with reduced freight inventory loss and improved passenger safety.

CYBERRISK.COM

Copyright © 2015 Cyberrisk.com Ltd All rights reserved.