Motherwell
automation

CYBER SECURITY AUDIT

10 Sangiorgio Court • Osborne Park, Western Australia 6017
T +61 (0)8 9212 4444 • F +61 (0)8 9212 4479
E sales@motherwell.net.au
www.motherwell.net.au

Cyber Security Audit - Austal Case Study - DNV GL Gap Analysis / Roadmap

Austal

Austal is a global shipbuilder and defence prime contractor and recognised world leader in the design and construction of customised commercial and defence vessels. Austal proudly lists many of the world's leading ferry operators, navies and defence forces as valued clients. As the world's largest aluminium shipbuilder, the company has earned a reputation built on innovative hull design, 'smart' maritime technology, modular manufacturing techniques and value-adding in-service support.

Austal's extensive product range includes passenger and vehicle-passenger ferries, patrol boats, high speed support vessels, surface combatants and revolutionary multi-role vessels. Austal also designs, installs, integrates and maintains sophisticated vessel command & control systems with its MARINELINK automation products, communications, radar systems and information management systems.

The Challenge: Cybercrime

Cybercrime is one of the most pervasive threats facing Australia and the most significant threat in terms of overall volume and impact to individuals and businesses. The Australian Cyber Security Centre (ACSC) Annual Cyber Threat Report 2019-20 report[1], identified *"Australians lost over $634 million to scams in 2019. While the true cost of cybercrime to the Australian economy is difficult to quantify, industry estimates have previously placed cyber security incidents as high as $29 billion annually."*

Cyber-attacks are becoming more prevalent as businesses become more connected to the global communications network. Within the global maritime industry, it is expected that 2020 will end with more than 500 major cyber security breaches, with substantially more going unreported. [2] In recognition of the threat that Cybercrime poses to its business and its customers, Austal embarked on a program to analyse its vulnerability to Cyber-attacks; particularly with respect to compliance with relevant industry cyber security standards.

The Objective: DNV GL Compliance

Austal operates in an environment that requires compliance with strict maritime Cyber Security requirements. The Austal designed automation system "MARINELINK" is a complete hardware and software solution. MARINELINK integrates the operational technology/third party systems and provides decentralised control of all vessel systems.

Recognising the increase in connectivity of systems, the growing risk of cyber incidents and the importance of addressing cyber security in the design and operation of the vessel, DNV GL established a Class Notation of Cyber Security requirements addressing cyber security of vessels and their systems.

The Approach

Following an internal review of available options, Austal elected to engage an external independent party having both Cyber Security and control system expertise to audit Austal facilities; to this end Austal engaged Motherwell Automation. The scope of Motherwell Automation primarily involved performing a compliance Gap Analysis between Austal facilities and DNV GL requirements and included:

- Review of current documentation
- Review of network and security system design
- DNV GL compliance assessment of Austal's custom developed IMACS (Integrated Monitoring Alarm and Control System) 'MARINELINK' (see further information at https://marinelink.austal.com/) that provides real-time, onboard and remote location systems and control and monitoring functionality for a variety of vessels
- Cyber security audit
- Penetration testing

Relevant DNV GL rules, standards and codes of practice against which compliance was assessed included:

- DNV GL-RP-0496 (Recommended Practice)
- DNV GL-CP-0231 (Class Programme – Type Approval)
- DNV GL-RU-SHIP-Pt1Ch2 Section 6 (Rules for Classification: Ships Class Notation)
- DNV GL-RU-SHIP-Pt4Ch9 (Control and monitoring systems)
- DNV GL-RU-SHIP-Pt6Ch5 Section 21 (Equipment and design features Sec21 Cyber Security)

Assessment

The compliance assessment was undertaken primarily via two work-fronts comprising:

- Gap Analysis
- Penetration Testing

Gap Analysis

- Review and summary of applicable DNV GL requirements for effective communication to the client

- Review all Austal documentation and system design standards including:
  - √ Cyber security policies & assessments
  - √ Network topologies
  - √ System software lists /descriptions / versions

- Network Review, including:
  - √ Network Discovery
  - √ Endpoint Probing
  - √ Network Foot Printing / Banner Grabbing
  - √ TCP / UDP Port Enumeration
  - √ Network Backbone Scanning and Monitoring
  - √ Log Review
  - √ Web Interface Review
  - √ Application Security Review
  - √ Vulnerability Assessment
  - √ VoIP Security
  - √ Wireless Testing
  - √ Physical Security

- Workshops with Austal personnel to:
  - √ Outline the critical areas of the MARINELINK System in relation to DNV GL security requirements
  - √ Review the level of compliance with those requirements and, in particular, compliance with IEC 62443-3-3 Foundational Requirements of OT systems
  - √ Review how non-compliance may be addressed

- Workshop outcomes were then used to develop the network analysis and penetration testing criteria on a client vessel

Penetration Testing

Functional and technical testing of the MARINELINK System environment, performing non-intrusive penetration testing to determine the real-world compliance to DNV GL requirements; this included:

- Reconnaissance (information gathering)
- Evaluation methodology
- Non-intrusive network analysis
- Threat Modelling
- Vulnerability Identification
- DNV GL Security Requirements Tests, including:
    - √ Network Assessment
    - √ Non-Repudiation
    - √ DoS / Network Storm
    - √ ACLs & Network Policies
    - √ Brute force Prevention and Credentials / Passwords
    - √ Syslog Capabilities and Behaviour
    - √ Mobile / Portable Code
    - √ Traffic Encryption and Packet Capture
    - √ Executables / Software and Digital Certificates
    - √ Workstation / Component Setup Review
    - √ Timeserver
- Recording of discovered vulnerabilities
- Detailed reporting of test results

Outcomes

The collaboration between Austal and Motherwell Automation produced the following outcomes:

Roadmap

Motherwell Automation developed a detailed roadmap outlining the steps that must be taken by Austal to address identified vulnerabilities and reach full DNV GL compliance by 2021. This includes:

- √ Updating/development of overarching Policies and Procedures
- √ Updating/development of internal design Philosophies and Procedures
- √ Re-evaluation of Foundational Requirements
- √ Risk management assessment to prioritise each requirement
- √ Implementation of requirement solutions

Compliance

Implementing the Roadmap will ultimately provide full compliance with relevant DNV GL requirements.

This will not only enhance the reputation and capabilities of Austal within its chosen markets, but will provide increased protection against cyber-attacks and cybercrime in general.

Continuous Improvement

Cybercrime is continually evolving and the threats posed by Cybercrime are increasing in terms of frequency, sophistication and impact. As a consequence, it is Austal policy that its in-house protections against Cybercrime are constantly monitored and upgraded as required to combat emerging cyber threats.

To assist Austal on its path of continuous improvement, Motherwell Automation can provide a suite of services to help protect the business from ever-present and ever-growing Cyber threats; such services include:

- √ Reviewing updated DNV GL requirements
- √ Independent Austal documentation review
- √ Recommendations on modifications to practices, guidelines, policies and procedures as required to comply with updated DNV GL requirements
- √ Penetration testing / support for new and existing vessel builds
- √ Cyber Security training and awareness
- √ Support with network design and implementation
- √ Software / Firmware management

Motherwell Automation

Motherwell Automation is a dynamic Perth-based company that has built an excellent reputation for providing Innovative Operational Technology solutions to the Australian market for over 30 years.

Motherwell Automation is committed to delivering a customer centric, best practice, result orientated approach to meeting client requirements; our engineering solutions encompass the entire lifecycle from design, supply, implementation and commissioning through to post project support and training.

The Motherwell Automation team comprises a diverse group of highly experienced engineers with a wealth of expertise in a broad range of industries including Mining & resources, Oil & Gas, Bulk materials, Power generation & Utilities and Cyber Security; amongst others.

In addition, Motherwell Automation has long standing partnerships with highly reputable, world leading manufacturers to represent and support a quality range of automation, control, power and cyber security related hardware and software products.

Embracing a culture of technical excellence and responsiveness to technological advances, Motherwell Automation delivers current and innovative whole-of-life solutions into client applications.

DNV GL: *A leading classification society and recognized advisor for the maritime industry headquartered in Høvik, Norway. It was created as a result of a merger between Det Norske Veritas (Norway) and Germanischer Lloyd (Germany).*

[1] *https://news.microsoft.com/en-au/features/direct-costs-associated-with-cybersecurity-incidents-costs-Australian-businesses-29-billion-per-annum/*

[2] *https://www.marinelink.com/news/maritime-cyber-attacks-increase-480311 (Vanguard 29/7/2020)*