LAGONI
INNOVATIVE ENGINEERING SOLUTIONS

The threat from cyber-incidents on the critical national infrastructure is real and poses huge risks both to the industry and wider economy. The risks and potential consequences are significant and must be addressed on numerous levels. Cyber Security is not simply a catchphrase. Addressing the ever-changing Industrial Control Systems (ICS) Cyber Security threat poses a significant challenge to the industry, one which Lagoni have invested heavily to support.

Due to the changing political scene and increased level of automation and connectivity in industrial infrastructure, there is an ever-growing need to cyber-secure ICS. There are a number of specific drivers including legislation, real world attacks and political uncertainty which have the potential to impact the ICS Cyber Security landscape. Importantly, Operational Technology (OT) Cyber Security must adopt a whole-lifecycle approach. Due to the ever-changing nature of cyber threats, ensuring that security solutions are maintained is of paramount importance.

CYBER SECURITY
Operational Technology

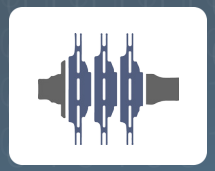
The Cyber Challenge

- OT Cyber Security is much more than mere technology deployment. Consideration needs to be given to people, processes and technology, which is very similar to the well-established approach to functional safety with which Lagoni are well versed.
- OT Cyber Security requires a different approach to that currently deployed in IT. OT Cyber Security primarily aims to protect data integrity rather than privacy.
- The Cyber Security risk is difficult to quantify as the likelihood is uncertain and not repeatable.
- The standalone skillsets in IT and OT, without sufficient process and engineering knowledge, can leave critical national infrastructure owners exposed in terms of compliance and Cyber Security management.

Our Approach

- Originating from a heavily regulated safety domain, our engineering culture has always been focused on providing high integrity mission critical solutions.
- We combine our Cyber Security specialist skillset with both ICS engineering and risk management specialisms, to ensure that any Cyber Security solution is fit for purpose.
- We have a risk-based approach to Cyber Security in the industrial control & automation space, which has been developed with HSE, NISD and International Standards in mind.
- By offering a lifecycle approach with stakeholder engagement at board, management and operational working levels; we are able to identify, design and deliver the most suitable OT Cyber Security solution, tailored to meets the needs of each client.

Case Studies



Cyber ICS Assessment

We have undertaken ICS Cyber Assessments on CNI assets. This provides a measurable benchmark for improvement and awareness

Risk Management

Lagoni have successfully carried out a risk assessment methodology to comply with the HSE, NISD and IEC62443 for the OT space for CNI asset owners

Counter Measure

We have implemented a detailed methodology that incorporates physical, cyber and operational policies to secure legacy brownfield systems, avoiding costly replacements.

ICS Penetration Testing

We have completed live testing against a brownfield assets, to assure CNI asset owners that counter measures are being managed correctly.