Technische Universiteit Delft

Offshore & Dredging Engineering

Last line of defence

Cyber security of industrial control systems

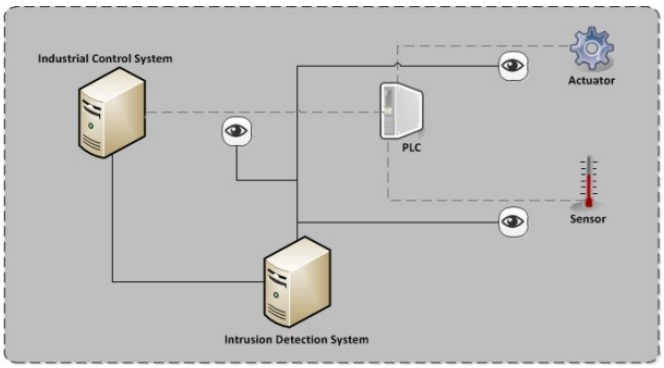
The world is rapidly embracing networked technology and transitioning into one of hyperconnectivity, a term first coined by social scientists Anabel Quan-Haase and Barry Wellman. Increased connectivity provides benefits such as automation and, remote access and control of networks and equipment, thereby decreasing operational costs. Maritime and offshore companies are increasingly automating their vessels and platforms to reduce the required workers on-board and centralise platform control.

With this tight coupling of complex ICT and industrial control systems however comes an increase in risks. These risks are further increased due to the application of security controls. Where in mechanical and structural engineering the focus lies on failure (e.g. safety factors), this is not necessarily the case for ICT related systems, which are often only verified to be working as specified and expected. Unexpected behaviour is not taken into consideration. Thus, while most vessels and platforms depend on automated systems, it seems little is being done to protect them from cyber incidents and attacks. The impact of security breaches on these systems can be disastrous due to the potential for physical damage to people and planet. This is especially true within the oil and gas industries. For example a fire at the Piper Alpha production platform in the North Sea in 1988, caused by an oil and gas leak, resulted in the loss of 169 lives. While computer viruses or worms might not directly injure people, or destroy equipment, automated control systems can.

This work thus focusses on the area where mechanical systems meet automation systems, a field called industrial control systems. An investigation into the current state of cyber security within the dredging industry has been conducted, which was followed by a threat analysis on industrial control systems. These systems operate at the heart of the dredging industry. This has revealed that malicious software can cause physical damage to equipment and injury to people. In an effort to improve the current state and help prevent cyber incidents from occurring the following research question has been formulated:

Can adversaries operating on Control System infrastructures be detected by an Intrusion Detection System which is monitoring the physical state?

To answers this question a novel intrusion detection system is designed which takes advantage of the physical state of the processes. This new concept deviates from other systems in that they obtain information from the network, as opposed to the physical process, where the data cannot necessarily be trusted. Additionally, when malicious events or cyber incidents occur within or behind the controller (PLC), the control network does not necessarily contain the required information detailing ongoing attacks. Looking at the physical system then allows for malicious attacks and cyber incidents to be detected by observing anomalous and unexpected behaviour of the monitored physical process. This enables the detection of advanced malicious threats which would be missed otherwise. The required information on the physical state of the process is obtained on the last line, between the controller and field devices.



Student
M. Luchs
October 26th, 2016

Sponsor
Heerema Fabrication Group

Thesis committee
Prof. Dr. Ir. C. van Rhee
Dr. ir. S. A. Miedema
Dr. Ir. C. Doerr
Ir. F. Van der Heijden