PRECURSOR ANALYSIS REPORT: INSIDER ATTACK ON THE MAROOCHY SHIRE SEWERAGE CONTROL SYSTEM IN 2000

Cybersecurity for the Operational Technology Environment (CyOTE)

30 DECEMBER 2022

CyOTE Cybersecurity for the Operational Technology Environment

U.S. DEPARTMENT OF ENERGY | *Office of* Cybersecurity, Energy Security, and Emergency Response

INL/RPT-22-70376

This document was prepared by Idaho National Laboratory (INL) under an agreement with and funded by the U.S. Department of Energy.

INL is a U.S. Department of Energy National Laboratory operated by Battelle Energy Alliance, LLC

This *paper* is the product of *research* conducted by the Cybersecurity for the Operational Technology Environment (CyOTE) program and was funded by the Department of Energy Office of Cybersecurity, Energy Security and Emergency Response (DOE CESER). No updates have been made since the date of publication and no further funding has been approved.

TABLE OF CONTENTS

FIGURES

TABLES

PRECURSOR ANALYSIS REPORT: INSIDER ATTACK ON THE MAROOCHY SHIRE SEWERAGE CONTROL SYSTEM IN 2000

1. EXECUTIVE SUMMARY

The Insider Attack on the Maroochy Shire Sewerage Control System in 2000 Precursor Analysis Report leverages publicly available information about the Maroochy Shire cyber attack and catalogs anomalous observables for each technique employed in the attack. This analysis is based upon the methodology of the Cybersecurity for the Operational Technology Environment (CyOTE) program.

Between late January and 23 April 2000, the newly installed Supervisory Control and Data Acquisition (SCADA) system controlling the municipal sewerage system run by the Maroochy Shire Council (MSC) in Queensland, Australia experienced numerous anomalous faults. This Precursor Analysis Report uses publicly available information to construct an attack timeline consisting of three phases. The first phase took place between January and February 2000 and resulted in anomalous system faults, prompting an investigation by HWT. The faults included loss of communication, loss of pump control, false alarms, suppressed alarms, and altered pumping station configurations. Hunter Watertech Pty Ltd. (HWT), the contractor that installed and configured MSC's SCADA system, investigated the faults and determined that many of the system's problems resulted from insider threat intrusions rather than equipment failure.

The second phase occurred in March 2000 when HWT comprehended MSC was experiencing a cyber attack that resulted in a significant sewage spill perpetrated by a disgruntled former HWT engineer. The clean-up took days and required the deployment of considerable resources. In total, MSC spent $176,000 AUD ($102,813 USD) and HWT spent more than $500,000 AUD ($292,084 USD) to rectify the incident.

The final phase took place on 23 April 2000, when the adversary modified and suppressed alarms, and was later apprehended by police.

Researchers and analysts identified 16 unique techniques (used in a sequence of 24 steps) utilized during the attack with a total of 94 observables using MITRE ATT&CK® for Industrial Control Systems. The CyOTE program assesses observables accompanying techniques used prior to the triggering event to identify opportunities to detect malicious activity. If observables accompanying the attack techniques are perceived and investigated prior to the triggering event, earlier comprehension of malicious activity can take place. Four of the identified techniques used during the Maroochy Shire cyber attack were precursors to the triggering event. Analysis identified 16 observables associated with these precursor techniques, three of which were assessed to have an increased likelihood of being perceived in the 20 days preceding the triggering event. The response and comprehension time could have been reduced if the observables had been identified earlier.

The information gathered in this report contributes to a library of observables tied to a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack. Asset owners and operators can use these products if they experience similar observables or to prepare for comparable scenarios.

2. INTRODUCTION

The Cybersecurity for the Operational Technology Environment (CyOTE) program developed capabilities for energy sector organizations to independently identify adversarial tactics and techniques within their operational technology (OT) environments. Led by Idaho National Laboratory (INL) under leadership of the Department of Energy (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER), CyOTE is a partnership with energy sector owners and operators whose goal is to tie the impacts of a cyber attack to anomalies in the OT environment to determine whether the anomalies have a malicious cyber cause.

2.1. APPLYING THE CYOTE METHODOLOGY

The CyOTE methodology, as shown in Figure 1. CyOTE Methodology applies fundamental concepts of perception and comprehension to a universe of knowns and unknowns increasingly disaggregated into observables, anomalies, and triggering events. The program utilizes MITRE's ATT&CK® Framework for Industrial Control Systems (ICS) as a common lexicon to assess triggering events. By leveraging the CyOTE methodology with existing commercial monitoring capabilities and manual data collection, energy sector partners can understand relationships between multiple observables, which could represent a faint signal of an attack requiring investigation. CyOTE can assist organizations in prioritizing their OT environment visibility investments.

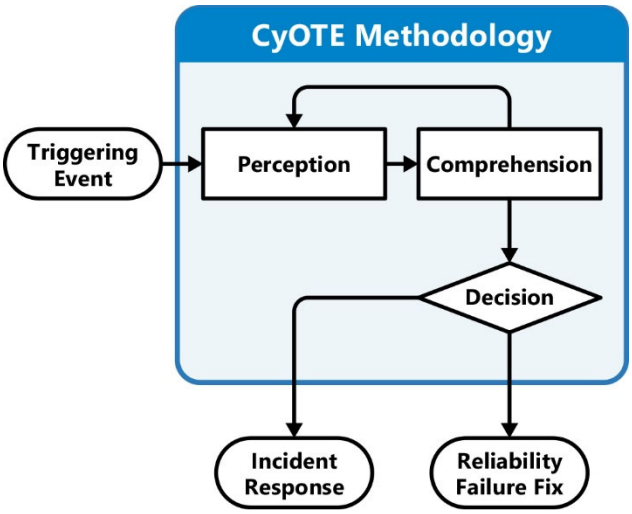


Figure 1. CyOTE Methodology

Historical case studies such as this one support continued learning through analysis of incidents that have impacted OT. This precursor analysis report is based on publicly available reports and provides examples of how key concepts in the CyOTE methodology appear in the real world, providing insights on how similar novel attacks could be detected earlier and therefore mitigated. The analysis enables OT personnel to independently identify observables associated with techniques known to be indicators of attack within OT environments. The identified observables highlight anomalous events for further investigation, which could enhance comprehension of malicious activity.

A timeline of events based on the CyOTE methodology portrays the attack-related observables associated with the precursor analysis report cyber attack. The timeline includes assessed dates, the triggering event, and comprehension of malicious activity by the organization. The point on this timeline when each technique appears is critical to the organization's ability to perceive and comprehend the associated malicious activity. Perception of techniques early in the timeline is critical, since halting those techniques will generally have greater potential to limit additional attack vectors using other techniques, defeat the cyber attack, and limit damage to operations.

Each technique has an assessed perceivability. Perceivability is a function of the number of observables and the potential for personnel to detect those observables. If a technique includes effects which personnel may detect, such as deletion or modification of system files or required user execution, then the technique would be more perceivable.

Differences in infrastructure and system configurations may present different challenges and opportunities for observable detection. For example, architecture-wide endpoint monitoring is likely to improve the perceivability of techniques which modify host files, such as the Data Destruction technique (T0809) for Inhibit Response Function and Theft of Operational Information technique (T0882) for Impact. Network monitoring and log analysis capabilities are likely to improve perceivability of techniques which create malicious network traffic, such as the Standard Application Layer Protocol technique (T0869) for Command and Control, External Remote Services technique (T0822) for Initial Access, and Connection Proxy technique (T0884) for Command and Control. Alternatively, enhancing the monitoring parameters of system files would increase the perceivability of techniques such as Data from Information Repositories technique (T0811) for Collection and the Service Stop technique (T0881) for Inhibit Response Function.

Comprehension can be further enhanced by technique artifacts created when adversaries employ certain attack techniques. The CyOTE program provides organizations with a library of observables reported in each historical case. The library can be used in conjunction with a repository of artifacts, data sources, and technique detection references for practitioners and developers to support the comprehension of indicators of attack.

2.2. BACKGROUND ON THE ATTACK

The Maroochy Shire cyber attack in Queensland, Australia was a targeted intrusion against the Maroochy Shire Council's (MSC) sewerage equipment control system that took place in 2000. The adversary was a former engineer for Hunter Watertech Pty Ltd. (HWT), the firm that installed and configured MSC's radio-controlled Supervisory Control and Data Acquisition (SCADA) system. Between January and April 2000, the individual used stolen HWT equipment to access and communicate with the system.[1]

The unauthorized commands issued using these devices caused numerous faults in MSC's sewage control system, ultimately leading to an overflow of 211,337 gallons of untreated sewage in March, polluting over 500 meters of open drain in a residential area before flowing into a tidal canal.[2] MSC spent $176,000 AUD ($102,813 USD) in repairs, monitoring, clean-up, and extra security. HWT reportedly spent more than $500,000 AUD ($292,084 USD) rectifying the incident.[3]

A timeline of adversarial techniques is shown in Figure 2. The timeline includes the estimated number of days prior to and after the triggering event. The timeline after the triggering event includes the assessed victim comprehension timeline.

The adversary served as the site supervisor for HWT on the MSC SCADA installation project from late 1997 until 3 December 1999, when he resigned after a disagreement with HWT. After his resignation, he applied for a job with MSC, who turned him down in January 2000.[4]

The intrusion timeline began later that month (D-20) when the adversary caused MSC's newly installed SCADA system to begin experiencing anomalous faults, such as loss of communication, loss of pump control, false alarms, and altered pumping station configurations.[5] MSC suspected it was faults within the SCADA system and brought HWT back on site to reinstall and do a thorough check of the system. This failed to solve the faults, and because there was no logging system, HWT engineers had limited visibility into what was occurring.[6]

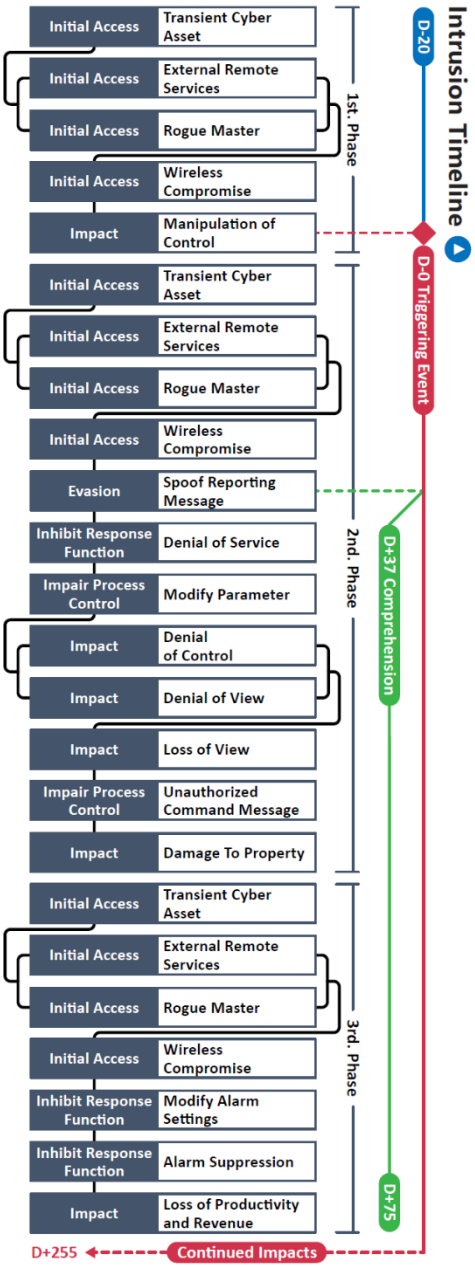


Figure 2. Intrusion Timeline

In early February (D-0), HWT installed a logging program to monitor and record all signals, messages, and traffic on the radio network.[7] After nearly two months of unexplained faults, on 16 March (D+37) HWT engineers confirmed the faults were caused by human intervention rather than equipment failure, though at that point were unable to identify the individual responsible.[8]

System faults increased in frequency and severity and the central computer was unable to exercise proper control. MSC resorted to mobilizing field workers to operate pumps manually, an insufficient workaround that resulted in the aforementioned sewage overflow on 26 March (D+47), which in turn incurred significant financial expense for the cleanup.[9]

On 23 April (D+75), the adversary disabled alarms at four pumping stations and suppressed alarm reporting to the central computer.[10] At around 10:00 PM that night, police pulled over the suspected adversary's car near one of MSC's radio repeater stations. In the car, police found a Protective Distribution System (PDS) Compact 500 remote terminal unit (RTU), a two-way radio, a laptop, a transformer, and cables to connect the equipment, all necessary to communicate with the SCADA system.[11] Until late January, the number of faults recorded never exceeded three or four per day but increased dramatically during the time the adversary accessed and manipulated the control system. Though the last intrusion occurred on 23 April (D+75), system problems had compounded to such an extent the level of faults did not return to normal until October.[12]

The Maroochy Shire cyber attack exemplifies the risk insider threats can pose to organizations' OT environments. The adversary's knowledge of the system and access to the proper equipment allowed him to disguise his actions and continue his intrusions even after the victim had comprehended a cyber attack was under way.

Analysis identified 16 unique techniques (used in a sequence of 24 steps) in a sequence and timeframe likely used by adversaries during this cyber attack (Table 1). These attack techniques are defined according to MITRE's ATT&CK® for ICS framework.

Table 1. Techniques Used in the Maroochy Shire Cyber Attack

Table 2. Precursor Analysis Report Quantitative Summary

Precursor Analysis Report Quantitative Summary	Totals
MITRE ATT&CK® for ICS Techniques	**24**
Technique Observables	**94**
Precursor Techniques	**4**
Precursor Technique Observables	**16**
Highly Perceivable Precursor Technique Observable	**3**

3. OBSERVABLE AND TECHNIQUE ANALYSIS

The following analysis may assist organizations in identifying malicious cyber activity earlier and more effectively. The following techniques and observables were compiled from publicly available sources and correlated with expert analysis.

3.1. TRANSIENT CYBER ASSET TECHNIQUE (T0864) FOR INITIAL ACCESS

The adversary gained initial access to MSC's SCADA system in late January 2000 and caused anomalous faults.[13] The adversary drove around the Maroochy Shire area with equipment, which he likely stole from HWT, to access and communicate with the SCADA system.[14] One of the stolen items was a PDS Compact 500 RTU, which was used by each of the MSC pumping stations to issue alarms, communicate with the main control room, and start or stop pump operations.[15] The other two pieces of equipment were a laptop with proprietary engineering software and a Motorola M120 two-way radio of the same type used in MSC's system.[16,17]

Support Staff personnel may have been able to observe the missing inventory. Additionally, Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites.

A total of five observables were identified with the use of the Transient Cyber Asset technique (T0864). This technique is important for investigation because physical access to cyber assets by an insider can pose serious risks to organizations and their clientele. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

Of the five observables associated with this technique, two are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 39 artifacts could be generated by the Transient Cyber Asset technique
Technique Observers[a]	Support Staff, Engineering, OT Staff, Management

[a] Observer titles are adapted from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster. CyOTE products utilize these job categories rather than organizational titles to both support comprehensive analysis and preserve anonymity within the victim organization. A complete list of potential observers can be found in Appendix C.

3.2. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

The proprietary software, PDSCONFIG,[18] developed by HWT and installed on the laptop the adversary used, was required to communicate remotely with the MSC SCADA system.[19] Engineering and OT staff used the software to access, run, and change configurations of the PDS Compact 500 RTUs in the sewerage system.[20,21] The adversary used the software to connect with the stolen PDS Compact 500 RTU which would then communicate with the central computer via radio link.[22] He made configuration changes to RTUs in the field and issued commands to sewerage stations via radio.[23]

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. If MSC's system had logging capabilities at this point in the timeline, Engineering, OT Cybersecurity, Support Staff, and IT Cybersecurity personnel may have been able to observe anomalous radio communication with the central computer.

A total of four observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it provides a point of initial access to an organization's network from external locations. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

None of the observables associated with this technique are assessed to be highly perceivable. Observables are listed in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.3. ROGUE MASTER TECHNIQUE (T0848) FOR INITIAL ACCESS

Once the adversary established a connection to the stolen PDS Compact 500 RTU with the laptop, he used the proprietary software to configure falsified network addresses on the RTU. The adversary sent false data and instructions to pumping stations with the falsified network addresses via either Distributed Network Protocol 3 (DNP3) or Modbus communication protocols, both of which could be used by this particular RTU, over radio.[24,25] By impersonating a legitimate RTU in the MSC system, the adversary avoided detection for some time.

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. If MSC's system had logging capabilities at this point in the timeline, Engineering, OT Cybersecurity, Support Staff, and IT Cybersecurity personnel may have also been able to observe the anomalous data, instructions, and radio traffic sent from the rogue master.

A total of three observables were identified with the use of the Rogue Master technique (T0848). This technique is important for investigation because impersonating a master may allow the adversary to avoid detection and is a mechanism by which an adversary can gain access to an organization's network. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

Of the three observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 11 artifacts could be generated by the Rogue Master technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.4. WIRELESS COMPROMISE TECHNIQUE (T0860) FOR INITIAL ACCESS

The MSC sewerage SCADA system consisted of 142 sewage pumping stations with two monitoring computers utilizing three radio frequencies. Each pumping station contained a PDS Compact 500 RTU capable of receiving instructions from the central control center, transmitting alarm signals and other data to the central computer, and providing messages to stop and start the pumps at the pumping station. Communications between each pumping station and between a pumping station and the central computer were by means of a dedicated (i.e., private) analog two-way radio system operating through repeater stations, each of which transmitted on a different frequency.[26] In a standard SCADA system, the control of all pumping stations can be done through the main SCADA station, which is located in the control room, or through one of the pumping station access points.[27] To communicate with the MSC control system, the adversary drove around issuing commands to pumping stations using an ultra-high frequency (UHF) Motorola M120 two-way radio tuned to the frequencies of the Buderim and Mount Coolum repeater stations.[28]

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near the Buderim and Mount Coolum repeater stations. If MSC's system had logging capabilities at this point in the timeline, Engineering, OT Cybersecurity, Support Staff, and IT Cybersecurity personnel may have also been able to observe the anomalous commands issued over radio to pumping stations.

A total of four observables were identified with the use of the Wireless Compromise technique (T0860). This technique is important for investigation because an adversary can use radio communications to issue commands to a control system. This technique appears at the beginning of the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent operational damage.

None of the observables associated with this technique are assessed to be highly perceivable. Observables are listed in in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the Wireless Compromise technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.5. MANIPULATION OF CONTROL TECHNIQUE (T0831) FOR IMPACT

The previous initial access techniques allowed the adversary to manipulate MSC's control systems in late January 2000, causing faults that included unexplained pump station alarms, increased radio traffic resulting in communication failures, modified configuration settings of pump station software, pumps running continually or turning off unexpectedly, pump stations locking up, and pumps turning off without any alarms.[29] At this time MSC suspected the new SCADA system was experiencing installation issues. HWT came back on site to reinstall and thoroughly check the system and verified it was operating properly, but this did not correct the faults.[30] System operators physically inspected various pipes and valves at pumping stations and found nothing. Except for simple messages such as "pump running" or "tank full," HWT and MSC engineers had little visibility into what was happening in the system because the system did not have logging capabilities.[31] In early February, HWT installed a program to log more information, including control messages and radio traffic.[32]

With a logging system now in place, Engineering, OT Staff, Management, and Support Staff personnel were able to observe increased radio traffic, anomalies in pump station alarms and control system configuration settings, and the anomalous states of controlled processes. OT Cybersecurity and IT Cybersecurity personnel may also have been able to observe these anomalies.

A total of eight observables were identified with the use of the Manipulation of Control technique (T0831). This technique is important for investigation because adversaries use it to negatively impact sensitive processes. Although it occurs early in the timeline, it represents the triggering event for this case study, as it is the point at which the victim initiated an investigation into the anomalous faults in its control system. Responding to this technique will effectively halt all future events. Terminating the chain of techniques at this point would limit operational damage.

Of the eight observables associated with this technique, six are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Manipulation of Control technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.6. TRANSIENT CYBER ASSET TECHNIQUE (T0864) FOR INITIAL ACCESS

In early March 2000, the adversary once again drove near operational sites with the equipment necessary to communicate with and gain access to MSC's control system.[33] Refer to the first instance of the Transient Cyber Asset technique (T0864) for details regarding the equipment.

Support Staff personnel may have been able to observe the missing inventory. Additionally, Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites.

A total of five observables were identified with the use of the Transient Cyber Asset technique (T0864). This technique is important for investigation because physical access to cyber assets by an insider can pose serious risks to organizations and their clientele. This technique appears after the triggering event, though still early in the timeline, and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from gaining access to the control system.

Of the five observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 39 artifacts could be generated by the Transient Cyber Asset technique
Technique Observers	Support Staff, Engineering, OT Staff, Management

3.7. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

As the adversary drove around MSC operational sites, he again used the proprietary software developed by HWT to communicate remotely with the SCADA system.[34] Refer to the first instance of the External Remote Services technique (T0822) for further details.

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. Engineering, OT Staff, Management, and Support Staff personnel were able to observe anomalous radio communication with the central computer. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of four observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it provides a point of initial access to an organization's network from external locations. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from gaining remote access to the control system.

Of the four observables associated with this technique, one is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.8. ROGUE MASTER TECHNIQUE (T0848) FOR INITIAL ACCESS

In early March 2000, the adversary again used the Rogue Master technique (T0848) in conjunction with the Transient Cyber Asset (T0864) and External Remote Services (T0822) techniques to access the MSC system and impersonate a legitimate RTU. At this point in the timeline, the adversary configured the PDS Compact 500 RTU he had stolen to transmit messages that identified it as pumping station 14.[35] This configuration led investigators to believe that pumping station 14 was the source of the signals that were causing faults in the system.[36] After physically checking the pumping station and determining it was working properly, engineers changed the identification of pumping station 14 to 3 so that any messages coming from station 14 would be identified as illegitimate.[37] With data logging capabilities now in place, it became apparent that the SCADA system was receiving radio traffic from a pumping station that did not exist.[38]

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. Engineering, OT Staff, Management, and Support Staff personnel were able to observe the anomalous radio traffic and commands issued by an illegitimate pumping station. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of five observables were identified with the use of the Rogue Master technique (T0848). This technique is important for investigation because impersonating a master may allow the adversary to avoid detection and is one of the mechanisms by which an adversary can gain access to an organization's network. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from sending commands to the control system and prevent operational damage.

Of the five observables associated with this technique, four are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 11 artifacts could be generated by the Rogue Master technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.9. WIRELESS COMPROMISE TECHNIQUE (T0860) FOR INITIAL ACCESS

As the adversary drove around MSC operational sites in March, he again used a UHF Motorola M120 two-way radio set to the frequencies of the Buderim and Mount Coolum repeater stations to issue commands to pumping stations.[39] Refer to the first instance of the Wireless Compromise technique (T0860) for further details.

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near the Buderim and Mount Coolum repeater stations. Engineering, OT Staff, Management, and Support Staff personnel were able to observe anomalous commands issued over radio to pumping stations in the logging system. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of four observables were identified with the use of the Wireless Compromise technique (T0860). This technique is important for investigation because the adversary can use radio communications to issue commands to the control system. This technique appears early in the timeline and responding to it will effectively halt all future events. Terminating the chain of techniques at this point would prevent the adversary from issuing commands to the control system and limit operational damage.

Of the four observables associated with this technique, three are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the Wireless Compromise technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.10. SPOOF REPORTING MESSAGE TECHNIQUE (T0856) FOR EVASION

On 16 March, the adversary spoofed reporting messages by causing faults in the MSC system that included false alarms from pumping stations and alarms failing to report to the monitoring system.[40] As noted in the second instance of the Rogue Master technique (T0848), he sent commands from the spoofed pumping station 14 address. A HWT investigator was temporarily successful in disabling the adversary's access to the system; however, the adversary changed his PDS Compact 500 RTU ID to that of pumping station 1 to regain access and continued spoofing alarm reporting messages. It was at this point in the timeline that HWT and MSC comprehended that a deliberate cyber attack was under way.[41]

The adversary's knowledge of the system allowed him to disguise his actions for a considerable amount of time. Nearly two months of troubleshooting occurred before HWT investigators considered malicious intent.[42]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the false alarms and anomalous radio traffic. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of four observables were identified with the use of the Spoof Reporting Message technique (T0856). This technique is important for investigation because it can allow an adversary to evade detection. Failure of alarms to report to the monitoring system allows operators to believe certain processes are operating normally while false alarms can cause operators to believe errors are occurring, distracting them from the actual source of the problem. This technique appears near the middle of the timeline and responding to it will prevent the adversary from evading detection. Terminating the chain of techniques at this point would limit operational damage.

All four of the observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 19 artifacts could be generated by the Spoof Reporting Message technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.11. DENIAL OF SERVICE TECHNIQUE (T0814) FOR INHIBIT RESPONSE FUNCTION

As the faults in the MSC system continued to occur, a HWT investigator communicated over the control system network with the illegitimate pump station 14 that was sending messages to corrupt the system. He was temporarily able to alter the system, so it excluded the spoofed messages. However, the adversary then removed the investigator's access to the network for a short period of time.[43]

Engineering, OT Staff, and Support Staff personnel were able to observe that the network was temporarily inaccessible. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe this anomaly.

A total of two observables were identified with the use of the Denial of Service technique (T0814). This technique is important for investigation because it can cause devices to be unable to send and receive requests so they may not perform expected response functions in reaction to other events in the environment. This technique appears near the middle of the timeline and responding to it will give defenders the ability to react to adversarial actions. Terminating the chain of techniques at this point would limit operational damage.

Both observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 14 artifacts could be generated by the Denial of Service technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Support Staff, IT Cybersecurity

3.12. MODIFY PARAMETER TECHNIQUE (T0836) FOR IMPAIR PROCESS CONTROL

Further problems occurred in MSC's control system when the adversary modified parameters by altering electronic signals with the stolen PDS Compact 500 RTU, causing erratic pump operations.[44] The adversary altered data so functions that should have occurred at affected pumping stations did not occur or occurred in unintended ways, such as stopping pumps.[45] OT staff were able to identify the illegitimate information with the logging system but were unable to stop the intrusion.[46]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the anomalies in pumping station operations. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

One observable was identified with the use of the Modify Parameter technique (T0836). This technique is important for investigation because modified systems and process critical parameters may be turned into dangerous, out-of-bounds, or unexpected values, leading to impact to equipment and/or control processes. This technique appears in the middle of the timeline and responding to it will prevent the adversary from causing the control system to operate in an unintended state. Terminating the chain of techniques at this point would limit operational damage.

The observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 18 artifacts could be generated by the Modify Parameter technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.13. DENIAL OF CONTROL TECHNIQUE (T0813) FOR IMPACT

As the faults increased in frequency and severity, the SCADA system was unable to exercise proper control.[47] HWT engineers again lost access to the network, preventing them from issuing any commands to the control system.[48]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the loss of access to and failure of commands to reach the control system. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of two observables were identified with the use of the Denial of Control technique (T0813). This technique is important for investigation because it can prevent operators and engineers from interacting with process controls causing the affected process to operate in an undesired state. This technique appears in the middle of the timeline and responding to it will allow defenders to regain control of the system. Terminating the chain of techniques at this point would limit operational damage.

Both of the observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of eight artifacts could be generated by the Denial of Control technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.14. DENIAL OF VIEW TECHNIQUE (T0815) FOR IMPACT

At the same time engineers and operators experienced the Denial of Control technique (T0813), the control center lost communications with various pumping stations.[49] The loss of communication prevented engineers and operators from viewing the state or behavior of the system.[50]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the loss of communication between the supervisory control station and pumping stations. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe this anomaly.

A total of three observables were identified with the use of the Denial of View technique (T0815). This technique is important for investigation because it can disrupt and prevent operator oversight on the status of the ICS environment. This technique appears in the latter half of the timeline and responding to it will allow defenders to regain visibility into the status of the system. Terminating the chain of techniques at this point would limit operational damage.

All three observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of four artifacts could be generated by the Denial of View technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.15. LOSS OF VIEW TECHNIQUE (T0829) FOR IMPACT

The intermittent loss of communication and control resulted in a more sustained loss of visibility into the sewage control system. MSC resorted to mobilizing field workers throughout the system to operate the pumps manually at affected pumping stations.[51]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the sustained loss of view of the control process, resulting in manual operation in the field. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of seven observables were identified with the use of the Loss of View technique (T0829). This technique is important for investigation because an adversary can effectively hide the present state of operations leading to potentially costly hands-on operator intervention. This technique appears in the latter half of the timeline and responding to it will allow defenders to regain visibility into the system. Terminating the chain of techniques at this point would limit operational damage.

All observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of four artifacts could be generated by the Loss of View technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.16. UNAUTHORIZED COMMAND MESSAGE TECHNIQUE (T0855) FOR IMPAIR PROCESS CONTROL

With access to the MSC SCADA system, the adversary was able to issue radio commands to RTUs at different pumping stations to cause anomalous pump behaviors. This affected the transport, control, and storage of sewage in the system, resulting in a mass imbalance for the plant.[52] Faults that occurred were similar to those MSC experienced prior to comprehension of the cyber attack and included pumps running when they should not, pumps not running when they should, loss of communication between pumping stations and the control center, and pump station lockups.[53]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe anomalous radio traffic resulting in communication failures and the anomalous pump behaviors. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of eight observables were identified with the use of the Unauthorized Command Message technique (T0855). This technique is important for investigation because it is the mechanism by which adversaries can instruct control system assets to perform actions outside of their intended functionality. This technique appears in the latter half of the timeline and responding to it will prevent the adversary from performing any actions that may cause an impact to physical processes. Terminating the chain of techniques at this point would limit operational damage.

Of the eight observables associated with this technique, seven are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Unauthorized Command Message technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.17. DAMAGE TO PROPERTY TECHNIQUE (T0879) FOR IMPACT

As mentioned in the Loss of View technique (T0829) section, MSC resorted to mobilizing field workers to operate pumps manually. On 26 March 2000, this costly workaround proved insufficient, causing the Boomba Street pumping station in Pacific Paradise to fail, releasing 211,337 gallons of untreated sewage into the community.[54,55,56] The raw sewage flowed into tidal canals and polluted over 500 meters of open drain and creek, affecting local parks, rivers, and the grounds of a local hotel. This resulted in harm to marine life and produced a sickening stench from the community's rivers.[57]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the overflow of untreated sewage and an increase in complaints from local citizens. OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have also been able to observe these impacts.

A total of two observables were identified with the use of the Damage to Property technique (T0879). This technique is important for investigation because it can represent tangible damage from other techniques used in an attack and has the potential to lead to loss of safety. This technique appears late in the timeline and responding to it would only limit the severity of physical damage. At this point in the timeline, most of the operational damage has been inflicted. Terminating the chain of techniques at this point would limit further impacts the adversary might seek to cause.

Both observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 18 artifacts could be generated by the Damage to Property technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity, IT Staff

3.18. TRANSIENT CYBER ASSET TECHNIQUE (T0864) FOR INITIAL ACCESS

On 23 April 2000 just after 7:30 PM, the adversary once again drove near operational sites with the equipment necessary to communicate with and gain access to MSC's control system.[58] Refer to the first instance of the Transient Cyber Asset technique (T0864) for details regarding the equipment.

Support Staff personnel may have been able to observe the missing inventory. Additionally, Engineering, OT Staff, and Management personnel may have been able to observe the presence of the adversary's vehicle near operational sites.

A total of five observables were identified with the use of the Transient Cyber Asset technique (T0864). This technique is important for investigation because physical access to cyber assets by an insider can pose serious risks to organizations and their clientele. This instance of the technique appears late in the timeline, beyond the point at which a defender could prevent operational damage. Terminating the chain of techniques at this point would limit further impacts the adversary might seek to cause.

All five observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 39 artifacts could be generated by the Transient Cyber Asset technique
Technique Observers	Support Staff, Engineering, OT Staff, Management

3.19. EXTERNAL REMOTE SERVICES TECHNIQUE (T0822) FOR INITIAL ACCESS

As the adversary drove around MSC operational sites, he again used the proprietary software developed by HWT on the laptop to communicate remotely with the SCADA system.[59] The adversary used the laptop to run the software file (Pdsconf.exe) at least 31 times prior to 19 April 2000, and last ran it on 23 April.[60] Refer to the first instance of the External Remote Services technique (T0822) for further details.

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. Engineering, OT Staff, Management, and Support Staff personnel were able to observe anomalous radio communication with the central computer. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of four observables were identified with the use of the External Remote Services technique (T0822). This technique is important for investigation because it provides a point of initial access to an organization's network from external locations. This instance of the technique appears late in the timeline, beyond the point at which a defender could prevent operational damage. Terminating the chain of techniques at this point would limit further impacts the adversary sought to cause.

Of the four observables associated with this technique, two are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the External Remote Services technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.20. ROGUE MASTER TECHNIQUE (T0848) FOR INITIAL ACCESS

The adversary again used the Rogue Master technique (T0848) in conjunction with the Transient Cyber Asset (T0864) and External Remote Services (T0822) techniques to impersonate a legitimate RTU in the MSC system. At this point in the timeline, the adversary configured the PDS Compact 500 RTU in his possession to transmit messages that identified itself as pumping station 4.[61]

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near operational sites. Engineering, OT Staff, Management, and Support Staff personnel were able to observe the anomalous radio traffic and commands issued by an illegitimate pumping station. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of three observables were identified with the use of the Rogue Master technique (T0848). This technique is important for investigation because impersonating a master may allow the adversary to avoid detection and is one of the mechanisms by which an adversary can gain access to an organization's network. This instance of the technique appears late in the timeline, beyond the point at which a defender could prevent operational damage. Terminating the chain of techniques at this point would limit further impacts the adversary might seek to cause.

All three observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 11 artifacts could be generated by the Rogue Master technique
Technique Observers	Engineering, OT Staff, Management, OT Cybersecurity, Support Staff, IT Cybersecurity

3.21. WIRELESS COMPROMISE TECHNIQUE (T0860) FOR INITIAL ACCESS

As the adversary drove around MSC operational sites, he again used the UHF Motorola M120 two-way radio set to the frequencies of the Buderim and Mount Coolum repeater stations to issue commands to pumping stations.[62] The adversary drove around the area on at least 46 occasions between 28 February and 23 April 2000, issuing radio commands to the sewerage equipment.[63] Refer to the first instance of the Wireless Compromise technique (T0860) for further details.

Engineering, OT Staff, Management, and Support Staff personnel may have been able to observe the presence of the adversary's vehicle near the Buderim and Mount Coolum repeater stations. Engineering, OT Staff, Management, and Support Staff personnel were able to observe anomalous commands issued over radio to pumping stations in the logging system. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of four observables were identified with the use of the Wireless Compromise technique (T0860). This technique is important for investigation because it is a method of gaining communications and unauthorized access to a wireless network. This instance of the technique appears late in the timeline, beyond the point at which a defender could prevent operational damage. Terminating the chain of techniques at this point would limit further impacts the adversary might seek to cause.

All four observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 28 artifacts could be generated by the Wireless Compromise technique
Technique Observers	Engineering, OT Staff, Management OT Cybersecurity, Support Staff, IT Cybersecurity

3.22. MODIFY ALARM SETTINGS TECHNIQUE (T0838) FOR INHIBIT RESPONSE FUNCTION

Between 7:30 PM and 9:00 PM on 23 April 2000, the adversary used the PDS Compact 500 RTU, identifying itself as pumping station 4, and proprietary software to access the SCADA system, disable alarms at four pumping stations, and override messages to or from the control center.[64] This caused alarms to not be reported to the central computer.[65]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the overridden alarm messages. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe this anomaly.

One observable was identified with the use of the Modify Alarm Settings technique (T0838). This technique is important for investigation because overriding reporting messages may prevent operators from responding to dangerous or unintended scenarios. This technique appears near the end of the timeline, beyond the point at which a defender could prevent operational damage. Terminating the chain of techniques at this point would limit further impacts.

The observable associated with this technique is assessed to be highly perceivable. It is italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 16 artifacts could be generated by the Modify Alarm Settings technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.23. ALARM SUPPRESSION TECHNIQUE (T0878) FOR INHIBIT RESPONSE FUNCTION

In addition to modifying alarm settings, the adversary suppressed alarm reporting to the central computer.[66] This prevented outgoing alarms from being raised and incoming alarms from being responded to. The adversary's intrusions concluded around 9:00 PM on 23 April 2000. Between 9:00 PM and 10:00 PM, MSC notified police of the adversary's presence near repeater stations. As a result, an all-points bulletin was issued, and police apprehended the adversary around 10:00 PM that night.[67]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the anomalous radio traffic and the mismatch in controlled process operating state and reported state. OT Cybersecurity and IT Cybersecurity personnel may have also been able to observe these anomalies.

A total of three observables were identified with the use of the Alarm Suppression technique (T0878). This technique is important for investigation because adversaries may target protection function alarms to prevent them from notifying operators of critical conditions. This technique appears near the end of the timeline, beyond the point at which a defender could take action to disrupt the attack.

All three observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of 13 artifacts could be generated by the Alarm Suppression technique
Technique Observers	Engineering, OT Staff, OT Cybersecurity, Management, Support Staff, IT Cybersecurity

3.24. LOSS OF PRODUCTIVITY AND REVENUE TECHNIQUE (T0828) FOR IMPACT

The Maroochy Shire cyber attack cost MSC $176,000 AUD ($201,813 USD) in repairs, monitoring, clean-up, and extra security. HWT spent an additional $500,000 AUD ($292,084 USD) to rectify the incident.[68] The adversary was able to gain access to and manipulate MSC's control system during a span of 95 days. This case exemplifies the risk malicious insiders from third party contractors can pose to an organization. Until late January, the number of faults recorded in the system never exceeded three or four per day, but the faults increased dramatically as intrusions were made. The faults caused by the adversary compounded problems in the MSC sewerage control system to such an extent that it was not until October that the number of faults returned to normal.[69]

Engineering, OT Staff, Management, and Support Staff personnel were able to observe the loss of productivity and revenue. OT Cybersecurity, IT Cybersecurity, and IT Staff personnel may have also been able to observe these anomalies.

A total of three observables were identified with the use of the Loss of Productivity and Revenue technique (T0828). This technique is important for investigation because it demonstrates the impact adversaries can cause by degrading the availability and integrity of control system operations, devices, and related processes. This technique appears at the end of the timeline, beyond the point at which a defender could take action to disrupt the attack.

All three observables associated with this technique are assessed to be highly perceivable. They are italicized and marked † in Appendix A.

CyOTE Capabilities for Technique Perception and Comprehension	
Artifacts (See Appendix B)	A total of five artifacts could be generated by the Loss of Productivity and Revenue technique
Technique Observers	Engineering, OT Staff, Management, Support Staff, OT Cybersecurity, IT Cybersecurity, IT Staff

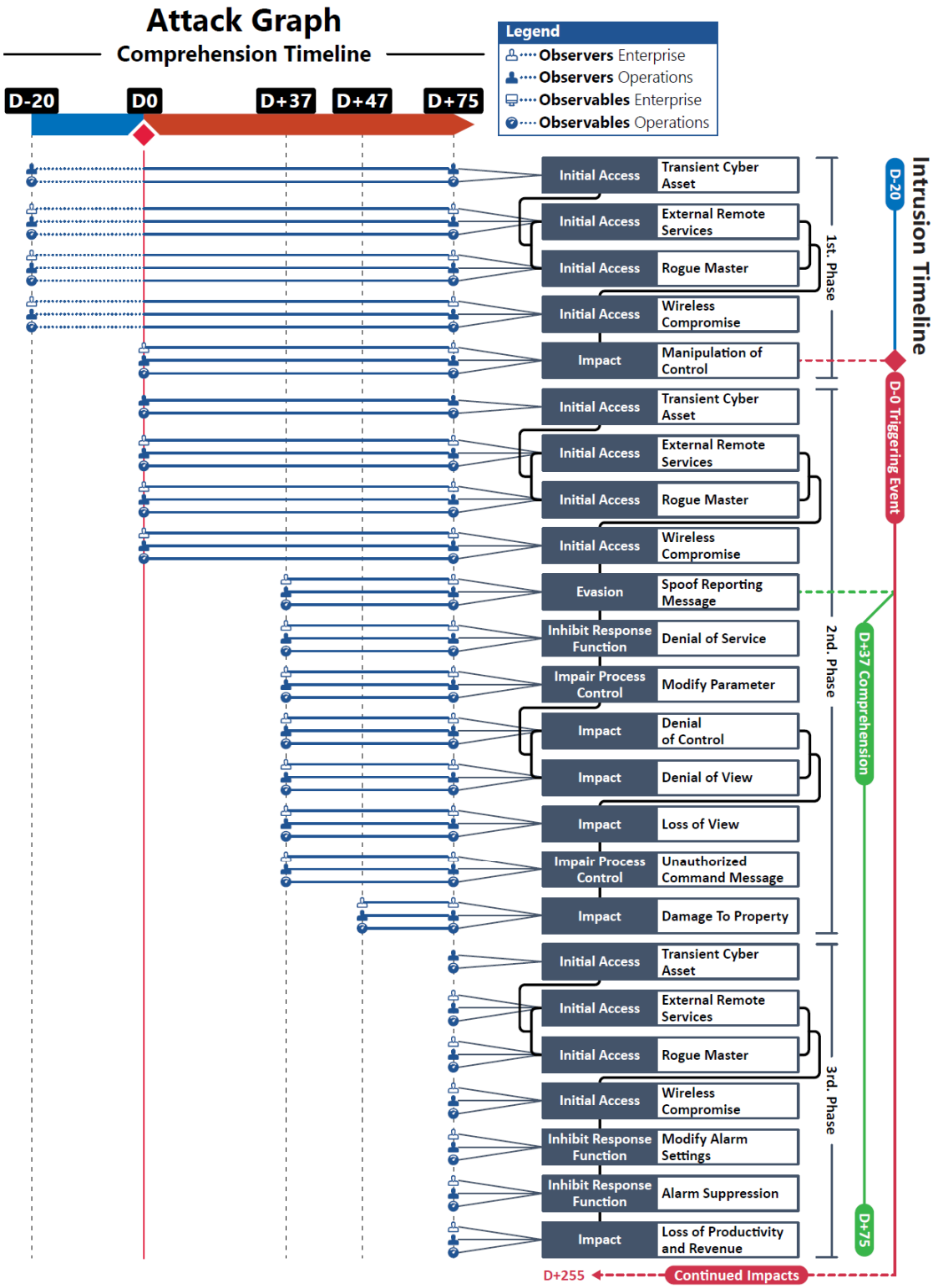


Figure 3. Attack Graph

APPENDIX A: OBSERVABLES LIBRARY

NOTE: Highly perceivable observables are italicized and marked †

Observables Associated with Transient Cyber Asset Technique (T0864)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2 †	*Missing Assets: Operational Technology (OT): Motorola M120 Two-Way Radio*
Observable 3 †	*Missing Assets: Operational Technology (OT): Protective Distribution System (PDS) Compact 500 Remote Terminal Unit (RTU)*
Observable 4	Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech
Observable 5	Anomalous Configuration Changes: to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500

Observables Associated with External Remote Services Technique (T0822)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2	Anomalous Configuration Changes: to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500: by Proprietary Controller Software: PDSCONFIG
Observable 3	Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech
Observable 4	Presence of Proprietary Software on Transient Asset: Laptop: Pdsconf.exe

Observables Associated with Rogue Master Technique (T0848)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2	Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech
Observable 3 †	*Anomalous Radio Traffic: from Anomalous Pumping Station Network Address*

Observables Associated with Wireless Compromise Technique (T0860)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2	Anomalous Radio Traffic: to Repeater Station: Buderim
Observable 3	Anomalous Radio Traffic: to Repeater Station: Mount Coolum
Observable 4	Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech

Observables Associated with Manipulation of Control Technique (T0831)	
Observable 1	Anomalous Increase in Radio Traffic: Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech
Observable 2 †	*Anomalous Pump Station Alarms*
Observable 3 †	*Anomalous Interruption of Communication: From Supervisory Control to Controlled Process: Sewage Pumping Stations: Alarm Monitoring Communication*
Observable 4	Anomalous Modification of Control System Software: Pumping Station Software
Observable 5 †	*Controlled Process in Anomalous State: Pumps Continually Running*
Observable 6 †	*Controlled Process in Anomalous State: Pumps Shut Off*
Observable 7 †	*Controlled Process in Anomalous State: Pumps Shut Off Without Alarms*
Observable 8 †	*Controlled Process in Anomalous State: Pump Station Lockups*

Observables Associated with Transient Cyber Asset Technique (T0864)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2 †	*Missing Assets: Operational Technology (OT): Motorola M120 Two-Way Radio*
Observable 3 †	*Missing Assets: Operational Technology (OT): Protective Distribution System (PDS) Compact 500 Remote Terminal Unit (RTU)*
Observable 4 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 5 †	*Anomalous Configuration Changes to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500*

Observables Associated with External Remote Services Technique (T0822)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2	Anomalous Configuration Changes: to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500: by Proprietary Controller Software: PDSCONFIG
Observable 3 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 4	Presence of Proprietary Software on Transient Asset: Laptop: Pdsconf.exe

Observables Associated with Rogue Master Technique (T0848)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 3 †	*Anomalous Radio Traffic: from Anomalous Pumping Station Network Address: Pumping Station 14*
Observable 4 †	*Controlled Process in Anomalous State*
Observable 5 †	*Anomalous Maintenance Ticket: Diagnostic Test of Control Process: Pumping Station: Diagnostic Test Passed*

Observables Associated with Wireless Compromise Technique (T0860)	
Observable 1	Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations
Observable 2 †	*Anomalous Radio Traffic: to Repeater Station: Buderim*
Observable 3 †	*Anomalous Radio Traffic: to Repeater Station: Mount Coolum*
Observable 4 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*

Observables Associated with Spoof Reporting Message Technique (T0856)	
Observable 1 †	*Anomalous Radio Traffic: from Anomalous Pumping Station Network Address: from Pumping Station 14: to Unspecified Pumping Stations*

Observables Associated with Spoof Reporting Message Technique (T0856)	
Observable 2 †	*Anomalous Radio Traffic: from Anomalous Pumping Station Network Address: from Pumping Station 1: to Unspecified Pumping Stations*
Observable 3 †	*Anomalous False Alarms*
Observable 4 †	*Failure of Alarms to Reach Supervisory Control System*

Observables Associated with Denial of Service Technique (T0814)	
Observable 1 †	*Loss of Access to Control System: Supervisory Control System*
Observable 2 †	*Failure of Commands to Reach Control System: Supervisory Control System*

Observables Associated with Modify Parameter Technique (T0836)	
Observable 1 †	*Control Process in Anomalous State: Anomalies in Pump Operations: Stoppage of Pumps*

Observables Associated with Denial of Control Technique (T0813)	
Observable 1 †	*Loss of Access to Control System: Supervisory Control System*
Observable 2 †	*Failure of Commands to Reach Control System: Supervisory Control System*

Observables Associated with Denial of View Technique (T0815)	
Observable 1 †	*Anomalous Temporary Loss of View: of Control Process: at Supervisory Control Station: of Pumping Stations*
Observable 2 †	*Anomalous Increase in Logon Failures: Observed on Network*
Observable 3 †	*Anomalous Increase in Logon Failures: Observed on Host*

Observables Associated with Loss of View Technique (T0829)	
Observable 1 †	*Sustained Anomalous Loss of View: of Control Process: at Supervisory Control Station: of Pumping Stations*
Observable 2 †	*Anomalous Sustained Logon Failures: Observed on Network*
Observable 3 †	*Anomalous Sustained Logon Failures: Observed on Host*
Observable 4 †	*Controlled Process Operating in Degraded State: Pumping Stations*
Observable 5 †	*Creation of Anomalous Maintenance Ticket: for Manual Operation: of Pumping Stations*
Observable 6 †	*Creation of Anomalous Maintenance Ticket: for Loss of View: of Supervisory Control Station*
Observable 7 †	*Controlled Process Operating in Degraded State: Manual Operation of Pumping Stations*

Observables Associated with Unauthorized Command Message Technique (T0855)	
Observable 1 †	*Anomalous Increase in Radio Traffic: Over Ultra High Frequency (UHF): from Anomalous Source: to Controlled Process: Pumping Stations*
Observable 2 †	*Anomalous Communication Failures: from Supervisory Control Station: to Remote Terminal Units (RTU): Pumping Stations*
Observable 3 †	*Anomalous Radio Commands: Over Ultra High Frequency (UHF): to Remote Terminal Units (RTU): Pumping Stations*
Observable 4	Anomalous Function Code Distribution
Observable 5 †	*Controlled Process Operating in a Degraded State: Continual Running of Pumps*
Observable 6 †	*Controlled Process Operating in a Degraded State: Pump Stoppage*
Observable 7 †	*Controlled Process Operating in a Degraded State: Pump Station Lockups*
Observable 8 †	*Controlled Process Operating in a Degraded State: Loss of Communication with Supervisory Control Station*

Observables Associated with Damage to Property Technique (T0879)	
Observable 1 †	*Controlled Process Failure: Pumping Station: at Boomba Street: Overflow of Untreated Sewage: 211,337 Gallons: into Surrounding Area: Open Drain and Creek*
Observable 2 †	*Anomalous Raw Sewage Smell in the Community: Increase in Complaints: to Maroochy Shire Council*

Observables Associated with Transient Cyber Asset Technique (T0864)	
Observable 1 †	*Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations*
Observable 2 †	*Missing Assets: Operational Technology (OT): Motorola M120 Two-Way Radio*
Observable 3 †	*Missing Assets: Operational Technology (OT): Protective Distribution System (PDS) Compact 500 Remote Terminal Unit (RTU)*
Observable 4 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 5 †	*Anomalous Configuration Changes to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500*

Observables Associated with External Remote Services Technique (T0822)	
Observable 1 †	*Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations*

Observables Associated with External Remote Services Technique (T0822)	
Observable 2	Anomalous Configuration Changes: to Controlled Process: Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500: by Proprietary Controller Software: PDSCONFIG
Observable 3 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 4	Presence of Proprietary Software on Transient Asset: Laptop: Pdsconf.exe

Observables Associated with Rogue Master Technique (T0848)	
Observable 1 †	*Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations*
Observable 2 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*
Observable 3 †	*Anomalous Radio Traffic: from Anomalous Pumping Station Network Address: Pumping Station 4*

Observables Associated with Wireless Compromise Technique (T0860)	
Observable 1 †	*Presence of Anomalous Vehicle: Owned by Former Employee: Containing Transient Cyber Assets: Protective Distribution System (PDS) Compact 500, Motorola M120 Two-Way Radio, Laptop, Cable Media, and Transformer: Near Operational Sites: Radio Repeater Stations*
Observable 2 †	*Anomalous Radio Traffic: to Repeater Station: Buderim*
Observable 3 †	*Anomalous Radio Traffic: to Repeater Station: Mount Coolum*
Observable 4 †	*Anomalous Commands Issued to Controlled Process: Sewage Pumping Stations: via Radio: Over Ultra High Frequency (UHF): Motorola M120 Two-Way Radio: Property of Integrator: Hunter Watertech*

Observables Associated with Modify Alarm Settings Technique (T0838)	
Observable 1 †	*Supervisory Control System Receives Anomalous Messages: Alarms Disabled: by Remote Terminal Unit (RTU): Protective Distribution System (PDS) Compact 500: from Anomalous Pumping Station ID: Pumping Station 4*

Observables Associated with Alarm Suppression Technique (T0878)	
Observable 1 †	*Anomalous Increase in Radio Traffic: Over Ultra High Frequency (UHF): from Anomalous Pumping Station ID: Pumping Station 4*
Observable 2 †	*Controlled Process Operating State Does Not Match Reported State: Anomalous State Not Reported: to Supervisory Control Station*

Observables Associated with Alarm Suppression Technique (T0878)	
Observable 3 †	*Anomalous Override of Command Messages: from Supervisory Control Station: to Remote Terminal Units (RTU): Protective Distribution System (PDS) Compact 500: at Pumping Stations*

Observables Associated with Loss of Productivity and Revenue Technique (T0828)	
Observable 1 †	*Anomalous Loss of Productivity: 95 Days*
Observable 2 †	*Anomalous Loss of Revenue: $292,084 USD for Hunter Watertech*
Observable 3 †	*Anomalous Loss of Revenue: $102,813 USD for Maroochy Shire City Council*

APPENDIX B: ARTIFACTS LIBRARY

Artifacts Associated with Transient Cyber Asset Technique (T0864)	
Artifact 1	TFTP Port
Artifact 2	Telnet Traffic
Artifact 3	RDP Traffic Port
Artifact 4	VNC Traffic Port
Artifact 5	SSH Traffic Port
Artifact 6	Network Discover Protocols
Artifact 7	.lnk File
Artifact 8	Media Transfer Protocol (MTP) Connections
Artifact 9	MAC Address
Artifact 10	Picture Transfer Protocol (PTP) Connections
Artifact 11	Mass Storage Class (MSC) Connections
Artifact 12	FTPS Port
Artifact 13	USB Version
Artifact 14	Changes to System Registry SYSTEM\MOUNTEDDEVICES
Artifact 15	USB Model
Artifact 16	DNS Queries Traffic
Artifact 17	USB Make
Artifact 18	HTTP Port
Artifact 19	HTTPS Port
Artifact 20	ARP Connections
Artifact 21	USB Serial Number
Artifact 22	First Time Device Connected
Artifact 23	User Agents
Artifact 24	Honey Pot Logs
Artifact 25	Network Connections with Honeypot
Artifact 26	Security Log Attempt to Access Removable Storage Object Event
Artifact 27	System Log Plug and Play Driver Installed Event
Artifact 28	Plug and Play Log File setupapi.log
Artifact 29	Changes to System Registry SYSTEM\CURRENTCONTROLSET\ENUM\USBSTOR
Artifact 30	Device Disconnected Time
Artifact 31	Drive Letter Creation

Artifacts Associated with Transient Cyber Asset Technique (T0864)	
Artifact 32	Source IP Address
Artifact 33	Last Time Device Connected
Artifact 34	Device User
Artifact 35	Security Log Failure to Access Removeable Device
Artifact 36	Bytes Received From
Artifact 37	Bytes Sent from System Resource Usage Manager
Artifact 38	FTP Port
Artifact 39	Wireless Transmission

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 1	Remote Session Key
Artifact 2	User Account Creation
Artifact 3	Remote Vendor Connections
Artifact 4	Session Authentication
Artifact 5	Failed Logon s Event
Artifact 6	Session Timestamp
Artifact 7	Logon Event Type
Artifact 8	Remote Services Protocols
Artifact 9	Logon Event Type
Artifact 10	VPN Connections
Artifact 11	System Registry Network Interfaces
Artifact 12	Remote Services Logon
Artifact 13	TLS Certificate
Artifact 14	Session Logoff Event
Artifact 15	Blocked Incoming Connections Event
Artifact 16	Logon Event Type
Artifact 17	User Privileges Change
Artifact 18	Encrypted Network Traffic
Artifact 19	Blocked Incoming Packet Event
Artifact 20	External IP Address
Artifact 21	Security Account Manager Registry Password Hashes
Artifact 22	Command Prompt Window Opened
Artifact 23	Dialog Box Pop-Up

Artifacts Associated with External Remote Services Technique (T0822)	
Artifact 24	Security Account Manager Registry Entries
Artifact 25	User Client Address
Artifact 26	User Account Name
Artifact 27	Domain Controller Log
Artifact 28	Mouse Movement

Artifacts Associated with Rogue Master Technique (T0848)	
Artifact 1	Application Logon Event
Artifact 2	Operational Application Log
Artifact 3	Operational Data Creation
Artifact 4	Operational Event Logs
Artifact 5	Process State Changes
Artifact 6	MAC Addresses
Artifact 7	Process Failures
Artifact 8	Process Timing Changes
Artifact 9	IP Addresses
Artifact 10	Process Alarm
Artifact 11	Command Packets

Artifacts Associated with Wireless Compromise Technique (T0860)	
Artifact 1	HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\ WINDOWSNT\CURRENTVERSION\NETWORKLIST\
Artifact 2	Wireless Network Logoff
Artifact 3	Program File Manipulation
Artifact 4	Process State Change
Artifact 5	Wireless Key Deauthorization
Artifact 6	Wireless Network Logon
Artifact 7	Controlled Device State Change
Artifact 8	Remote Network Traffic
Artifact 9	Wireless Connections
Artifact 10	Radio Connections
Artifact 11	Registry Changes for Network Connections
Artifact 12	Sender IP Address

Artifacts Associated with Wireless Compromise Technique (T0860)	
Artifact 13	Vendor Proprietary Protocol Use
Artifact 14	Host Inserts Packets
Artifact 15	Receiver IP Address
Artifact 16	Controlled Device Alarm
Artifact 17	Network Packet Metadata Change
Artifact 18	Common Network Traffic
Artifact 19	SSID Created in Registry
Artifact 20	Network Connection Reconfigured
Artifact 21	Controlled Device Failure
Artifact 22	Geolocation of Router in Registry
Artifact 23	Controlled Device Manipulation
Artifact 24	Logon Event
Artifact 25	Logoff Event
Artifact 26	User Account Information
Artifact 27	Controlled Device Reboot
Artifact 28	Industrial Network Traffic

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 1	Controller Set Point Change
Artifact 2	Event Log Creation
Artifact 3	Process Restart
Artifact 4	Process Shutdown
Artifact 5	Process State Change
Artifact 6	Process Initiated
Artifact 7	Controller Tag Change
Artifact 8	Controller Parameter Change
Artifact 9	I/O Modification
Artifact 10	Operational Data Modification
Artifact 11	Application File Modification
Artifact 12	Application Log Event
Artifact 13	Command Execution
Artifact 14	HMI Input Manipulation
Artifact 15	Altered Command Sequences

Artifacts Associated with Manipulation of Control Technique (T0831)	
Artifact 16	Engineering Workstation Mouse Movement

Artifacts Associated with Spoof Reporting Message Technique (T0856)	
Artifact 1	Control Device Increased Maintenance
Artifact 2	Mismatch of Process State with Controller Reports
Artifact 3	.dll File Creation
Artifact 4	Host Inserts Packets
Artifact 5	Radio Connections
Artifact 6	Wireless Connections
Artifact 7	Remote Network Traffic
Artifact 8	Industrial Network Traffic
Artifact 9	Application Log Event
Artifact 10	Receiver IP Address
Artifact 11	Alarm Failure
Artifact 12	Common Network Traffic
Artifact 13	Sender IP Address
Artifact 14	Application Modification
Artifact 15	Network Connection Reconfigured
Artifact 16	Network Traffic Filtered
Artifact 17	Host Denial of Service
Artifact 18	Network Flooding Traffic
Artifact 19	Control Device Failure

Artifacts Associated with Denial of Service Technique (T0814)	
Artifact 1	MAC Addresses
Artifact 2	ICMP Echo Port 7 Traffic Increase
Artifact 3	Application Failure
Artifact 4	Operational Data Corruption
Artifact 5	Application Log
Artifact 6	External Network Connections
Artifact 7	IP Addresses
Artifact 8	Network Traffic Connection Increase

Artifacts Associated with Denial of Service Technique (T0814)	
Artifact 9	Services Failure
Artifact 10	Ransom Notice
Artifact 11	Low Resources Warning
Artifact 12	Increase Industrial Protocol Exceptions
Artifact 13	TDS Traffic Increase Port
Artifact 14	Process Performance Degrades

Artifacts Associated with Modify Parameter Technique (T0836)	
Artifact 1	Device Set Points Changed
Artifact 2	Device Alert
Artifact 3	Device Failure
Artifact 4	Process Performance Degradation
Artifact 5	Application Log Events
Artifact 6	Machine State Change
Artifact 7	Industrial Protocol Packets
Artifact 8	Project File Changes
Artifact 9	Configuration Changes
Artifact 10	Non-Standard Application Calls
Artifact 11	New Software Installed
Artifact 12	Nonstandard Service Creation
Artifact 13	Process Creation
Artifact 14	.dll Changes
Artifact 15	Driver Modifications
Artifact 16	Alert Failure
Artifact 17	Network Traffic
Artifact 18	Remote GUI Manipulation

Artifacts Associated with Denial of Control Technique (T0813)	
Artifact 1	Network Ports Closed
Artifact 2	Input Failure
Artifact 3	Process Nonresponsive
Artifact 4	Network Ports Opened

Artifacts Associated with Denial of Control Technique (T0813)	
Artifact 5	Serial Communication Failure
Artifact 6	Process Reboot
Artifact 7	Process Failure
Artifact 8	Increased Network Packet Delivery

Artifacts Associated with Denial of View Technique (T0815)	
Artifact 1	Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application
Artifact 2	File System Modification Artifacts Might Be Associated with The Denial of View Might Be Present on Disk
Artifact 3	Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification
Artifact 4	Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness

Artifacts Associated with Loss of View Technique (T0829)	
Artifact 1	Blocking Communications Paths and Channels (Comms, Network Infrastructure, Host Packet Routing) Might Occur via an OS or Device Modification
Artifact 2	Masked Reconfiguration of Alarm Thresholds or Other Configuration Settings Might Result in Unexpected Lack of Situational Awareness
Artifact 3	File System Modification Artifacts Might Be Associated with The Loss of View Attack Might Be Present on Disk
Artifact 4	Application Logic Hooks or Modifications Might Prevent Proper Reporting to/from an Industrial Application

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 1	MAC Addresses
Artifact 2	Application Level I/O Manipulation
Artifact 3	Process Alarm Event
Artifact 4	Process Alarm
Artifact 5	Operational Data Created
Artifact 6	OS Level I/O Manipulation
Artifact 7	IP Addresses
Artifact 8	Operational Application Log

Artifacts Associated with Unauthorized Command Message Technique (T0855)	
Artifact 9	Process Logic Change
Artifact 10	Protocol Specific Command Packet
Artifact 11	Machine State Change
Artifact 12	Process Restart
Artifact 13	Process Failure
Artifact 14	Network Resets
Artifact 15	Protocol Metadata Change
Artifact 16	Process Timing Change

Artifacts Associated with Damage to Property Technique (T0879)	
Artifact 1	Pressure Relief
Artifact 2	Reduction In Traffic Volume to Device
Artifact 3	Frequent Maintenance Failures
Artifact 4	Damage to Property Due to Equipment Degradation
Artifact 5	Damage to Property Due to Malicious Network Traffic
Artifact 6	Breakers Closing and Opening Rapidly
Artifact 7	Safety Systems Engaged
Artifact 8	Increase In Connecting Errors to Device
Artifact 9	Loud Vibrations
Artifact 10	Liquid Spills
Artifact 11	Damage to Property Due to Equipment Malfunction
Artifact 12	Catastrophic Failure
Artifact 13	Surges In Power
Artifact 14	Ladder Logic Configuration Changes
Artifact 15	Industrial Network Traffic
Artifact 16	Smoke
Artifact 17	Process Trip
Artifact 18	Alarms

Artifacts Associated with Modify Alarm Settings Technique (T0838)	
Artifact 1	User Logs
Artifact 2	Network Traffic

Artifacts Associated with Modify Alarm Settings Technique (T0838)	
Artifact 3	Mismatch Between System Status and Physical Process
Artifact 4	Alarm Failures
Artifact 5	Alert Failures
Artifact 6	Application Logs
Artifact 7	Dialog Box Creation
Artifact 8	Configuration Changes
Artifact 9	False Positive Reporting
Artifact 10	System Operating Outside of Parameters
Artifact 11	Increase In Vendor Support Sessions
Artifact 12	Increase In Maintenance Reports
Artifact 13	Device Failure
Artifact 14	False Negative Reporting
Artifact 15	Dangerous Physical Changes
Artifact 16	Operational Data Performance Degradation

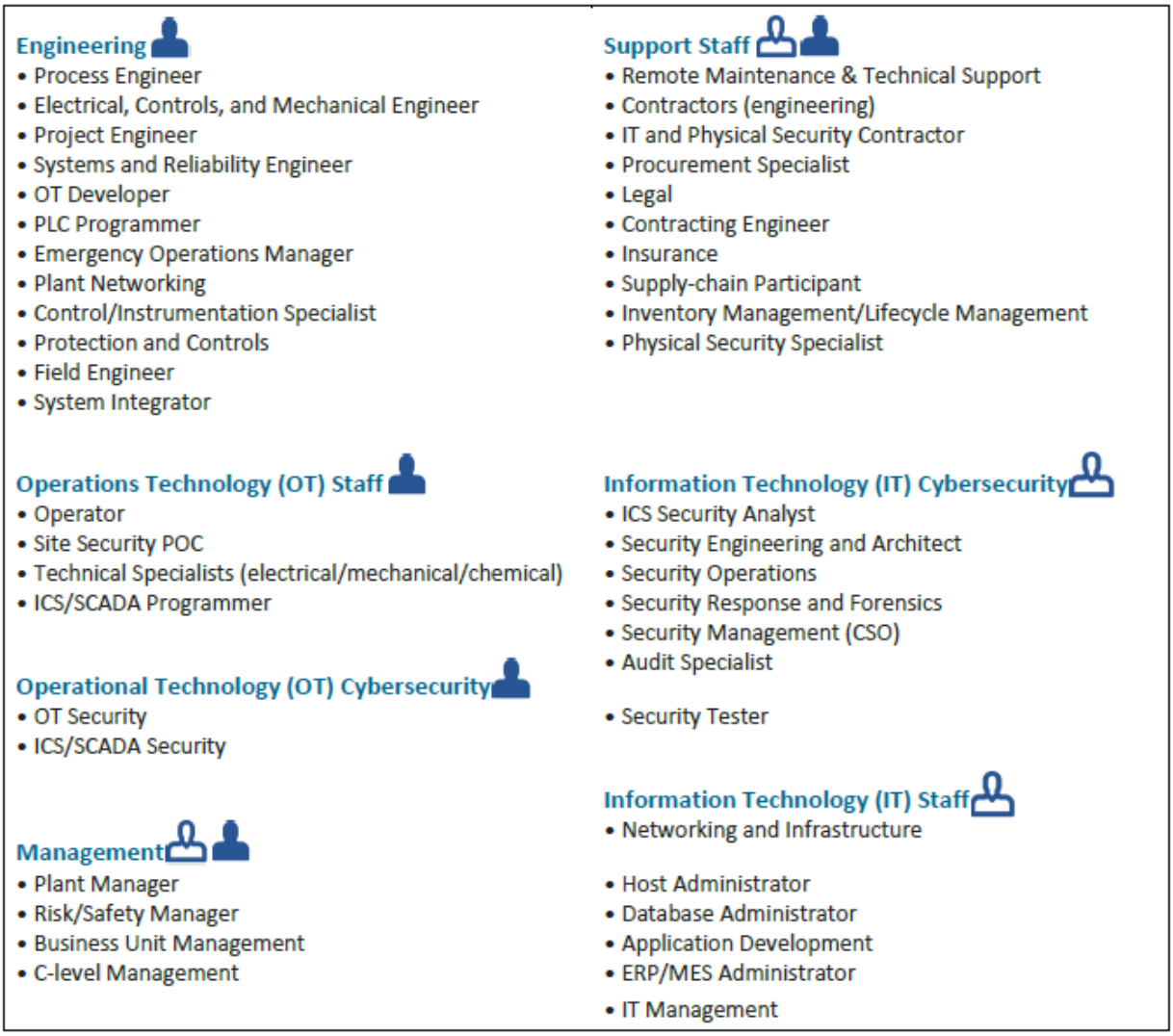
Artifacts Associated with Alarm Suppression Technique (T0878)	
Artifact 1	Change in Process Output
Artifact 2	Modification of Alarm Set Points
Artifact 3	Runaway Process State
Artifact 4	Catastrophic Failures
Artifact 5	Configuration Change Logs
Artifact 6	Increased Number of Output Quality Assurance Failures
Artifact 7	Insertion of Malicious Industrial Protocol to Suppress True Process Values
Artifact 8	Modification of SQL Database Inputs
Artifact 9	SQL Protocol Network Traffic
Artifact 10	Mismatch Between Sensor Reporting and Physical Process
Artifact 11	Increased Maintenance Issues
Artifact 12	Control System Degradation
Artifact 13	External Connection to Operational Database

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 1	Loss of Confidence in a Safety System Due to Unreliability Might Result In a Risk Management Driven Shutdown of a Plant

Artifacts Associated with Loss of Productivity and Revenue Technique (T0828)	
Artifact 2	Wormable or Other Highly Propagating Malware Might Result in The Shutdown of a Plant to Prevent Ransomware or Other Destructive Attacks
Artifact 3	Extortion Attempts Might Lead to Reduced Operations Due to Potential Presence of Malicious Attackers
Artifact 4	Loss of Control of Critical Systems Due to Ransomware or Loss of Confidence Might Lead to a Degraded Productivity or Revenue Operating State
Artifact 5	File System Modification Artifacts Might Be Associated with The Loss of Productivity and Revenue Attack Might Be Present on Disk

APPENDIX C: OBSERVERS

This is a collection of standardized potential observers that work in operational technology organizations. It has been slightly modified by the CyOTE team from the Job Role Groupings listed in the SANS ICS Job Role to Competency Level Poster to communicate the categories of potential observers during cyber events.



REFERENCES

[1] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[2] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[3] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[4] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[5] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[6] [Institution of Electrical Engineers (IEE) Computing & Control Engineering | Steve Mustard | “Security of Distributed Control Systems: the Concern Increases” | https://dokumen.tips/documents/security-of-distributed-control-systems-the-concern-increases.html?page=1 | February 2006 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[7] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[8] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[9] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[10] [The MITRE Corporation | Marshall D. Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://www.acsac.org/2008/program/case-studies/Abrams.pdf | December 2008 | Accessed on 2 August 2022 | The source is publicly available information and does not contain classification markings]

[11] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[12] [Institution of Electrical Engineers (IEE) Computing & Control Engineering | Steve Mustard | “Security of Distributed Control Systems: the Concern Increases” | https://dokumen.tips/documents/security-of-distributed-control-systems-the-concern-increases.html?page=1 | February 2006 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[13] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[14] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[15] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[16] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[17] [The MITRE Corporation | Marshall D. Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://www.acsac.org/2008/program/case-studies/Abrams.pdf | December 2008 | Accessed on 2 August 2022 | The source is publicly available information and does not contain classification markings]

[18] [Angelfire | Vitek Boden | “Vitek Boden V ‘Queen’” | https://vitekboden.angelfire.com/index.html | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[19] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[20] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[21] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[22] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[23] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[24] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[25] [Institute of Electrical and Electronics Engineers (IEEE) | Dimitrios Pliatsios, and others | “A Survey on SCADA Systems: Secure Protocols, Incidents, Threats and Tactics” | https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9066892 | 2020 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[26] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[27] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[28] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[29] [International Conference on Critical Infrastructure Protection | Jill Slay and Michael Miller | “Lessons Learned from the Maroochy Water Breach” | https://link.springer.com/content/pdf/10.1007/978-0-387-75462-8_6.pdf | 2008 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[30] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[31] [Institution of Electrical Engineers (IEE) Computing & Control Engineering | Steve Mustard | “Security of Distributed Control Systems: the Concern Increases” | https://dokumen.tips/documents/security-of-distributed-control-systems-the-concern-increases.html?page=1 | February 2006 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[32] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[33] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[34] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[35] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[36] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[37] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[38] [Institution of Electrical Engineers (IEE) Computing & Control Engineering | Steve Mustard | “Security of Distributed Control Systems: the Concern Increases” | https://dokumen.tips/documents/security-of-distributed-control-systems-the-concern-increases.html?page=1 | February 2006 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[39] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[40] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[41] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[42] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[43] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[44] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[45] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[46] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[47] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[48] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[49] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf |

23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[50] [MITRE ATT&CK | “Denial of View” | https://attack.mitre.org/techniques/T0815/ | 20 October 2022 | Accessed on 27 October 2022 | The source is publicly available information and does not contain classification markings]

[51] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[52] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[53] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[54] [Angelfire | Vitek Boden | “Vitek Boden V ‘Queen’” | https://vitekboden.angelfire.com/index.html | Accessed on 17 August 2022 | The source is publicly available information and does not contain classification markings]

[55] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[56] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[57] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[58] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[59] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[60] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[61] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[62] [Supreme Court of Queensland | “R v Boden [2002] QCA 164” | https://archive.sclqld.org.au/qjudgment/2002/QCA02-164.pdf | 10 May 2002 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]

[63] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[64] [International Conference on Human Aspects of Information Security, Privacy, and Trust | Hao Wang, Nathan Lau, and Ryan Gerdes | “Application of Work Domain Analysis for Cybersecurity” | https://link.springer.com/chapter/10.1007/978-3-319-58460-7_27 | 13 May 2017 | Accessed on 21 September 2022 | The source is publicly available information and does not contain classification markings]

[65] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[66] [The MITRE Corporation | Marshall Abrams and Joe Weiss | “Malicious Control System Cyber Security Attack Case Study – Maroochy Water Services, Australia” | https://apps.dtic.mil/sti/pdfs/AD1107275.pdf | 23 July 2008 | Accessed on 26 July 2022 | The source is publicly available information and does not contain classification markings]

[67] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[68] [Massachusetts Institute of Technology | Nabil Sayfayn and Stuart Madnick | “Cybersafety Analysis of the Maroochy Shire Sewage Spill” | https://web.mit.edu/smadnick/www/wp/2017-09.pdf | May 2017 | Accessed on 1 August 2022 | The source is publicly available information and does not contain classification markings]

[69] [Institution of Electrical Engineers (IEE) Computing & Control Engineering | Steve Mustard | “Security of Distributed Control Systems: the Concern Increases” | https://dokumen.tips/documents/security-of-distributed-control-systems-the-concern-increases.html?page=1 | February 2006 | Accessed on 27 July 2022 | The source is publicly available information and does not contain classification markings]