# Autonomous security countermeasure plan for power systems

The Maritime (semi-) Autonomous Systems for Mine Countermeasures (MAS MCM) will deliver a world-class mix of (semi-) autonomous underwater, surface and aerial technologies and capabilities for maritime mine countermeasures for future acquisition with a focus on interoperability between systems.

In this paper, we focus on the security of complex networks such as BGP, exploiting network redundancy (multiple routes between most source/destination pairs) and trading off evolvability (how quickly new routes are incorporated into the network) to provide more autonomous security for the autonomous systems of the Internet. 2. Background

However, with the rapid advancement of technology, a new era of autonomous mine countermeasure systems has emerged, promising safer and more efficient operations. At the forefront of this revolution is the MAGNUSS Project, a cutting-edge initiative that aims to push the boundaries of autonomous mine countermeasure technology.

Thales and MHI (Mitsubishi Heavy Industries) have entered into a partnership to develop a dual-frequency sonar demonstrator for mine countermeasures that will be installed on an Autonomous Underwater Vehicle (AUV). The project follows an agreement between the defence procurement agencies of France and Japan. Dealing with the threat of mines ...

for malicious actors threatening the security of the AEVs and their applications, potentially resulting in accidents, injuries, property/infrastructure damages, even taking human lives. In this paper, we analyze emerging power electronics security challenges and propose a novel preliminary countermeasure

The ViSE digital twin platform provides the means to explore, optimize, and evaluate a range of security objectives, with system-level coordination playing a vital role in multiple use cases. While it is possible to abstract the details of vehicular components (beyond the necessary comprehension for the given use cases), vehicular communications, in ...

Magnetic sensor technologies are being developed at NAVSEA, Coastal Systems Station to enhance the ability of Autonomous Underwater Vehicles (AUVs) to perform detection, localization and classification (DLC) of mines for mine countermeasures in Surf Zone/Very Shallow Water (SZ/VSW) environments. This work involves the design, development, and ...

Following the M& S CoE participated to the meeting of the 136 Specialist Team of the Information System Technology (IST), another STO panel regarding Security Challenges for Multi-domain Autonomous and Unmanned C4ISR Systems . During the workshop was given by the CoE representative the contributes to the

team regarding the SIRI experience and in ...

Mines are one of the most cost-effective and moderated weapon systems that are easy to deploy, but difficult to clear. Not only has the development of the mine countermeasure (MCM) underwater unmanned vehicle (UUV) improved cost- and time-effectiveness in operation, but also it has avoided unnecessary human casualties.

The Uncrewed & Autonomous Systems degree offers courses that examine major challenges found when dealing with uncrewed systems technology such as: ... Propulsion and Power; Teaming and Regulation; Uncrewed & Autonomous Systems Career Opportunities Careers and Employers ... Cybersecurity and Countermeasure Considerations: 3: UNSY 325: Uncrewed ...

2.1 Sensing and World State Identification. Definition: Sensing and World state identification is the AICA"s high-level function that allows a cyber-defense agent to acquire data from the environment and systems in which it operates as well as from itself in order to reach an understanding of the current state of the world and, should it detect risks in it, to trigger the ...

Space & Naval Warfare Systems Center, San Diego Page 3 of 9 Undersea Networked Acoustic Communication and Navigation for Autonomous Mine-Countermeasure Systems Figure 6 (left). A radio/acoustic communication (racom) buoy equipped with line-of-sight Freewave digital packet radio. Photo courtesy of Ken Rogers, SPAWAR Systems Center, San Diego.

The proposed approach uses the Failure, Attack and Countermeasure (FACT) graph to connect safety failures, security attacks, and the associated countermeasures and is helpful for designing or tailoring the safety and security processes, and selecting appropriate countermeasures for autonomous vehicles taking into consideration the driving automation levels. --Safety is the ...

4 o Unlike the International Space Station (ISS), Astronauts will only occupy the Gateway occasionally. o NASA wants to develop autonomous operations for long periods of time (~days) . o Due to the availability of the deep space network, there will be periodic communication losses from Earth to the Gateway. o Therefore, advanced autonomous control strategies will be ...

2.1 Safety risk assessment standards. Safety is an important issue that affects process industries. IEC 61508 [] defines the safe failure fraction (SFF) and the safety integrity level (SIL) to confirm the degree of safety-related system fail-safe, and it sets out a risk-based approach for deciding the SIL for systems performing safety functions.. Whereas IEC 61508 is ...

2.1 Safety risk assessment standards. Safety is an important issue that affects process industries. IEC 61508 [] defines the safe failure fraction (SFF) and the safety integrity level (SIL) to confirm the degree of safety-related ...

# Autonomous security countermeasure plan for power systems

To identify and mitigate the security risks involved in AV holistically, in this chapter, we provide a comprehensive taxonomy for attack surfaces and countermeasures for defense. Specifically, four different attack surfaces are defined, namely ECUs, sensors, intra-vehicular links, and inter-vehicular links.

represent the line power flows in forward and backward directions, respectively. Matrix AT DA (i.e., multiplication of AT and DA) represents power consumption at the buses. The state estimated solution (from Equation (1)) provides the estimate of bus voltages from which the system power-flows can be computed. Summing up the net power flows

6)Finally, in the last step, security countermeasures are added to the model and their relationships are established. Similarly to matrices X-A and X-B from the previous step, two new matrices Z-A and Z-B are added to dene the coverage of attacks and failures by security countermeasures. The security countermeasures, added in this step, could ...

Scoring CAPAs by Countermeasure level is called an Input Metric or a Leading Indicator. Input metric = scoring system using Countermeasure Ladder. The team"s CAPAs are measured with scores and the feedback provided helps move it further up in the ladder. The examples shared in the six levels of Countermeasure Ladder with typical CAPAs are at ...

The selection of safety and security countermeasures for autonomous vehicles depends on the driving automation levels, defined by the international standard SAE J3016. ... such as, power plants or water treatment systems, they face some unique challenges, which have to be taken into consideration when analyzing their safety and security ...

The Cyber-Physical Systems (CPS) attacks and vulnerabilities are increasing and the consequences of such attacks can be catastrophic. The CPS needs to be self-resilient to cyber-attacks through a precise autonomous and timely risk mitigation model that can analyze and assess the risk of the CPS and apply a proper response strategy against the ongoing ...