Securing Navigation of Unmanned Maritime Systems

Tope Omitola
Cyber-Physical Systems Research Group
Electronics and Computer Science, University of Southampton
t.omitola@ecs.soton.ac.uk
Jon Downes
Fluid Structure Interactions
School of Engineering, University of Southampton
jon.downes@soton.ac.uk
Gary Wills
Cyber-Physical Systems Research Group
Electronics and Computer Science, University of Southampton
gbw@ecs.soton.ac.uk
Mark Zwolinski
Sustainable Electronic Technologies Group
Electronics and Computer Science, University of Southampton
mz@ecs.soton.ac.uk
Michael Butler
Cyber-Physical Systems Research Group
Electronics and Computer Science, University of Southampton
mjb@ecs.soton.ac.uk

Abstract

Unmanned Maritime Systems (UMS), such as Unmanned Surface Vehicles (USVs), are increasingly playing a critical role in expanding the undersea superiority of a nation, addressing growing challenges, such as, inter alia, in piracy, natural resource disputes, drug trafficking, weapons proliferation, as well as being highly used for science and survey missions. Autonomous capabilities in USVs can reduce the costs of reaching into distant environments and using that reach to meet a particular mission's objectives. However, to take on increased autonomy in unmanned systems, USVs will increasingly require the ability to be untethered from human interaction, and a key enabler to effecting this is accurate navigation. USVs have traditionally depended on Global Navigation Satellite Systems (GNSS), which are known to have security and safety vulnerabilites. Using systems-theoretic process analysis (STPA), this paper provides systematic analyses of the attack surfaces and of the impact of cyber attacks against the navigational aspects of Unmanned Surface Vehicles. As part of these analyses, we identify

In: S. M. Schillai, N. Townsend (eds.): Proceedings of the International Robotic Sailing Conference 2018, Southampton, United Kingdom, 31-08-2018

potential threats, vulnerabilities and attacks in the Positioning, Navigation and Timing (PNT) functionalities of USVs. These analyses can be used to drive a USV's architecture, leading to the design of more effective and secure USV operations.

1 Introduction

Over 90% of information, people, goods and services flow across the worlds oceans (Navy,). Protecting a country's residents and economic prosperity is, therefore, essential and dependent on the ability to persistently monitor ocean surface and sub-surface activities, in order to identify, classify and mitigate emerging threats. Unmanned Maritime Systems (UMS), such as Unmanned Surface Vehicles (USVs), are increasingly playing a critical role in expanding the surface and underwater superiority of a nation, and addressing growing challenges, such as, inter alia, in piracy, natural resource disputes, drug trafficking and weapons proliferation. USVs are also employed in other areas of economic life, such as (a) Maritime search and rescue, (b) Hydrologic surveys, (c) Port surveillance, (d) Underwater Inspection, (e) Naval Defence, and their greater use could save the global marine industry up to £80 billion per annum by "potential reductions in capital costs, manning costs and fuel costs" (Rolls-Royce,).

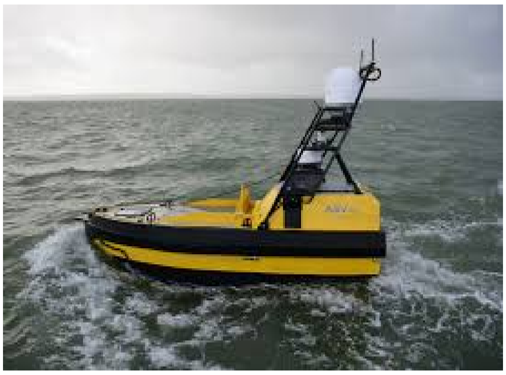

Figure 1: ASV C-Worker USV from asvglobal.com

Because of their position at the air-sea interface, USVs have the ability to relay radio frequency transmissions in air and acoustic transmissions undersea. Thus they are a key piece in the vision of networked maritime space, both in defence and civil. Figure 1 shows an example commercial USV, while figure 2 shows an example of how BP is making use of UMS in its networked maritime space (the picture shows a number of USVs, e.g. C-Worker, WaveGlider and Autonaut, plus some underwater vehicles, such as the Seaglider, working together to monitor the ocean surface and the seabed).

Autonomous capabilities in USVs can reduce the costs and risks of reaching into distant environments while using that reach to meet missions' objectives. Marine vehicles are taking on higher levels of autonomy to perform unmanned missions, therefore securing their autonomous navigation and control modules becomes increasingly important.

2 Autonomy, Navigation and Control

Autonomy incorporates "systems which have a set of intelligence-based capabilities that allow it to respond to situations that were not programmed or anticipated in the design (i.e., decision-based responses). Autonomous systems have a degree of self-government and self-directed behavior (with the humans proxy for decisions)" (Air Force Research Laboratory, 2013). USVs must be capable of avoiding ships, docks, floating debris, and navigation aids must ensure that these USVs are able to avoid these obstacles and other marine assets, and remain in navigable waters. In addition, USVs must operate in accordance with collision regulations (COLREGS)[1].

[1] http://www.collisionregs.com/MSN1781.pdf

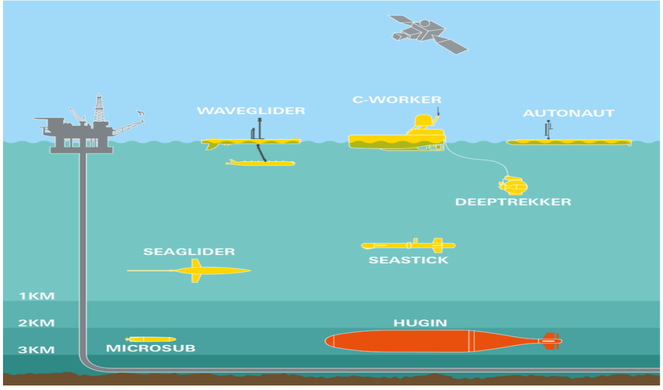

Figure 2: An example application of collection of UMS (from *"How a new robot fleet is monitoring the underwater world"* at http://www.bp.com/en/global/corporate/bp-magazine/innovations/ocean-monitoring-with-robot-technology.html)

Because not all maritime traffic (including military and commercial) always follow the COLREGS, therefore, assured autonomous navigation and control are very important to develop and maintain in USVs.

There are a wide range of definitions of autonomy depending on the field. In the maritime sector, the most widely agreed definition is given in (UK,), and has six levels. These levels are, in ascending order of autonomy:

- Level 0: Manned; Vessel/craft is controlled by operators aboard
- Level 1: Operated; Under Operated control where all cognitive functionality is within the human operator
- Level 2: Directed; Under Directed control some degree of reasoning and ability to respond is implemented into the Unmanned Vessel. However, the authority to make decisions is with the operator
- Level 3: Delegated; The Unmanned Vessel is now authorised to execute some functions. The control initiative emanates from the Unmanned Vessel and decision-making is shared between the operator and the Unmanned Vessel
- Level 4: Monitored; The Unmanned Vessel will sense environment and report its state. The operator may monitor the events, and
- Level 5: Autonomous; The Unmanned Vessel will sense environment and report its state. The operator may monitor the events.

At the very highest level, missions are specified as a series of waypoints, with functionality tags (such as profile, station keep, dock) with the vehicle attempting to maintain a straight course between waypoints. Many USVs have the capacity for real-time bidirectional communication between the control station and the USV, where the USV can have the waypoints, steering, and communication commands sent to it in near-real time.

During USV navigation, there are three main operations to carry out. These are: (a) Route Planning (waypoints' elicitation), (b) Monitoring of the Navigation, and (c) Updates to Route Planning, if and when necessary. Once the USV starts moving, locomotion along the route has to be monitored, by the USV and/or the control station, for various reasons, such as obstacle avoidance, asset detection, and changes in weather, thereby making accurate and secure navigation of these autonomous vessels essential for safety.

2.1 Navigating Autonomous Marine Vessels Safely and Securely

USVs are required to be at least as safe as the equivalent human-operated surface vessels. Some of the safety concerns for USVs that have navigation as core include: (a) their ability to avoid collisions with other marine assets, such as floating objects (e.g. bouys, etc.) or other marine vessels, (b) their ability to navigate safely in coastal areas, (c) ability to handle emergencies, such as failure recovery and repairs at sea of itself or of other marine vessels.

To be safe in its operation, a USV should endeavour not be a safety hazard to itself, other surrounding marine assets, or the maritime environment, of which it is a part. USV navigation is usually provided by the Global

Navigation Satellite Systems (GNSS), of which the General Positioning System (GPS) is a part of. Depending on the level of autonomy of the corresponding USV, successful navigation, and mission operations, require precise positioning, timing and collision avoidance. All these depend on the accuracy of the GNSS values provided to the USV.

2.2 Positioning And Navigating with Global Navigation Satellite Systems (GNSS)

Global Navigation Satellite Systems (GNSS), such as the Global Positioning System (GPS), Russia's GLONASS, the European Union's Galileo and China's COMPASS, provide important positioning, navigation and timing information to military, civilian and commercial users around the world. GNSS comprises mainly three components (Ioannides et al., 2016): (a) the User Segment, (b) the Control and Uplink Segment and (c) the Space Segment.

The Space segment consists of a constellation of operating satellites that transmit one-way signals that give the current GNSS satellite position and time. These signals are generated by the satellites' payloads that also contain one or more atomic clocks. These clocks are used to precisely time the signals and to provide good frequency reference. The navigation signals are optimised for various applications but they share a similar structure. For a given satellite, m, the transmitted signal, $s(t)$, is modelled by: $s_m(t) = \sqrt{2P_m}c_m(t)cos(2\pi f_{RF}t)$, where m denotes the satellite index, P is the transmit power, $d(t)$ the broadcast navigation message, $c(t)$ a pseudo-randomly alternating chipping sequence, t denotes time, and f_{RF} is the nominal carrier frequency.

The control segment consists of a global network of ground facilities that track the satellites, monitor their transmissions, perform analyses, and send commands and data to the constellation. As the locations of these stations are precisely known and the orbital motion of the satellites follows Kepler's laws, these data can be used to determine and predict the satellite positions. The user segment consists of the GNSS receiver equipment, which receives the signals from the GNSS satellites and uses the transmitted information to calculate the user's three-dimensional position, velocity and time. Figure 3 shows a schematic diagram of GPS showing the three segments.

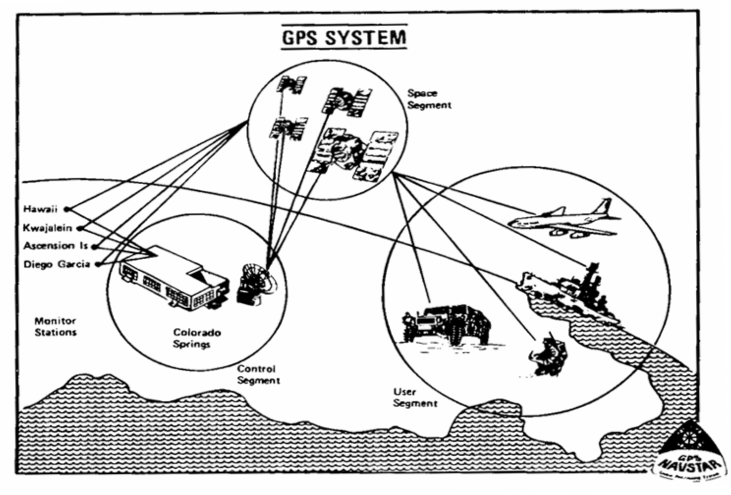

Figure 3: The Three GPS Segments, from (Humphreys, 2011)

2.3 GNSS Vulnerabilities

GNSS signals are very weak, as low as $-160dBW$, and unencrypted. As such, the system is vulnerable to unintentional and intentional interference. The result of such interference could be the complete failure of the vessel's GNSS receiver or, possibly worse, the presentation to the vehicle of hazardously misleading information for navigation and situational awareness. In general, three attack types are distinguished (Maarse, 2016): spoofing, jamming, and meaconing attacks. Meaconing is the interception and rebroadcasting of navigation signals in order to confuse navigation, while jamming is the intentional interference of the GNSS signals via the emission of radio frequency energy of sufficient power and with the proper characteristics to prevent receivers in the target area from tracking the GNSS signals. Spoofing is the broadcast of false signals with the intent that the victim receiver will misinterpret them as authentic signals. The victim might deduce a false position fix, a false clock offset, or both.

Although GNSS signal jamming has been popular in recent times, interest in GNSS spoofing has intensified of late due to successful "spoofing in the wild" that have been reported. Examples include, the Iranian military forcibly capturing a highly classified CIA drone in Dec. 2011. An Iranian engineer involved in the capture claimed that they spoofed the drone into landing in Iran when it thought it was landing at its base in Afghanistan (Rawnsley,). A scientific satellite was reported to have received spoofing-like GPS interference over Ukraine (Divis, 5 09). A yacht was spoofed deluding the receiver, causing the vessel's autopilot system and crew to navigate along a course laid out by the adversary (Bhatti and Humphreys, 7 05; **?**). Spoofing could send marine vehicles, off-course, especially in low-visibility conditions, threatening safety and security.

2.4 Safe and Secure Navigation of Unmanned Marine Systems (UMS)

The rising level of autonomy brings with it new hazards and risks that need to be handled and/or mitigated in order to enjoy its economic benefits. Due to their importance, safety and security impose constraining requirements that need to be fulfilled in the design and implementation of the navigation module of unmanned marine systems, such as USVs. Safety analysis methods, such as HAZOP (Tyler et al., 2015), work on an existing design and are ill-suited to assess the kinds of cyber-physical systems employed in UMS. Systems and system designs have become so complex that waiting until a design is completed to perform safety and security analyses on it is impractical. Even if by dint of sheer will it is possible to perform such analyses, changing the design after the fact is usually impractical (financially and intellectually). Much of this effort, therefore, goes into proving that existing designs are safe and/or secure rather than building designs that are safe from the beginning. The only hope for practical and cost-effective safe design approaches in these systems is to design safety and security in from the beginning.

Due to the interactions between the software and the physical parts of cyber-physical systems, and the ensuing emergence that are the results of these component interactions, research suggests that designing secure safety-critical systems poses a substantial challenge (Oates et al., 2013) with a view that engineering "complex embedded and cyber-physical systems requires a holistic view on both product and process" (Schlinglof, 2016). Security and safety need to be incorporated across the engineering life-cycle to ensure such systems are safe from accidents and hazards, and secure from deliberate threats.

3 Security and Hazard Analyses of the Navigation Component of Unmanned Marine Systems (UMS)

Accidents have traditionally been conceived of as occurring from a sequence of directly related failure events, each of which leads to the next event in the chain of events. Increased system complexity and interactions, and the introduction of software, are leading to new types of accidents, accidents that are more a result of inter-component interactions (and not just intra-component failures). Traditional analysis methods work with accident models that are based on the fault-error-failure chain (Avizienis et al., 2004). While these models are valid to describe failures of single components, they are insufficient to describe system failures in complex interconnected systems. Systems-Theoretic Accident Model and Processes (STAMP) (Leveson, 2004) is an accident causality model based on systems theory. It expands the traditional model of causality beyond a chain of directly-related failure events or component failures to include more complex processes and unsafe interactions among system components.

STAMP is based on the three concepts of safety constraints, a hierarchical safety control structure and process models. STAMP considers events leading to accidents occur because safety constraints were not successfully enforced. Safety constraints on a system are imposed by the laws of physics, the regulatory and organisational frameworks, the systems with which it interacts, and/or the functions it performs, and design and development decisions. System-level constraints are first identified and responsibility for enforcing them is divided and allocated. Then, during system design and development, system-level safety constraints are broken down and sub-constraints are allocated to the system components.

STAMP considers systems as hierarchical control structures where each level imposes constraints on the activity of the level beneath it. The standard control structure involves four components of Controller, the Controlled entity, Actuators and Sensors (figure 4).

The controller issues control actions implemented by actuators that affect the state of the controlled entity/process. Sensors capture changes in the state of the controlled process and transmit them to the controller

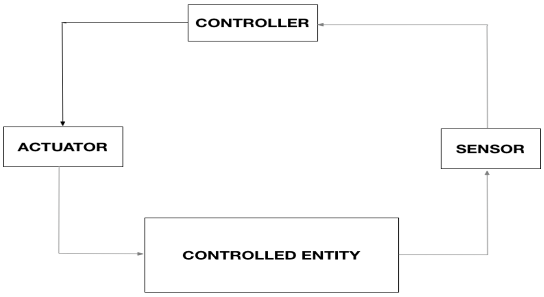

Figure 4: Standard control structure as used in STAMP

process which uses this feedback information to issue new actions to keep the controlled process in the desired safe operational state. In STAMP, the controller has a model of the controlled process. The controller maintains this model with the feedback information provided by the sensors and, based on this model, determines the control actions.

Accidents, in STAMP, are violations of safety constraints that were not adequately enforced by control actions because the model of the controlled process in the controller departs from the actual behaviour of the controlled process. This discrepancy is the source of the four possible causes of accidents: (a) A control action required for safety was not provided; (b) An unsafe control action was provided; (c) A control action required for safety was provided too early or too late or in the wrong sequence; and (d) A control action required for safety was stopped too soon or applied too long.

Based on STAMP, System Theoretic Process Analysis (STPA) (Leveson and Thomas, 2018) and STPA-Sec (Young and Leveson, 2013) were developed as new hazard analyses techniques to evaluate the safety and security of a system. STPA starts from fundamental system engineering activities, including the identification of losses or accidents to be avoided, the hazardous behaviour that could lead to these losses, safety requirements and constraints, and the basic system control structure used to avoid these losses. STPA relies on four safety related activities of system engineering, viz: (a) determination of unacceptable accidents. An accident, in STPA, is defined as “an unplanned or undesired event that result in a loss of human, human injury, property damage, environmental pollution, mission loss, etc.”; (b) determination of the system boundaries. Boundaries determine which conditions related to accidents are considered part of the system and which are considered part of the environment; (c) Identification of high-level system hazards. A hazard is a system state or a set of conditions that, together with a particular set of worst-case environmental conditions, will lead to an accident; and (d) the identification, determination and definition of system safety constraints. System safety constraints are the conditions the system itself, its organisation and its development process must fulfil to prevent hazards from occurring. STPA-Sec buttresses STPA in being used to analyse the security of systems. It changes the traditional bottom-up approach to security, where threats are used to derive the security requirements, to a top-down approach where the outcomes are more relevant.

STPA has two steps: (1) the identification of potential inadequate control actions that can lead to hazardous states; and (2) the determination of how these unsafe control actions can occur. Through these two steps, STPA and STPA-Sec help to generate detailed safety and security requirements and constraints that must be implemented in the design in order to prevent the identified unacceptable losses.

3.1 Using STPA and STPA-Sec in the Security Analyses of UMS Navigation Module

Two main steps can be identified in STPA Analysis: (1) Identification of the possible accidents in the system, of system-level hazards leading to these accidents, and of the system constraints that can prevent and/or mitigate these hazards; and (2) identification of the scenarios that could lead to these unsafe control actions. Table 1 shows the results of our applying STPA Analysis on the UMS Navigation Module, helping to discern the accidents, the system-level hazards, and the constraints of the Navigation Module (NM).

3.1.1 Identification of accidents, system-level security hazards and security constraints

In table 1, we see the accidents (A**X**) that may occur in the system, the hazards that may cause the accidents to occur (H**Y**), and the security constraints (safe control actions) (C**Z**) that can prevent or mitigate such hazards. Section 3.1.2, below, expands on and identifies the unsafe actions that may be caused by these hazards.

A1			Unavailability of the Navigation Module (NM)
	H1.1		NM receives continuous stream of un-usable GNSS signals via a jamming attack
		C1.1	NM shall assure assure the accurate and timely receipt of received GNSS signals
	H1.2		Malevolent manipulation of hardware and software layers of NM to alter GNSS data interpretation
		C1.2	NM shall guarantee the authenticity of its software and hardware components
A2			Un-authorised disclosure of GNSS information
	H2		There is un-authorised disclosure of GNSS information
		C2	NM shall assure GNSS data are disclosed only to authorised parties
A3			Received GNSS information are not genuine
	H3.1		GNSS information have been intentionally altered via a spoofing attack
		C3.1	NM shall assure assure the integrity of received GNSS signals
	H3.2		NM receives replayed GNSS signals via a meaconing attack
		C3.2	NM shall assure the integrity of received GNSS signals
	H3.3		GNSS information have been un-intentionally altered (probably due natural accident)
		C3.3	NM shall assure the integrity of received GNSS signals
A4			NM physical antennae poorly installed
	H4.1		Antennae installed position inhibits clear view of sky or clear signals from satellites
		C4.1	NM operational staff shall assure correct installation of NM's antennae
	H4.2		Antennae improperly matched to NM receiver
		C4.2	NM operational staff shall assure accurate matching of antennae to receiver
A5			Users' Psychological Error
	H5		Over-reliance of users on provided GNSS data
		C5	NM shall assure availability of other sources of accurate UMS positioning and timing data
A6			Unintentional Radio Frequency (RF) interference
	H6		Noise from nearby RF transmitters interferes with genuine GNSS signals
		C6	NM shall assure un-intentional RF interference

Table 1: Accidents, system-level security hazards and security constraints in Navigation Module of UMS

3.1.2 Identifying Unsafe Control Actions (UCA)

After the preliminary hazard analyses carried out in table 1, the next step is to use STAMP's four general categories of unsafe control actions (Leveson and Thomas, 2018) of: (a) "Not providing causes hazard", (b) "Providing causes hazard", (c) Wrong timing/ordering causes hazard", and "Stopping too soon/applying too long causes hazard", to identify the conditions under which the hazardous controls, as enumerated in table 1, could lead to system hazards.

Tables 2 and 3 present our use of STAMP to analyse some controls and outputs issued by the NM. The first column identifies the analysed control. The second column records the consequences of not providing a safe control. The third column records the consequences of providing an unsafe control (i.e. the controller allows the controlled process to perform actions in a context where hazards may occur). The fourth column records the consequences of providing a safe control too early or too late or in a wrong order. The fifth column records the consequences of stopping a safe control too soon or applying it too long. Every UCA must be traceable to one or more system-level hazards (Leveson and Thomas, 2018).

These identified unsafe control actions, with the related hazards, serve many functions. They can be used to shape early design decisions regarding the security of the system to be built. When the conditions under which a control action may be unsafe are stated, these help the engineers to perceive those instances, eliminate those instances from the system design or find ways to mitigate them. When translated into requirements, they form parts of the constraints to be enforced by the system design.

Control Action	**Not Providing Causes Hazard**	**Providing Causes Hazard**	**Wrong Time or Wrong Order Causes Hazard**	**Stopped Too Soon or Applied Too Long**
NM assures authenticity of its software & hardware components	**UCA1**: Malevolent components installed in NM [H1.2] **UCA2**: Unauthorised principals able to alter GNSS data interpretation [H1.2, H2, H3.2]	None	Same as UCA1 & UCA2	Same as UCA1 & UCA2 (Stopped Too Soon)
NM mitigates jamming attack	**UCA3**: Denial of Service attack (of GNSS data) [H1.1, H5]	None	Same as UCA3	Same as UCA3 (Stopped Too Soon)
NM provides authorised disclosure of GNSS data	**UCA4**: Un-authorised entities able to elicit USV position (information leakage) and/or able to replay GNSS information (traffic analyses). Possibility of taking control of USV & sabotage mission [H2, H3.1, H3.2] **UCA5** Tampering, i.e., deliberately destroying or corrupting data [H2, H5]	None	Same as UCA4	Same as UCA4 (Stopped Too Soon)
NM assures integrity of GNSS data	**UCA6**: Spoofing attack: Received GNSS data probably intentionally altered [H3.1, H5S] **UCA7** Meaconing attack: Received genuine GNSS data replayed back to USV after timed delay, leading to GNSS error readings [H3.2, H5]	None	Same as UCA6 & UCA7	Same as UCA6 & UCA7 (Stopped Too Soon)

Table 2: Unsafe Control Actions of the Navigation Module of UMS (1/2).

4 Conclusion and Future Work

The vast majority of global trade flows across the world's oceans. Unmanned marine systems (UMS) are increasingly being used to facilitate and secure these trade flows. The security of the autonomous navigation of these systems is becoming increasingly important. Therefore, accurate positioning, velocity, and timing (PVT) values are essential to their safe navigation. These PVT values are usually provided by the Global Navigation Satellite Systems (GNSS) signals that are received and decoded by the UMS' receivers. These signals are very weak and un-encrypted. Their accurate reception and decoding are, therefore, open to many vulnerabilities. This paper has used systems, and control, theory and STPA to analyse these vulnerabilities. We identified the major system-level security hazards and constraints, and especially of unsafe control actions. Our analyses can be used as a springboard to drive their mitigation and/or resolution, thereby helping to designing a more effective and secure UMS' navigation components.

In future work, we will extend these analyses with STPA causal scenarios, and using the Event-B (Abrial,

Control Action	Not Providing Causes Hazard	Providing Causes Hazard	Wrong Time or Wrong Order Causes Hazard	Stopped Too Soon or Applied Too Long
NM operational staff installs antennae properly	**UCA8**: Erroneous GNSS data received [H4.1, H4.2, H5]	None	Same as UCA8	Same as UCA8 (Stopped Too Soon)
NM provides additional Positional, Velocity, Timing (PVT) sources in addition to GNSS	**UCA9**: Probability of over-reliance of users on GNSS data [H5]	None	Same as UCA9	Same as UCA9 (Stopped Too Soon)
NM provides provides mitigation of unintentional RF interference	**UCA10**: Erroneous GNSS data received [H1.1, H5]	None	Same as UCA10	Same as UCA10 (Stopped Too Soon)

Table 3: Unsafe Control Actions of the Navigation Module of UMS (Table 2 contd.) (2/2).

2010) formalism, will develop a framework for security analysis for autonomous navigation of unmanned marine systems.

References

Abrial, J.-R. (2010). *Modeling in Event-B: System and Software Engineering.* Cambridge University Press.

Air Force Research Laboratory, Dayton, O. (2013). U.s. air force, autonomy science and technology strategy.

Avizienis, A., Laprie, J.-C., Randell, B., and Landwehr, C. (2004). Basic concepts and taxonomy of dependable and secure computing. In *IEEE Transactions on Dependable and Secure Computing*, volume 1, pages 11–33.

Bhatti, J. and Humphreys, T. (2017-05). Hostile control of ships via false gps signals: Demonstration and detection. *Navigation.*

Divis, D. A. (2015-09). Scientists document possible drone jamming. *Inside Unmanned Systems.*

Humphreys, T. (2011). State of the art and future trends in radionavigation. Briefing to USPTO.

Ioannides, R. T., Pany, T., and Gibbons, G. (2016). Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. In *Proceedings of the IEEE*, volume 104.

Leveson, N. (2004). A new accident model for engineering safer systems. *Safety Science*, 42(4):237–270.

Leveson, N. G. and Thomas, J. P. (2018). *STPA Handbook.*

Maarse, M. (2016). A systematic approach towards gnss receiver vulnerability analysis on remotely piloted aircraft systems.

Navy, U. S. United states navy biography. http://www.navy.mil/navydata/leadership/quotes.asp?q=253&c=6. 2018-06-28.

Oates, R., Thom, F., and Herries, G. (2013). Security-aware, model-based systems engineering with sysml. In *Proceedings of the 1st International Symposium on ICS & SCADA Cyber Security Research*, pages 78–87.

Rawnsley, A. Iran's alleged drone hack: Tough, but possible. http://www.wired.com/dangerroom/2011/12/iran-drone-hack-gps.

Rolls-Royce. Rolls-royce written evidence (auv0083). http://data.parliament.uk/writtenevidence/committeeevidence.svc/e and-technology-committee-lords/autonomous-vehicles/written/42075.html.

Schlinglof, B.-H. (2016). Cyber-physical systems engineering. In Liu, Z. and Zhang, Z., editors, *Engineering Trustworthy Software Systems*, volume 9506, pages 256–289. Lecture Notes in Computer Science.

Tyler, B., Crawley, F., and Preston, M. (2015). *HAZOP: Guide to Best Practice (3rd ed.)*. IChemE.

UK, M. Being a responsible industry - an industry code of practice. https://www.maritimeuk.org/documents/197/CODE_OF_PRACTICE_V1.0_-_Up_to_24m_-_Final.pdf.

Young, W. and Leveson, N. (2013). Systems thinking for safety and security. In *Proceedings of the 29th Annual Computer Security Applications Conference*, pages 1–8.