Maritime Communications and Use of Autonomous Systems

Andrew Bolster

October 13, 2015

1 Maritime Communications Environment

The key challenges of underwater acoustic communications are centred around the impact of slow and differential propagation of energy (RF, Optical, Acoustic) through water, and it's interfaces with the seabed / air. The resultant challenges include; long delays due to propagation, significant intersymbol interference and Doppler spreading, fast and slow fading due to environmental effects (aquatic flora/fauna; surface weather), carrier-frequency dependent signal attenuation, multipath caused by the medium interfaces at the surface and seabed, variations in propagation speed due to depth dependant effects (salinity, temperature, pressure, gaseous concentrations and bubbling), and subsequent refractive spreading and lensing due to that same propagation variation[PKL06].

The attenuation that occurs in an underwater acoustic channel over a distance d for a signal about frequency f in linear and dB forms respectively is given by

$$A_{\text{aco}}(d,f) = A_0 d^k a(f)^d \quad (1)$$

$$10\log A_{\text{aco}}(d,f)/A_0 = k \cdot 10\log d + d \cdot 10\log a(f) \quad (2)$$

where A_0 is a unit-normalising constant, k is a spreading factor (commonly taken as 1.5), and $a(f)$ is the absorption coefficient, expressed empirically using Thorp's formula (3) from [Sto07]

$$10\log a(f) = 0.11 \cdot \frac{f^2}{1+f^2} + 44 \cdot \frac{f^2}{4100+f^2} + 2.75 \times 10^{-4} f^2 + 0.003 \quad (3)$$

Refractive lensing and the multipath nature of the medium result in supposedly line of sight propagation being extremely unreliable for estimating distances to targets. The first arriving beam has as the very least bent in the medium, and commonly has reflected off the surface/seabed before arriving at a receiver, creating secondary paths that are sometimes many times longer than the first arrival path, generating symbol spreading over orders of seconds depending on the ranges and depths involved. Extensive Forward Error Correction coding is used on such channels to minimise packet losses.

$$A_{\text{RF}}(d,f) \approx \left(\frac{4\pi df}{c}\right)^2 \text{ where } c \approx 3 \times 10^8 ms^{-1} \quad (4)$$

Thus, the multi-path channel transfer function can be described by

$$H(d,f) = \sum_{p=0}^{P-1} h(p) = \sum_{p=0}^{P-1} \Gamma_p / \sqrt{A(d_p,f)} e^{-j2\pi f \tau_p} \tag{5}$$

$$\text{where } \tau_p = d_p/c, c \approx 1500ms^{-1}$$

where $d = d_0$ is the minimal path length between the transmitter and receiver, $d_p, p = \{1, \ldots P-1\}$ are the secondary path lengths, Γ_p models additional losses incurred on each path such as reflection losses at the surface interface, and $\tau_p = d_p/c$ is the delay time ($c \approx 1500ms^{-1}$ is the nominal speed of sound underwater).

Missing figure

Non-Linear Marine Propogation Figures from Ghia

Comparing $A_{aco}(d,f)$ with the RF Free-Space Path Loss model $A_{\text{RF}}(d,f) \approx \left(\frac{4\pi df}{c}\right)^2$, the impact of range on signal power is exponential underwater, rather than quadratic in RF space ($A_{\text{aco}} \propto f^{2d}$ vs $A_{\text{RF}} \propto (df)^2$). While both frequency dependant factors are quadratic, approximating the factors in (3), $f \propto A_{\text{aco}}$ is at least 4 orders of magnitude higher than $f \propto A_{\text{RF}}$

2 Need for Trust in Maritime Networks

As autonomous underwater vehicles (AUVs) become more capable, and economical, they are being used in many applications requiring trust. These applications are using the collective behaviour of teams or fleets of these

AUVs to accomplish tasks [Cai11]. With this use being increasingly isolated from stable communications networks, the establishment of trust between nodes is essential for the reliability and stability of such teams. As such, the use of trust methods developed in the terrestrial MANET space must be reappraised for application within the challenging underwater communications channel.

3 Trusted Development and Operation of Autonomous Systems

3.1 Introduction

The aim of the section is to explore where trust is likely to impact on an indicative system (of systems) that contains autonomous elements. To assist with exploring this, an indicative scenario is selected from the Maritime domain. This scenario centres on autonomous Mine Counter Measures and/or Hydrography, Capability (MCM/MHC) operations, incorporating Human Factors, Command and Control considerations, and Vehicle to Vehicle (V2V) distributed communication, from the perspective of trusted and semi-trusted operation.

Possibly need to include discussion of the nature and levels of autonomy up here, but is a fairly common concept

3.2 Trust Perspectives

In human trust relationships it can be seen that there can be several perspectives of Trust for example organizational, sociological, interpersonal, psychological and neurological[LS04]. We have already defined two trust perspectives when considering the design and operation of autonomous systems (Table **??**). Examples of roles that interact with a system from both of these trust perspectives are provided in Tables 1 and 2.

	Role		
	Designer	**Acquirer**	**Disposer**
Definition	Responsible for developing the system	Responsible for acquisition of the system	Responsible for the disposal of a system.
Level	Organisation	Organisation	Organisation
Perspective	The designer of an Autonomous System develops trust through the application of known and trusted tools to well understood problems (e.g. a well-defined requirement set) using competent and trusted staff. The trust perspective therefore could be regarded as the **Design perspective**.	The Acquirer of a System develops trust through prior experience of the vendor and similar products. For any given product this is supplemented by the examination of engineering evidence provided by the Designer Organisation. Although there will be several trust aspects to the role, for the purposes of this paper this role can be seen as having a **Design perspective** since the Acquisition process needs to develop trust that the systems it is buying will be designed to be trustworthy in operation.	System disposal does not necessarily indicate destruction. Where assets are passed to 3rd parties (e.g. though sale) the disposer must be confident that the autonomous behaviour can be reduced (where necessary) to a known and acceptable level. This perspective is therefore part of the **Design perspective** since there will be trust that (possibly advanced) behaviours can be prevented from being passed unwittingly to second user organisations; particularly since they may use the systems in a different context.

Table 1: Examples of Roles that require a Design Perspective of Trust in Autonomous Systems.

	Role		
	Commander	**Operator**	**User**
Definition	Responsible for the system tactical activity (e.g. mission / activity setting)	Responsible for the ongoing control of the system when deployed on a particular mission / activity	An end user of the capabilities provided by the system.
Level	Person	Person	Person/System/Org.
Perspective	The Commander places trust in the acquisition process to provide reliable assets. However, their trust perspective is **operational**.	An operator develops initial trust in a system through training and experience of similar systems. When interacting with a deployed system, the ongoing trust is maintained through correct and understandable system behaviour. This can be regarded as **Operational Trust**	A user of a Systems capability may not have any knowledge of the System itself but will need to develop trust in ability to provide trustworthy services. Again, this may be regarded as a form of **Operational Trust**

Table 2: Examples of Roles that require a Operational Perspective of Trust in Autonomous Systems.

3.3 Design Trust

Five aspects of Design Trust have been identified:

1. **Formal Specification of Dynamic Operation**: Autonomous Systems (AS) may be required to operate in complex, uncertain environments and as such their specification may need to reflect an ability to deal with unspecified circumstances. This includes engaging with dynamic systems of systems environments where an autonomous system may cooperate with a system not envisaged at design time. *How can systems that are required to demonstrate that they meet their require-*

ment be specified flexibly enough to permit adaptive behaviours?

2. **Security**: Any unmanned system has the potential to be used for illegitimate purposes by unscrupulous 3rd parties who could exploit security vulnerabilities to gain control of the system or sub-systems. Any system that has the potential to cause harm from such actions must have security designed in from the start to ensure that the system can be trusted to be resilient from cyber attack. Current accreditation schemes rely on a security assessment of a known architecture and there are mutual accreditation recognition schemes that could be encoded in dynamic discovery handshake protocols. This would produce a secure network assured through the accreditation of its component systems. For example, the Multinational Security Accreditation Board (MSAB) deals with Combined Communications Electronics Board (CCEB) and NATO Accreditations to provide security assurance of internationally connected networks. Encoding such agreements into secure handshakes could enable dynamic accreditation of autonomous systems cooperating in a coalition environment. It is not known whether these have been demonstrated, so the question is: *Can autonomous systems be designed to understand the security situation when interfacing with known or unknown systems?*

3. **Verification and Validation of a Flexible Specification**: Following on from the description of a flexible specification, establish that the AS conforms and performs in accordance to the specification. This has direct implication for the trust in the resultant system. How can systems demonstrate that they will behave acceptably when the environment is unknown?

4. **Trust Modelling and Metrics**: This could be argued as part of the Verification and Validation of the system. However, models are increasingly being embedded into system design as a reference. Thus it is useful to consider this element separately. *How can trust be modelled sufficiently to span the space of most potential behaviours to help ensure that systems will be trusted when moved into operational environments? Can this be measured to allow comparison and minimum requirements set?*

5. **Certification**: The certification requirements placed on specific systems will vary depending on domain and national approaches to certification. However, the common element in the requirement for certification is that a certified system is deemed as sufficiently trustworthy for use within its context of certification. Additionally Certification also relies on the predictability of a system. Because the aim of autonomous systems is to deal effectively with uncertain environments, *can they (autonomous systems) be certified without being demonstrated in the environment within which they will adapt new behaviour?*

Clearly, compliance with existing military and commercial standards can play a significant role in demonstrating the trustworthiness of any systems design. If a system has been designed to a Standard then it has known properties that have been accepted as good practice. However, these do not address the issue of the five areas listed above. The following sub section briefly outlines existing Standards for context.

3.3.1 Current Unmanned System Interface Standardisation

There are three main organisations that are developing or have developed assurance standards for Unmanned Systems in commercial, civil and military applications:

- NATO Standardization Office (NSO)

- Society of Automotive Engineers (SAE)

- American Society of Testing and Materials (ASTM)

NATO Standardization Office Faced with the growing adoption of similar but disparate UAV systems within NATO territories and coalition nations, STANAG 4586[NAT12] was promulgated in 2005 and defined a logistic and interoperability framework to provide commonality in the command and comtrol architecture and implementations of UAV/Ground station communications.

This included a particularly interesting development in the form of "Vehicle Specific Module" (VSM) interoperability, whereby existing systems could be grandfathered into 4586 compliance by the addition of a VSM to operate as a protocol translator. This VSM could be mounted on the remote system, utilising a 4586 compliant Data Link Interface (DLI), or mounted on the UCS utilising a proprietary DLI to the remote system. 4586 described five Levels of Interoperability (LOI) for compliant UAV systems, shown in Table 3. This structure has been criticised as being short sighted and at odds with the reality of modern and proposed autonomous vehicle operations [CBM10], specifically that in modern autonomous systems, there is no such thing as direct control or Operator-in-the-loop, especially in the case of BLOS systems, and that in increasingly autonomous systems, operation is done as Human Supervisory Control (HSC), or more commonly described as Operator-on-the-loop, whereby the operator interacts with the intermediate autonomous system and that autonomous system eventually performs that task on the hardware.

LOI	
1	Indirect receipt/transmission of UAV related payload data
2	Direct receipt of Intelligence, Surveillance and Reconnaissance (ISR) data where direct covers reception of UAV payload data by the UCS when it has direct communication with the UAV
3	Control and monitoring of the UAV payload in addition to direct receipt of ISR/other data
4	Control and monitoring of the UAV, less launch and recovery
5	Launch and Recovery in addition to LOI 4

Table 3: Levels of Interoperability for STANAG 4586 Compliant UCS

Further, 4586 predominantly deals with a one-to-one mapping between operators and nodes, when this is quite against the current state of the art; greater focus is being made in collective and collaborative assignment and having a single operating agent managing a group of autonomous nodes in-field, and handing off vehicle management responsibilities to the individual nodes.

SAE Levels of Autonomy possibly from [BFR14]

Society of Automotive Engineers (SAE) The AS-4 steering group is responsible for the development and maintenance of the Joint Architecture for Unmanned System (JAUS) standards, which provide several service sets for Inter-System cooperation and interoperability, either in the form of a specified design language (JSIDL[1]) or as a direct framework implementation, such as the JAUS Mobility, Mission Spooling, Environment Sensing, or Manipulator Service Sets[2].

This provides a stack-like interoperability model akin to the OSI internetworking standard, providing logical connections between common levels

[1] JAUS Service Interface Definition Language

[2] SAE AS6009, AS 6062, AS 6060, and AS 6057 respectively

across devices regardless of how subordinate layers are implemented.

Importantly, JAUS service models are open-sourced under the BSD-license, and a development toolkit is available for anyone to develop JAUS-compatible communications and control protocols[Ney].

It is also important to note that JAUS is part funded, and heavily utilised by, US Army and Marine Robotic Systems Joint Project Office (RS-JPO), which manage the development, testing, and fielding of unmanned (ground) systems for those respective forces. This includes now legacy M160 mine clearance platform and the highly popular (both with forces and their in-field operators) iRobot Packbot inspection and explosive ordance disposal (EOD) family of robotic platforms.

American Society of Testing and Materials (ASTM) The ASTM F38 committee has developed a LoS, single-asset-single-operator stove-piped framework for Unmanned Air Systems that is too constrained in scope for applicability to a more heterogeneous operating environment[Ame07]. However, the F41 Committee, focused on Unmanned Maritime Vehicle Systems (UMVS) has collectively developed a range of interoperable standards, covering Communications, Autonomy and Control, Sensor Data Formats, and Mission Payload Interfacing. Of particular interest is the Autonomy and Control standard [Ame06], which highlighted a requirement on the vehicle system to be able to recognise an authorised client, be that a human operator or an additional collaborating vehicle. Further, the standard states that the responsibility of the safety and integrity of any payload remains with the vehicle. This standard was withdrawn in 2015 due to ASTM regulations requiring standards to be updated within 8 years of approval, and has no direct replacement within ASTM, but stands as a useful guiding perspective on autonomy standards within industry.

ASTM F41 UMVS Architecture

3.4 Operational Trust

This work is considering autonomous systems as entities of wider systems, we refer to these here as Autonomous Collaborative Systems. As described earlier, Operational Trust has two main aspects, trust in the system to behave as expected and trust in the interfaces between systems (human/machine and machine/machine). Of all of the interfaces in an Autonomous Collaborative System, the most problematic is that arguably that between the System of Autonomous Systems (SoAS) and the human operator / team of operators. Cummings identified the main challenges to Human Supervisory Control (HSC), summarised below:[CBM10]

3.4.1 Information Overload

Operator efficiency exhibits an optimum at moderate levels of cognitive engagement, above which cognitive ability is overloaded and performance drops (Otherwise known as the Yerkes-Dodson Law). Additionally, in the case of under-engagement, operators can fall foul of boredom, and become desensitised to changing factors. *However, predicting this point of over-saturation is an open psychophysiological research problem.*

3.4.2 Adaptive Automation

Automation is well tailored to consistent levels of activity. This is quite simply not the case many domains. Particularly in defence and military applications, activity is characterised by long periods of "routine" punctuated by high intensity, usually unpredictable, activity. At those interfaces between "calm" and "storm", where real time situational awareness is imperative, temporary Information Overload is highly probable. Adaptive Automation enables autonomous systems to increase their level of automation (LOA) based on specific events in the task environment, changes in operator performance or task loading, or physiological methods. It is taken as given that for routine operations, and increased LOA reduces operator workload, and vice versa. However, this relationship is highly task dependent and can create severe problems in cases of LOA being greater, or indeed lesser, than is required. In the cases of overly-high LOA, operator skill is degraded, situational awareness is reduced as the operator is not as engaged, and the automated system may not be able to handle unexpected events, requiring the operator to take over, which, given the previous points, is a difficult prospect. Alternatively, in sub-optimal LOA, Information Overload can result in the case of high intensity situations, but also the system can fall foul of overly-sensitive human cognitive biases, false positive pattern detection, boredom, and complacency in the case where less is going on. Therefore, as a corollary to Information Overload challenges, there is a need to define the interrelationship between levels of situational activity (or risk) and appropriate levels of automation. *Under what circumstances can AA be used to change the LOA of a system? Does the autonomous system or the human decide to change LOA? What LOAs are appropriate for what circumstances?*

3.4.3 Distributed Decision Making

In a modern, non-hierarchical, often distributed or cellular military management system (Network Centric Warfare doctrine for example), tools are increasingly being used to mitigate information asymmetry within command and control. A simple example of this is shared watch-logs in Naval operations, providing temporal collaboration between watch-teams separated in time. The DoD Global Information Grid is another example of a spatial collaborative framework. Recent work has demonstrated the power of collaborative analysis and human-machine shared sensing technologies even with low levels of training on the part of the operators providing superior results and resource efficiencies than either humans or machines alone in survey and search-and-rescue scenarios (Ahmed et al.2014). As these temporal and spatial collaboration tools increase in complexity and ability, decisions that previously required SA that was only available at higher echelons within the standard hierarchy are available to commanders on the ground, or even to individual team members, enabling the potential for informed decisions to be taken faster and more effectively, enabled by automated strategies to present relevant information to teams based on the operational context. However there are a range of operational, legal, psychological and technical challenges that need to be addressed before confidence in these distributed management structures can be established. Studies into situational awareness sharing techniques (telepresent table-top environments, video conferencing, and interactive whiteboards) have generally yielded positive results, however investigations into interruptive-communications (such as instant messaging chat) have demonstrated a negative impact on operational efficiency. In short, the biggest problem with distributed decision making in the context of supervisory systems is that *there is no consensus*

Check Security

on whether it is advantageous or not, and what magnitude of operational delta is introduced, if any.

3.4.4 Complexity

Beyond simple Information Overload, increasing complexity of information presented to operators is having a negative effect on operational efficiency. In HSC, displays are designed to reduce complexity, introducing abstractions with an aim to presenting the minimum amount of information to the operator required to maintain an accurate and up-to-date mental model of the environmental and operational state. This has led to the development of many domain specific decision support interfaces, however, in academic research, there has been nothing but mixed results. One commonly raised negative is the general bias on the cool factor of interfaces. Immersive 3D visual, aural, or haptic interfaces that at first appraisal seem to provide more approachable information to the operator, and are indeed tacitly preferred by operators in use. However, there has not been any evidence to demonstrate performance improvement when using these tools, and in-fact, *improving the "fidelity" of the interfaces has led to operators overly-relying on these representations of the environment rather than remaining engaged in the environment.*

3.4.5 Cognitive Biases and Failing Heuristics

In many areas, operators and commanders are required to make rapid decisions with imperfect information, driven by massively increased information availability and rates of change in areas such as battlefield tactics and global finance markets. However, Human decision making isnt always rational (especially under pressure), and operators use personally derived heuristics to make “rational shortcuts”. This is a double edged sword, where these heuristics can be employed to greatly reduce the normative cognitive load in a stressful situation, but also introduce destructive biases, where these shortcuts make assumptions that dont bear out in reality.

For example, in the context of decision support systems, “Autonomy Bias” has been observed as a complement to the already well known “Confirmation Bias”[3] and “Assimilation Bias”[4] , where operators that have been provided with a “correct” answer by a decision support system do not look (or see, depending on perspective) for any contradictory information, and will unquestionably follow, increasing error rates significantly.

This behaviour isnt only the reserve of decision support systems, but also in the generic allocation of operator attention; scheduling heuristics are used to decide how much time tasks should be worked on, and time and again, humans are found to be far from optimal in this regard, especially in time-pressured scenarios where these heuristics are in even more demand. Even when operators are given optimal scheduling rules, these quickly fall apart, often due to primary task efficiency degradation after interruption. This highlights a critical interface in the adoption of complex autonomous systems that still demand Man in the loop functionality; if a system is required to have full-time concentrated supervision (e.g. flying a UCAV), but also event-based reactive decision making (e.g. alerts from non-critical subsystems), both tasks are negatively impacted. In an assessment of factors influencing trust in autonomous vehicles and medical diagnosis support systems, Carlson et al also identified that a major factor in an operator or users

[3] Confirmation Bias is the tendency for people to preferentially select from available information that information that supports pre-existing beliefs or hypotheses.

[4] Assimilation Bias is often thought of as a subset of Confirmation Bias, whereby it specifies that instead of seeking out information supporting of current views, any incoming data is interpreted as being supportive of a particular view without questioning that view, even if it appears contradictory.

trust in a system was not only dependant on past performance and current accuracy but also on "soft factors" such as the branding and reputation of the manufacture / designer.(Carlson et al. 2014)Further, autonomous decision support / detection / classification systems have an "uncanny valley" to overcome in terms of accuracy, in that there is a dangerous period when such systems are used but not perfect, but operators become complacent, causing an increased error rate, until such a time that those autonomous systems can match or exceed the detection rates of their human counterparts.

Check Security

3.4.6 Summary of Human Factors impacting Operational Trust in Defence Contexts

When dealing with human supervision of autonomous or semi-autonomous systems, there is an inherent conflict between the expectations of the operator, the hopes of system architects. System Architects aim to provide more and more information to the operator to justify a systems operation, and Operators in reality need less and less information to be efficient when things are going well, and responsive in a dynamic environment. This places huge demands on Human Interface design and indeed on communications design to provide this timely, relevant, interactive connection between any autonomous system and the end operator(s). Recent work has presented the idea of taking user interface (UI) inspiration from the entertainment sector, in terms of UI best practises developed over two decades of Real-Time Strategy game development [JPL07], and follow up work into automated mission debrief demonstrated that such operational support could improve causal situational awareness of an operator when compared to a human-baseline [JL11]. In terms of the human factors challenges raised by Cummings, they are often contradictory in their direction, particularly when contrasting between Adaptive Automation and Cognitive Biases challenges. This is a key part of the “soft trust” perspective, where the operators and commanders need to be able to implicitly and explicitly trust the operation of a remote system with limited feed-back bandwidth, high latency, or long-term operation such that direct remote operation is infeasible or undesirable. To be able to trust that systems ability to continue on a course, survey an area, notify on detection of an anomaly, etc.is going to be the corner stone of any autonomous systems justification in the future.

3.5 Conclusions

With demand for smaller, more decentralised marine survey and monitoring systems, and a drive towards lower per-unit cost, TMFs are going to be increasingly applied to the marine space, as the benefits they present are significant. Beyond the constraints of the communications environment, knock on pressures are applying in battery capacity, on-board processing, and locomotion. These pressures simultaneously present opportunities and incentives for malicious or selfish actors to appear to cooperate while not reciprocating, in order to conserve power for instance. These multiple aspects of potential incentives, trust, and fairness do not directly fall under the scope of single metric trusts discussed above, and this context indicates that a multi-metric approach may be more appropriate.

However, the implications of trust in autonomy beyond securing communications and data are an area in need of further research (BAE Systems, 2013. Maritime Autonomy Final Report - Combined Response,)Of particular concern is the verification of autonomous behaviours. Technology Readiness Level deficiencies were identified in the Maritime Capability Contribution of Unmanned Systems (MCCUS) Osprey Phase 1 report(Clark,

Need to check security status of this source

H. et al., 2012. Maritime Capability Contribution of Unmanned Systems,),, with a particular focus on failsafe behaviour. The addition of increased onboard autonomy in MUxS, properly understood and verified, would greatly improve this future capability, similar to recent developments in the UAS arena[CBM10]. There are opportunities for increased decentralisation and in-field collaboration(Walton, R., 2012. Maritime Autonomy PDR Pack.), however, difficulties in Trust between human operators and autonomous systems have already been clearly identified[CBHS11],and this has been demonstrated by the recent decision by the German government to renege on its 500M investment in the Euro Hawk programme, due to concerns about civil certification of the onboard autonomy[Meh13] In order for these new distributed structures to be relied upon to provide operational performance, reliability and to maintain in-field situational awareness, vulnerabilities to disruption, interruption, and subversion need to be understood and minimised.

Need to check security status of this source

Need to check security status of this source

References

[Ame06] American Society of Testing and Materials. ASTM F2541-06 Standard Guide for Unmanned Undersea Vehicles (UUV) Autonomy and Control. Technical report, 2006.

[Ame07] American Society of Testing and Materials. ASTM F2500 - 07 Standard Practice for Unmanned Aircraft System (UAS) Visual Range Flight Operations. Technical report, 2007.

[BFR14] Jenay M Beer, Arthur D Fisk, and Wendy a Rogers. Toward a Framework for Levels of Robot Autonomy in Human-Robot Interaction. *Journal of Human-Robot Interaction*, 3(2):74–99, 2014.

[Cai11] Andrea Caiti. Cooperative distributed behaviours of an AUV network for asset protection with communication constraints. *OCEANS, 2011 IEEE-Spain*, 2011.

[CBHS11] Jessie Y. C. Chen, Michael J. Barnes, and Michelle Harper-Sciarini. Supervisory Control of Multiple Robots: Human-Performance Issues and User-Interface Design. *IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, 41(4):435–454, 2011.

[CBM10] Mary L. Cummings, Sylvain Bruni, and Paul J. Mitchell. Chapter 2¡BR¿ Human Supervisory Control Challenges in Network-Centric Operations, 2010.

[JL11] Nicholas A. R. Johnson and David M. Lane. Narrative monologue as a first step towards advanced mission debrief for AUV operator situational awareness. *2011 15th International Conference on Advanced Robotics (ICAR)*, pages 241–246, 2011.

[JPL07] Nick Johnson, Pedro Patron, and David Lane. The importance of trust between operator and AUV: Crossing the human/computer language barrier. *OCEANS 2007 - Europe*, pages 1–6, June 2007.

[LS04] John D Lee and Katrina A See. Trust in automation: designing for appropriate reliance. *Human factors*, 46(1):50–80, 2004.

[Meh13] Aaron Mehta. Political, Financial Threads Underscore German Euro Hawk Saga. *Defense News*, June 2013.

[NAT12] NATO Standardization Office. STANAG 4586 STANDARD INTERFACES OF UAV CONTROL SYSTEM (UCS) FOR NATO

UAV INTEROPERABILITY Ed: 3. Technical report, NATO, Brussels, Belgium, 2012.

[Ney] Neya Systems LLC. The JAUS Toolset.

[PKL06] Jim Partan, Jim Kurose, and Brian Neil Levine. A survey of practical issues in underwater networks. *Proceedings of the 1st ACM international workshop on Underwater networks WUWNet 06*, 11(4):17, 2006.

[Sto07] Milica Stojanovic. On the relationship between capacity and distance in an underwater acoustic communication channel, 2007.