whitepaper

14 May 2014

Ship security alert systems are failing at the time they are needed most

Ship security alert systems are a statutory requirement, but conforming only to the minimum standards undermines their practical value when ships are under threat. Fortunately, with a little thought and application, ship security alert systems can be vastly more effective.

What is the point of a Ship Security Alert System (SSAS)? Since 2006, when all ships were required to have installed ship security alert systems, shipping has been subjected to a significant rise in serious organised crime: Somali piracy and piracy in West Africa being the most public examples. In the last two and a half years, we have responded to nine cases where tankers have been hijacked for the purpose of stealing their cargo, providing investigation and incident management services. And in all but one case, crews have either not activated the SSAS, or when they have done so, it has been disabled apparently by the vessels' assailants. Consequently, a technology that could and should have been of substantial assistance in terms of incident response and investigation, has failed.

The IMO adopted the International Ship and Port Facility Code (ISPS Code) in 2002, principally as a response to international concerns about terrorism following the events of 9/11. The ISPS Code incorporated an amendment to SOLAS – Regulation XI-2/6 – which requires passenger ships and cargo ships of 500 gross tonnes and upward and mobile offshore drilling units to have ship security alert systems.

The intended purpose of ship security alert systems is simple: to alert shipowners, Flag Administrations and Contracting Governments that the security of the ship is under threat or has been compromised.[1] In reality, however, the practical effectiveness of ship security alert systems is far from their intended purpose, and crucially, their potential intrinsic value in the event of a major security incident: ship security alert systems are not working as they should when they are needed.

Why? The first problem with ship security alert systems is that, technologically-speaking, most on the market are compromises. The implementation of the ISPS Code imposed additional financial costs on shipowners and increased the working-time burden on ships' Masters and crews. As a concession, type approval standards permit ship security alert systems to be integrated with ships' existing radio and satellite communication systems, and in particular day to day fleet tracking technology.

What this overlooks is the fact that if, for whatever reason, a ship's communications system goes offline, or is actively taken down, an SSAS integrated into the same system will cease to function.

[1] Section 2.1, SOLAS Regulation XI-2/6

14 May 2014

Regulation XI-2/6 was subject to revision in May 2003,[2] and its only stipulation toward the operational independence of ship security alert systems from other radio systems (communications systems) on board relates to the power supply to the SSAS. It states:[3]

"*Where the ship security alert system is powered from the ship's main source of electrical power, it should, in addition, be possible to operate the system from an alternative source of power*."

This has widely been interpreted to mean that ship security alert systems should have a battery-powered backup. However, it has not resulted definitively in the installation of ship security alert systems that are wholly operationally independent of other communications systems on board ships.

Further, while some (generally more expensive) ship security alert systems allow shipowners to communicate with them remotely ('ping') from ashore, other (cheaper) ship security alert systems will only communicate one-way, from ship to shore. Consequently, it is not possible to track a ship installed with a low-cost ship security alert system if it has not been activated on board the ship.

The second problem with ship security alert systems currently is the guidance that has been widely adopted relating to the procedures commonly implemented on board ships in relation to the activation of ship security alert systems, as well as the location of the activation points themselves.

With regard to *Activation Points*, MSC.147(77) states that:

"*Activation points should be capable of being used on the navigation bridge and in other locations. They should be protected against inadvertent operation. It should not be necessary for the user to remove seals or to break any lid or cover in order to operate any control*."

We have conducted many ship security surveys over the years and what we find almost universally on initial survey is that there is an activation point on the navigation bridge and an activation point in only one other location. Rare is the occasion that there are activation points in multiple locations on a ship.

Notwithstanding that this conforms to the regulations as they are currently drafted, by locating activation points only on the navigation bridge and one other location, it assumes that whoever identifies a threat to the security of the ship is on the navigation bridge or in the locality of the other activation point at the time. In practice, this isn't usually so.

In addition to this, shipowners seem not able to resolve the contradiction of protecting activation points from inadvertent operation while at the same time making it unnecessary for users to remove seals or to break any lid or cover in order to operate any control.

[2] MSC.147(77), Adoption of the Revised Performance Standards For A Ship Security Alert System (Adopted on 29 May 2003)

[3] Section 3.1, 3. Power Supply, MSC.147(77), Adoption of the Revised Performance Standards For A Ship Security Alert System (Adopted on 29 May 2003)

14 May 2014

In our experience, the activation point on the navigation bridge is often located inside a cupboard or in a location that is physically hard to reach, ostensibly because it makes the activation point visibly hard to detect by anyone unlawfully boarding and taking control of the vessel. What it actually does is to make the task of discreetly and quickly activating the SSAS very difficult in the first place.

Two other factors compound these issues.

Because the confidentiality of Ship Security Plans (SSPs) is seemingly deemed to be inviolate beyond the knowledge of the Master and the Ship Security Officer (SSO) – who incidentally is still often the Master – we frequently find that the other officers on a ship do not know where the SSAS activation points are located. This makes no sense, as the Master and SSO are not on duty all the time. To first have to alert the Master and/or SSO to a security threat to the ship simply delays the prompt activation of the SSAS. In cases that we have investigated, a crew member having attempted to alert the Master and/or SSO first has prevented the activation of the SSAS at all.

There is also the problem that the circumstances in which a ship security alert should be initiated is undefined by regulation or formal guidance beyond where the security of the ship is under threat or has been compromised. As things stand, MSC 147(77) states additionally, but only, that:

"*The procedures for the use of the ship security alert system… are given in the ship security plan agreed by the Administration.*"

Unless the circumstances in which a ship security alert should be initiated is clearly prescribed in the ship's security plan and the crew drilled in that detail, the scope for any crew member misreading the circumstances is too great.

Fortunately, it is possible to ensure that ship security alert systems work effectively at the time they are needed most.

First, when an SSAS is installed on a ship, it must be technologically and operationally independent of any other radio or communications on board the ship. Often referred to as redundancy, it means that if the ship's other radio or communications is disabled, the SSAS should continue to work.

Second, while the regulations permit the installation of only two activation points, it makes sense to have more in places around the ship where crew are likely to be on a regular basis.

Third, all activation points should be easy to access: if no one can get to them the SSAS cannot be activated on the ship.

Fourth, it is naïve to assume that the Master and/or the SSO will be on duty when a threat to the ship is identified. Therefore, all officers – if not all members of the crew – should know where the activation points are so that the SSAS can be activated quickly in such circumstances.

14 May 2014

Fifth, it is crucial to set out clearly for the crew in what circumstances they should activate the SSAS and they should practise recognising those circumstances on a regular basis.

The theoretical purpose of ship security alert systems is a good one and it doesn't cost much in time or money to ensure that they work in practice. Thought about and implemented properly, ship security alert systems will work when they are need most, especially where the assailants' objectives are to take the ship and/or its cargo.

ABOUT GRAY PAGE

Established in 2003, Gray Page is a specialist maritime consulting group that solves problems around the world for organisations operating in the international shipping market.

Often working in sensitive circumstances and complex environments, we provide investigative, intelligence and risk management expertise. We help our clients manage commercial and operational risks, respond to crisis events and recover from the damage caused by the default, negligence or malicious acts of third parties.

GRAY PAGE SERVICES

- Investigations
- Business intelligence
- Crisis management
- Asset protection
- Expert witness

CONTACT US
United Kingdom
Email: enquiries@graypage.com
Tel: +44 1865 861 400

Singapore
Email: enquiries.singapore@graypage.com
Tel: +65 6337 6327

Crisis Response Team:
Tel: +44 (0)1865 861 444 (emergencies only)