



A WHOLE NEW VISION UNDERWATER

Commercial in Confidence

FarSounder, Inc.

SPS for the Ship Operator: Diver Detection Sonar Explained

(F31561 Rev. 1.0)

FarSounder, Inc.
43 Jefferson Blvd.
Warwick, RI 02888
United States

phone: +1 401 784 6700
fax: +1 401 784 6708

info@farsounder.com
www.farsounder.com

Revision Issue Date: June, 2011

© **Copyright 2011 FarSounder, Inc.**

All rights reserved. This document contains confidential information that is proprietary to FarSounder, Inc. This commercially sensitive information is being provided to the recipient solely for the purpose specified and shall not be reproduced, disclosed or supplied, in whole or in part, to any other person without the prior written consent of FarSounder, Inc.

Although every precaution has been taken in the preparation of this document, FarSounder, Inc. assumes no responsibility for errors or omissions. Furthermore no liability is assumed for damages resulting from the use of information contained herein.

Table of Contents

Preface.....3

What is the "threat" target for the yacht SPS sonar.....3

Target detection limits.....4

What the customer should care about.....5

Testing the sonar.....6

Conclusion.....7

Preface

With the growing number of threats today, Ship Protection Systems including active diver detection sonar are becoming of greater interest to more and more vessel owners. As with any technology, it is important to understand its capabilities and limitations when evaluating various products. When comparing these products, one question that users often face, is what metrics should they be considering? This paper is intended to provide a brief background on such capabilities, limitations, and metrics.

There are a number of Active Diver Detection Sonars, but the physical principles of operation are the same for each one: the sonar transmits the underwater sound pulse ("ping") and then listens to the echo reflected by the target. The sonar repeats the ping at a given update rate and the sequence of observations with many pings ("ping-to-ping history") is analyzed to make decisions.

There are always a number of reflectors such as the sea bottom and surface, rocks, unwanted targets like fish schools and other marine life, etc. These targets can acoustically shade one another (for example, one cannot see fish hidden behind a large rock or ship wake).

Additionally, there is always some amount of acoustic noise present, caused by surface waves, ship traffic, etc. The noise can disturb the sonar in two ways: First it may mask the target echo and so limit the sonar's ability to detect the target; Second, it may be mistaken as the target echo - which is referred to as a false detection or false alarm.

The sonar must perform with some required quality, which means to enable the decision of "that type of target is present, now at that range and bearing". As one can see from the explanations above, this kind of decision cannot be reliably made with just a single ping. The sonar processing chain consists of target detection at every single ping, target tracking via the ping-to-ping history (with the understanding that the target could be lost during some pings) and target classification (at least into two classes of threat/non-threat).

What is the "threat" target for the yacht SPS sonar

Here is a brief list of possible threat targets:

1. Diver with SCUBA (this equipment provides air bubbles, which makes the target acoustically stronger, as the sonar can see the reflections from the diver's body, air tank and exhaled bubbles)
2. Diver with closed-circuit re-breather (CCR) (no bubbles)
3. Diver with propulsion vehicle (underwater scooter) – an acoustically strong target

4. Small radar-invisible (plastic) boat
5. Mini-submarine

This list clearly shows two things. First, the sonar must be able to "detect/track/classify" for the least reflecting target (with the smallest acoustic target strength) at the distance which is still large enough to provide the yacht crew with time enough to respond. What "respond" means could be different in different situations: to simply pull anchor and get underway, to send the patrol boat to intercept, etc.

Second, it is important to integrate all of the security sensors (sonars, hi-res security radars, infra-red, CCTV) to enable the best reliable decisions. For example, if the sonar sees a large moving target which the radar can see as a container ship, this target is not a threat. If the sonar sees a small target intentionally moving towards the yacht and this track started at the same point where the radar saw a suspicious anchored boat, then the chance this target is a threat becomes greater. If the sonar can see targets which other sensors cannot, it is definitely the underwater target.

Target detection limits

Assuming the case where there is only one target, so other targets cannot interrupt the detection, then there are 3 major factors which limit the sonar's detection ability (and therefore the detection range):

1. Target strength (reflectivity)
2. Noise level
3. Underwater sound propagation conditions

The last one needs further explanation. Underwater sound does not propagate as a straight path (or ray), (like radio waves in standard marine radars). Instead, it propagates in bent rays (like radio waves in over-the horizon radars). When bent, these underwater rays may hit the bottom, losing part of their acoustic energy while reflecting some energy forward, or they may be totally absorbed. The sound also attenuates while propagating through the water. Propagation depends on the environment and could be very different in summer vs. winter, in shallow vs. deep water, at river estuarine areas, and in salt vs. freshwater.

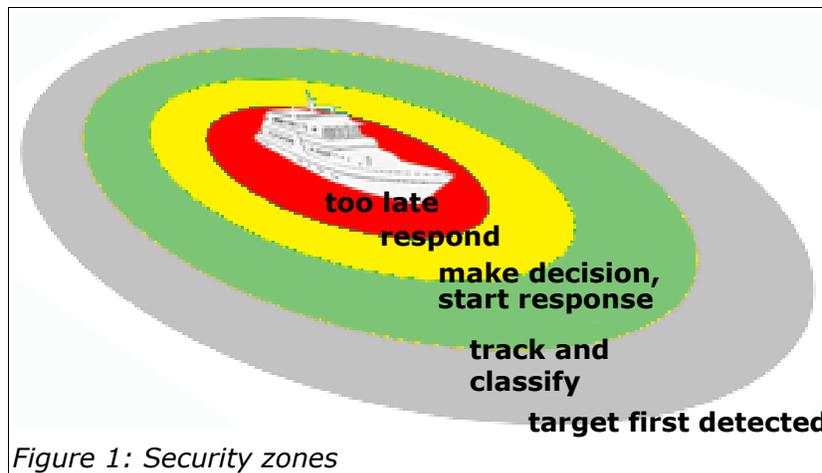
The worst conditions generally are produced by: hot summer, shallow water and high sea state (which means more wave-induced acoustic noise). Luckily, threat intrusion is less probable at a high sea state. All the above said threat targets usually need calm weather to operate most effectively.

What the customer should care about

As stated above, the sonar processing is a chain in time - from the first detection to the final classification. So the initial intruder detection range must be at least:

$$(\text{time to track and classify} + \text{time to make decision and start respond}) \times \text{intruder speed} + \text{safe distance to respond}$$

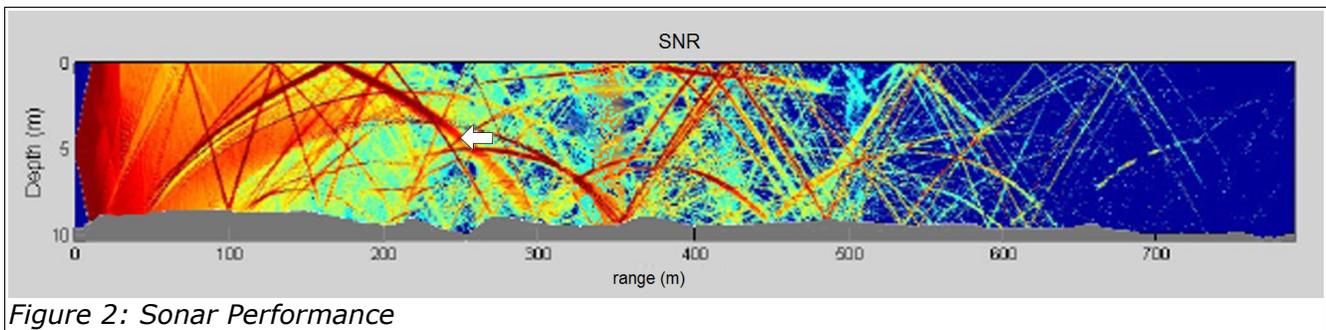
The following Figure 1 shows the view of decision events as security zones.



Let's consider the worst case scenario, namely the less reflective threat target (diver with closed-circuit re-breather), summer type of propagation conditions, shallow water (10m), rough bottom, and reasonable sea state (3). Maximum CCR diver speed is 1knot (especially with load). With that low target strength and poor propagation environment, it might take up to 100 consequent pings to track and classify. With a typical sonar update rate of 2 seconds, the time to track and classify is about 3 minutes for a 100 ping history. Let's guess that a reasonable summary time to make a decision is 2 minutes (bridge officer sees the alarm, reports to captain, decides on response, makes commands). Finally, guess the safe distance to respond is 100m. This means that the "first detection" range must be 250m.

This example shows that it is not only that the sonar (as well as other surveillance equipment) must provide a good enough detection range and reliable tracking/classification. It also clearly shows that the security staff must be well organized. An additional 3 minute loss in decision making and response may be fatal. Electronic surveillance is not a magic wand and cannot see beyond physical limits.

Figure 2 shows an example of those physical limits: how the sound propagates (see the bent rays) and how the sonar see the target.



In this plot the sonar location is at 0m range, 5m depth. The target can be at an arbitrary point: any depth from surface to bottom, any range from 0 to 800m. Color depicts Signal-to-Noise Ratio (SNR) where red color indicates a high SNR and the target is nicely detectable. Green color means it is good enough and the target is still 100% detectable. Deep blue means it is not detectable. One can see that at 250m and closer the target (if not shaded by other targets) is 100% detectable with no gaps. That distance marked by the white arrow. It is also detectable starting from 500m, but now there would be detection gaps which must be taken care of while tracking. Beyond 500m this kind of target is not detectable in that environment.

Interestingly, that same target in winter conditions would be visible up to almost 700m.

Customers should note that some Diver Detection Sonars only provide specifications for the best conditions, not for the worst ones.

Testing the sonar

There are 3 different kinds of tests.

First is the functionality test – to verify that the equipment is operating correctly. This means the hardware and software work with no failure, but regardless of any specified features such as range of detection, quality of detection and tracking.

Second is the customer acceptance test – to verify the major specification features like approximate detection range, without details. That kind of test should be fast and simple enough, and not too expensive. It does not require the exact comparison to ground truth, and should be based on the very approximate comparison of sonar performance with the product specification.

Third is the manufacturer test(s) – to verify every detail of the product performance. This test is expensive. First of all, it requires statistics. For the same target and same sound propagation conditions, the target route must be repeated many times to estimate the mean, the variance and the probability of every feature.

For example, a detection range specified as "detect that target in these conditions at that range with probability of detection 0.9 and probability of false alarm $10e-2$ " means the target route must be repeated 100 times to verify that the sonar can detect the target at that range 90 out of 100 times and the false alarm happened only once.

This also means that the ground truth is needed to prove the correct localization with detection. Usually this means that the target must be equipped with a recording GPS to verify the detected target position is correct. This also means that ground truth is required for the all the other targets in the area. If some detection other than the diver target happens, it must be possible to prove that this detection is a true false alarm, not another target like a fish school or rock. Otherwise the detection should be considered as true detection, but for another target.

The environmental ground truth must be measured to make sure what propagation conditions we are talking about. Usually the water salinity, temperature, and density vs. depth is measured by using the special probe. That measurement must be repeated at least every 4 hours, because these parameters are time variable.

Finally, the Sonar Performance Simulator must be used to check that the observed performance is consistent to the theoretically expected performance. This is an expensive tool, because it simulates the sonar (with full scale processing), target reflectivity and the sound propagation in the ground truth environment.

Conclusion

One of the most important aspects in selecting a diver detection solution is understanding how it fits into the ship's overall security solution. What is the vessel's response plan? Where will the vessel be anchored? These questions help ensure that the sonar's performance capabilities meet the customer's expectations. Once the capabilities are understood, it is necessary to then understand what physical limitations are present. The local environmental conditions can greatly effect detection range of any sonar system. The chosen system should be specified to perform at the needed level under the *worst* expected conditions to be of value.

Overall, the most important thing in delivering an effective SPS solution is close teamwork and understanding between the customer, electronics integrator and sonar vendor.