Efficient Procurement of Low Vulnerability Warships

J S Schofield[ab] MMath MA (Cantab) CMath FIMA MRINA, D J Wright[a] BSc AMIET

[a] *Survivability Consulting Limited, Dunfermline, UK*
[b] Corresponding Author. Email: jschofield@survivability.co.uk

Synopsis

In recent decades the UK has made significant advances in its approach to, and its results from, the management of naval platform vulnerability. This paper explores the history, guiding principles and assessment techniques of successful vulnerability management.

World War II lessons learned are reviewed and shown to be still relevant today. These include structural and systems design features for the management of blast and fragmentation.

Requirements must be set which are realistic and contractual. Through the design of several classes of ship using current vulnerability management principles it is now clear what can be achieved. Therefore realistic requirements can be effectively set.

Quantitative vulnerability assessment is a key part of the design process, from the earliest concept to build and beyond. It is never too early to consider vulnerability, as the biggest gains can be made for the least cost during the early concept phases. However, early promise can be compromised by careless addition of supporting systems and services, so continuous monitoring is required.

In order for vulnerability assessments to keep pace with and guide the direction of the developing design, efficient assessment tools are needed. If the model takes too long to build, the tool offers purely an audit function, rather than being a design aid. Such a tool is also an important input to Operational Analysis of the in-service fleet. As such, very large parameter spaces of results are needed, for the full threat spectrum against the whole fleet in a range of scenarios.

SCL has developed the Purple Fire tool to facilitate the sorts of assessment required for modern platform designs, weapon programmes and operational analysis in support of the fleet. It provides the analyst with the ability to construct platform representations very quickly, meaning less model build time and more analysis time. It automates the consideration of large parameter spaces allowing in-depth assessments to be conducted quicker than ever.

Keywords: Vulnerability, historical lessons, requirements specification, vulnerability assessment, Purple Fire.

1. Introduction: Naval Vulnerability in World War II

During WWII when a ship was damaged or lost, the Royal Navy required an action report from the ship's officers. Damage surveys of vessels that returned to port were also undertaken for the Director of Naval Construction. Recommendations for changes that would reduce or eliminate preventable problems re-occurring were very much a part of both reports.

Those recommendations agreed by the Admiralty would then be promulgated to the fleet in Admiralty Fleet Orders. These were routine orders that contained anything from information on new dangers discovered, to administrative regulations on scales of equipment to be carried, to changes in ship organisation. They also included instructions for modifications to be carried out by ship's company, dockyard or in design practice to be followed for new builds.

The Royal Navy's biggest lessons of WWII related to the severity of shock damage and fragment damage to the increasingly complex cables & pipework. Loss of all propulsive or electrical power made for a cheap kill of operational capability. Loss of power or data connection to sensors, external communications or weapons systems was almost as bad. Electrical power was important to the vessel not just in the outer battle, but also in the inner one. Lack of lighting, pumping or internal communications would hamstring damage control efforts needed to plug leaks and recover capability.

There was a tendency to: apply armour first; next use isolation to prevent the entire network failing; then provision of emergency sources of power or pumping; and finally consider how to make better use of the installed capacity. While this did generate improvements, the order of tackling the problems was practically the reverse of what we now know to be the most efficient.

Avoiding loss of steering control was treated as a very high priority and is perhaps illustrative of something we have almost forgotten can be a problem. Vertical as well as transverse separation of alternative cables is something actively promoted by UK vulnerability analysts for the last two decades based on computer simulations. It is amusing to realise that it was not, as had been claimed, counter to shipbuilding practices, but

http://doi.org/10.24868/issn.2515-818X.2018.024

had previously been implemented and proven. The vulnerability of vital cables or pipe runs was such a feature of early action damage reports that in the first year of WWII a study of the characteristic of shells and bombs was made. It was quickly realised that shell fragments inside a ship were restricted to a cone with the apex at the point of burst and the trajectory generally at less than 30 degrees to the horizontal. This meant that if two redundant cables ran along opposite sides of the hull on the same deck the one nearest to the point of burst would have a high degree of immunity from damage, as illustrated on the left of Figure 1 which recreates the WWII analysis. Bombs usually detonated within 30 degrees of the vertical and produced a side spray of fragments. For duplicated cables, both would now be at risk, but immunity of one could be restored by separating the cables by a deck. This is shown on the right of Figure 1 where both cables A and B are in the swept region but their alternatives of D and C are not. The swept areas illustrated are clipped by ricochet limits. Modern sea skimming anti-ship missiles approaching other than orthogonal to the ship produce a similar pattern of fragments to the bombs, but arrive horizontally.

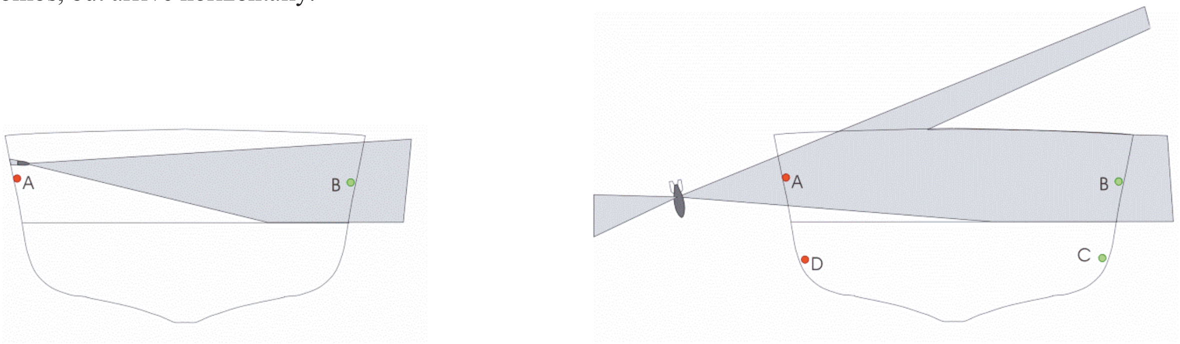


Figure 1: Transverse and vertical cable separation as considered in WWII vs. shells (left) and bombs (right)

Fragment protection of the whole ship was a feature of WWII lessons, both to prevent fragments entering from external detonations and prevent longitudinal spread from internal detonations. Modern vulnerability reduction has seen some fragment protection of key spaces, but not as a matter of course for the whole-ship. Conversely little in the way of blast protection was seen in WWII lessons but modern build techniques have allowed much improved performance.

The WWII shock program was targeted at finding fixes to problems revealed by action damage. This test-and-adjust approach has become problematic in a world of contractual relationships between owners, primes and sub-contractors. That the old approach worked in keeping a ship fighting is evident from the historical record. What is needed now are modern processes and methods to ensure the same outcome in current procurements. There is a tendency for modern warship designs to concentrate on peacetime performance, be it economy, maintainability or comfort. Whilst these are important to ensure the ship numbers and availability needed for operations in times of tight budgets, we should be designing for war, then adapt for peace, not the other way round.

2. Vulnerability Requirements

Requirements must be set which are realistic and contractual. Through the design of several classes of ship using current vulnerability management principles it is now clear what can be achieved. Therefore realistic requirements can be effectively set.

2.1. Using lessons already learned

We have already seen that vulnerability lessons have been learned for many years. More recent classes than the WWII examples above have had their own lessons. A pragmatic approach is simply to mandate certain features as providing a good baseline for low vulnerability, without undertaking additional analyses, on the basis that ‘we know certain things just work’. Whilst this may be uncomfortable to those seeking to scrutinise every possible variable, in the world of limited time and budget it is an efficient way to get a long way towards a low vulnerability solution in the very early stages of a design. The UK MOD’s mandated features were produced in response to industry’s request that such features would ease the design process and reduce costs.

Mandated features can relate to:

- Protection of certain key main bulkheads;
- Protection of high value compartments, magazines and machinery spaces;
- Shock mounting of key systems;
- Separation of propulsion machinery;

- Separation of generation machinery;
- Separation of steering machinery;
- Systems design for damage tolerance.

The last aspect is worthy of more discussion. Zoning of key service systems such as chilled water and power distribution, including separated redundant supply routes (pipes and cables), is important to vulnerability. Data networks such as the Combat Management System and Platform Management System tend to have significant redundancy for reliability purposes, but it is important that the layout of such networks is optimised and that the knock-on effects of damage are studied, such as the time needed for a second server to take over from a damaged master. The key is that much is known about how to build low vulnerability into many systems on board, so there is no need to start from a blank sheet of paper.

2.2. Applying numerical requirements

To build on a baseline design that incorporates the mandated features and demonstrate its low vulnerability, it is necessary to set numerical requirements and undertake measurements against those requirements efficiently, facilitating vulnerability management, rather than creating an onerous measurement process. Vulnerability requirements can relate to avoiding specific effects (such as the loss of the platform due to a given threat or significant munition reactions), or avoiding the loss of given important functions (such as propulsion or war-fighting roles). Thus the traditional “Float”, “Move” and “Fight” aspects come into play. Of course, depending on what aspects of a ship’s systems are damaged by a weapon strike, various levels of capability may be available after damage. The question arises, what level of “Move” and what type of “Fight” do we wish to retain after weapon damage? Thus follows the question, what weapons are we designing against?

In fact, it is sensible to design different levels of capability to withstand different levels of threat. Hence against an “Extreme Threat” we may accept loss of many systems but demand the survival of essential damage control and lifesaving functionality along with a very low level of propulsions. Against a less severe “Design Threat” we would want to be able to retain a greater level of propulsion (such as higher speed and better manoeuvrability) along with the ability to defend the platform from subsequent attacks and undertake a degraded level of wider roles, such as area defence or offensive operations.

It has been found that defining a small number of key “Move” and “Fight” functions against “Extreme” and “Design” threats allows vulnerabilities to be driven out of a design, but setting out to optimise for a larger number of functions is not as effective. In fact, concentrating on finding and mitigating vulnerabilities on a small number of key functions often helps a wider set of functions due to improvements in supporting functions like data, electrical and cooling systems.

In the UK, the concepts of mandated features and numerical vulnerability requirements are encoded in MOD’s Key Threshold Requirements for Surface Ship Vulnerability.

2.3. The Vulnerability Reduction Strategy

As each design phase introduces a greater level of detail this invariably means additional failure modes. In order to remain within requirements or mitigate significant increases in vulnerability different systems will require attention as the design develops. The UK MOD’s Vulnerability Reduction Strategy is a prioritized list of measures to be applied in this management process:

1. Prevent catastrophic loss (magazine explosion, sinking);
2. Remove single point failures;
3. Concentrate remaining critical elements;
4. Separate alternative sources of capability;
5. Protect remaining vulnerabilities (improve build standard, use armour or shock mounting systems);
6. If all else fails don’t place critical items in areas most likely to be hit.

There is nothing complicated in the above common-sense steps, but they act as a simple basis to focus the analyst and designers. Sometimes critical components or locations are obvious, but with increasing warship complexity the interplay between seemingly unrelated systems becomes important. This is why it is desirable to track vulnerability during the evolution of the design and not just at the end in an audit role. This means measuring against requirements as a design aid to identify where and why vulnerability occurs to generate recommendations and test potential design changes that mitigate vulnerability.

3. Quantitative Vulnerability Assessment

Assuming the vulnerability management process starts from mandated features and keeps track during the developing design, so must quantitative vulnerability assessment be a key part of the design process from the earliest concept to build and beyond. It is never too early to consider vulnerability, with the biggest gains to be made for the least cost by considering vulnerability in the earliest structural layouts. The later vulnerability is considered, the more limited the scope for design change and the greater the cost of the more limited changes available. The cost attributed to vulnerability management should be judged against the potential cost of doing nothing – which is the unnecessary loss of ships and ship's company.

A vulnerability assessment requires representations of the platform under consideration, the threats which it is designed to withstand and the scenarios in which the two interact.

3.1. Platform representation

For effective assessments to identify all potential vulnerabilities the vulnerability model should cover:

- Hull and superstructure;
- Additional external features such as skegs, sponsons, walkways and bulwarks;
- Internal decks and bulkheads;
- Stiffening;
- Equipment components relating to Float, Move and Fight capability;
- Cables and pipes for associated distribution systems sufficient to represent all primary and alternative modes of operation;
- Crew disposition(s);
- Logical representation (as fault trees) of the range of Float, Move and Fight functions discussed above.

The fidelity of the model must be sufficient only for the fast-running damage algorithms built into the assessment code, thereby allowing many thousands of damage locations to be assessed in a short space of time. For instance, a particular bulkhead might be represented for blast purposes by a single panel with thickness and material specification rather than being a meshed structure as would be seen in a Finite Element model. Stiffeners are similarly represented in terms of their geometric and material characteristics to assess their effect on fragmentation spread, whipping and residual strength. In order for vulnerability assessments to keep pace with and guide the direction of the developing design, the platform representation needs to be constructed rapidly, within a handful of weeks, and must be modified readily as the design changes or as options for particular design features need to be compared.

3.2. Threat representation

The Design and Extreme Threats discussed above must be identified and characterised, in terms of their fusing, blast and fragmentation effects in particular.

3.3. Scenario representation

A standard assessment defines uniform distributions of trajectories on which the threat may approach the platform, on each trajectory the effect of damage (e.g. blast, fragmentation, shock, whipping, flooding) will be assessed on structure and systems. Typically for a design process port and starboard orthogonal directions are sufficient to identify all vulnerabilities, although more directions are often used for the wider parameter spaces discussed below.

Other types of scenario might consider attacks in a specific region of the platform to compare the performance of different design options, the risk from and consequences of a weapon affecting stored munitions, or attacks likely to affect the ability of the crew to move around the platform in the case of an Escape & Evacuation assessment.

3.4. Parameter spaces

The extension to the ability to undertake vulnerability assessment of new designs is the ability to characterise the vulnerability of the fleet as a whole for wider operational analysis, whilst the flip-side of vulnerability assessment is lethality assessment to understand and optimise the capability of weapons to achieve results across a wider range of scenarios. Thus there is a variety of parameter spaces which a tool needs to address if a single consistent approach to be achieved.

4. Purple Fire

4.1. Overview

Under development since 2013, SCL's Purple Fire tool facilitates the sorts of assessment required for modern platform designs, weapon programmes and operational analysis in support of the fleet. Its formal benchmarking against the UK's extant assessment tool in 2017 marked its maturity, whilst the tool proved itself efficient and capable.

It represents the distillation of SCL staff's combined nine decades of experience in naval vulnerability & lethality assessment into a single comprehensive modelling environment. It simulates both target platforms and threat weapons together with a diverse range of potential scenarios for their interaction. A platform target model contains all of the required aspects, a case study of which is presented later.

A full range of threats can be modelled including their payload, fusing and kinetic characteristics, penetration performance and fragment distributions.

A vast range of possible threat-target interaction scenarios can then be simulated giving the analyst complete freedom to specify attack locations, salvos, targeting biasing, etc... Each encounter is simulated to assess the impact of all the relevant damage mechanisms: external / internal blast, fragmentation, shock, whipping and bubble jetting as well as secondary effects like fire and flooding.

Such simulations generate a wealth of output data for analysis including equipment & system vulnerabilities and crew casualties in both statistical and graphical forms, supporting the analyst to rapidly determine problems and suggest their mitigation.

Built from the outset to handle vast data sets, it is ideally suited to running complex optimisation studies involving multiple target threat combinations over diverse scenarios. Moreover, Purple Fire's capabilities differentiate it from other available tools in a number of areas. Many of these relate to specific details of great importance to the user but not the wider stakeholder community. However, a number of substantial features are worthy of expansion here.

4.2. Efficiency

The main strength lies in the efficiency of platform model building, parameter space definition, simulation and analysis, which take significantly less user and processor time than predecessor codes. All of these aspects are facilitated by the fact that the tool stores all input and output data in spread sheets manipulated by an Excel add-in. Experience showed that given a bespoke tool, analysts tend to end up writing pre- and post-processors and manipulating inputs and outputs in Excel anyway. This should not give the impression that Purple Fire is "just a spreadsheet tool", far from it. Rather it should show that the tool has a very efficient method for data entry and analysis, built on a standard application used by all engineers.

4.2.1. Ease of platform build

The spread sheet nature of the data allows the user to see, interrogate and manipulate multiple parts of a model with ease, duplicating and editing components in an intuitive manner. In general form the representation of targets is similar to other vulnerability codes but editing of complex compartment layouts is easier and there are specific improvements such as the amount of structural detail possible. Figure 2 illustrates the explicit stiffener definition and visualisation possible. This is used in the simulation of residual strength, underwater whipping and also has an effect on the penetration of fragmentation through a platform.

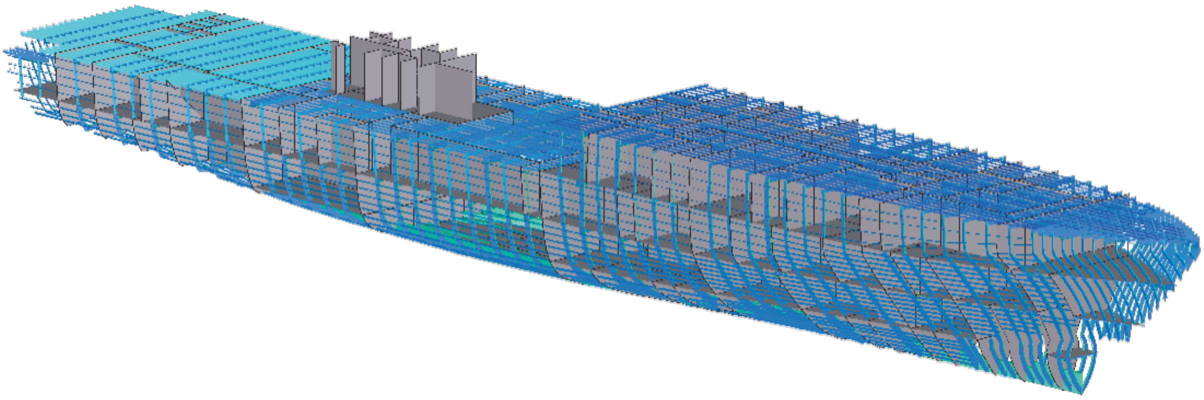


Figure 2: Example structural detail

The functionality built into the platform model can be efficiently displayed in the form of Block Diagrams representing the possible ways of performing a given function. For example, there may be redundancy of power supply to a given user, with power taken from one of two switchboards, each of which is supplied from a different diesel generator. This is represented by a diagram of series and parallel legs, where if a route can be traced from top to bottom without passing through an undamaged item the function is deemed to be available. The functions can very quickly become extremely complicated – imagine the diagram for a Destroyer's ability to provide AAW – but by breaking this up into small chunks and providing robust visualisation the tool helps the analyst understand the functions. An example of a real function, expanded to a limited degree but illustrating the convenient viewing of a high level of complexity, is shown in Figure 3 (where it is not expected that the text be readable at the scale of this document).

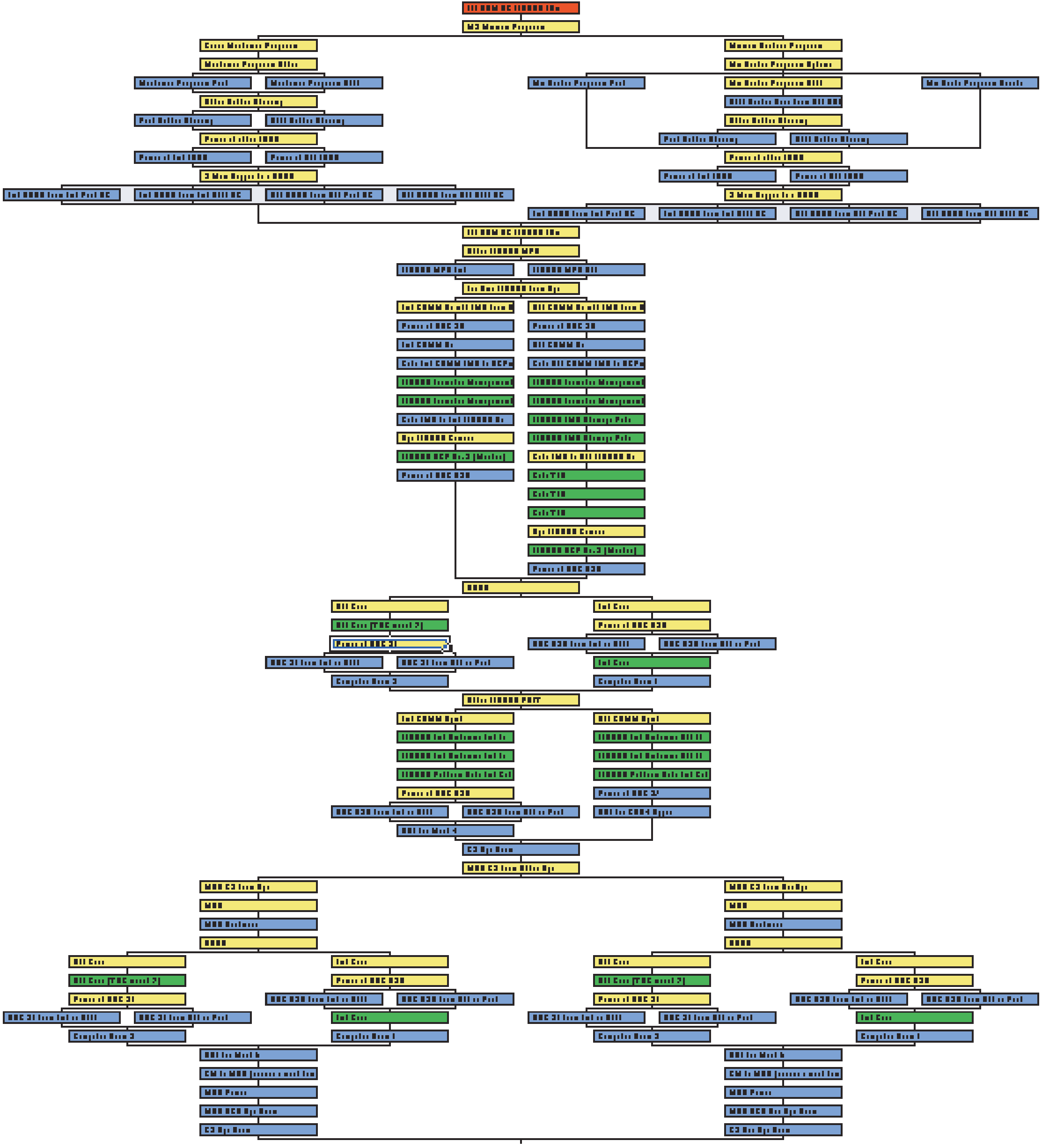


Figure 3: Example Functional Block Diagram (text not expected to be readable at this scale)

4.2.2. Automation of parameter spaces

Perhaps the biggest advance is the ease with which parameter spaces can be set up without resorting to separate pre-processors or text editing tools. A parameter space can be configured from a range of input variables, such that a single input line can represent a wide range of simulations. For example, a single entry to test a set of design variants against a range of missiles from a range of angles might be:

- Target=variant1, variant2, variant3;

- Threat=missile1, missile2, missile3;
- Azmiuth=0,45,90,135,180,225,270,315;
- Elevation=0,15,30,45;
- GridSeparation=1.

Thus a parameter space of 3x3x8x4=288 grids, each of potentially thousands of attack trajectories separated by 1m, is automatically populated. In real-life cases a single line of parameterising can represent thousands of grids, thus huge parameter spaces can be set up very simply. Importantly, this leaves easy checking with all inputs on one screen, and low probability of user error. This is in contrast to more manually intensive methods of setting up individual files and folders for different scenarios, even with the aid of external tools.

4.2.3. Automation of parallel processing

The resulting parameter space is then automatically deployed for simulation across multiple processors, with efficient error handling meaning that should an individual grid crash (and despite a robust code this is always possible) this is coped with gracefully and there is no knock-on effect to other simulations.

The efficiency of processing is such that in a substantial benchmarking of the new capability against its predecessor, runtime and file storage were reduced by up to an order of magnitude for an exactly equivalent parameter space.

4.2.4. Automation of data analysis

Experience has shown that a standard set of a small number of types of results table are desired by the user for the range of assessments normally undertaken. The generation of these are again automated, with the user specifying a number of analysis tables, each according to what parameters should be fixed or varied, with the code instantly extracting results for analysis in consistently formatted outputs without the possibility of the user error normally applicable in the manipulation of data in spread sheets.

4.2.5. Overall efficiency

The combined effect of the above aspects is a saving in the effort required for assessment tasks of around 20%, higher in the case of the most complex parameter spaces, which makes vulnerability advice available even more readily in the design process and at lower cost.

4.3. System criticality assessment

The design process of a warship is typically time-constrained and the quicker recommendations can be made the more likely they are to be taken up. This was the impetus the development of the system criticality algorithm to provide threat independent analysis of target model's system fault trees through the identification of the critical items in the tree. Instead of using a threat with a given damage potential as during a vulnerability assessment, the criticality algorithm systematically assesses each system to determine the effect of its constituents on the overall fault tree. This method only requires a sub-set of the total data required in a target model (i.e. basic structural definition, equipment location and logical "Float", "Move" and "Fight" systems) and can be completed much faster than a vulnerability assessment.

Criticality analysis identifies the importance of the components of a system (be it "Fight" or "Move"):

- Critical Items: items which if killed disable the parent function (coloured red in diagrams);
- Redundant Items: items which if killed in pairs will disable the parent function (coloured yellow in diagrams);
- Dual Redundant Items: items which if are killed in triplets will disable the parent function (coloured blue in diagrams).

Of course, the reason why equipment criticality cannot replace lethality/vulnerability assessments is because a target's systems have both physical location as well as logical definition, as illustrated in a generic example in Figure 4. This shows the criticality of equipment for an anti-air warfare system.

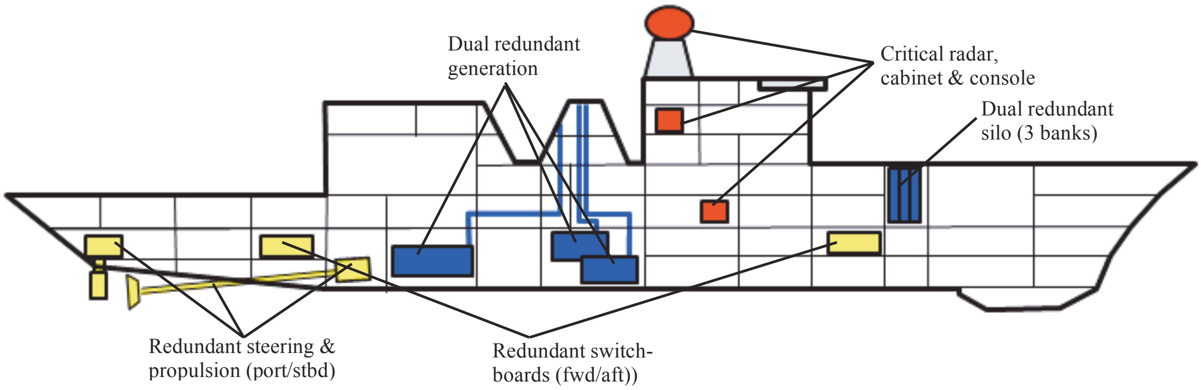

Dual redundant generation
Critical radar, cabinet & console
Dual redundant silo (3 banks)
Redundant steering & propulsion (port/stbd)
Redundant switch-boards (fwd/aft))

Figure 4: Equipment coloured by criticality for an example AAW system

The essential limitation of equipment criticality is evident from Figure 4 as the colouring of items doesn't identify which pairs or triplets are grouped together. Consequently, while critical items coloured red means that disabling any of these items kills the parent function, in contrast, we cannot tell which of the redundant items coloured yellow need to be killed to kill the parent function. All that can be said is that two of these redundant items must be disabled.

More useful for vulnerability/lethality estimates is the generalisation of criticality to compartments. In this case each compartment's criticality to the function is determined primarily by its own contents but also regard to the contents of adjacent compartments. A pair of compartments whose kill will disable the function is coloured yellow, but if these compartments are neighbours then the kill may be easier, so they are upgraded to orange. This generalisation is useful since it can identify regions to target to kill the ship's function (provided that the weapon is big enough to cause damage). The generic example of this is shown in Figure 5.

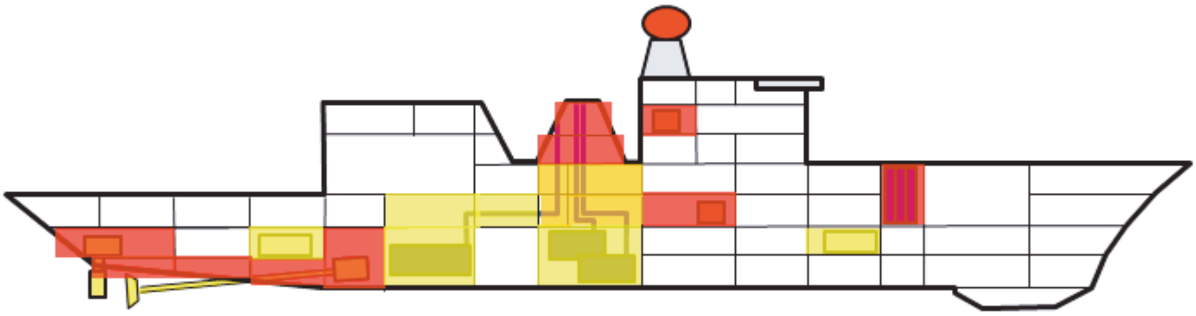


Figure 5: Example compartment criticality based on equipment contents

From Figure 5, a number of key effects are shown which are typical of criticality analysis. This includes:

1. The missile silo as a whole is critical even though the individual cells are not;
2. The same observation applies for the funnel;
3. The aft and forward machinery spaces are redundant and both must be killed to disable the system;
4. Both gearboxes (also both shafts) are in the same compartment making it critical;
5. Both switchboards must be killed to disable the electrical system.

Note that, again, Figure 5 alone cannot identify which yellow compartments must be killed together without further knowledge on the system. However, just as compartment criticality can reveal which pairs of equipment must be killed, compartment pairs can be identified by extending criticality to the zone level.

The benefit of criticality assessment is that it can rapidly identify:

1. A general level of robustness of the target before even assessing vulnerability;
2. Optimisation of weapon targeting in lethality assessments.

4.4. Crew movement

Beyond the desire to simply build low-vulnerability warships the UK MoD has a established duty of care to its personnel including ensuring a design possesses adequate lifesaving and abandonment measures. Quantitative vulnerability analysis can also aid in this. Purple Fire links to the world-class maritimeEXODUS (mEX) code developed by the Fire Safety Engineering Group at the University of Greenwich in order to undertake E&E assessments.

mEX represents multi-compartment geometry of the vessel and the spaces within which the agents can move as a mesh of nodes linked by a system of arcs. Each node represents a region of space typically occupied by a single agent.

The node network can be quite complex given the geometry of a ship, as can be seen in Figure 6. This also shows the outline of the hull and other obstacles which provides the physical interpretation of the node network. A complete ship model can be built from multiple deck geometries linked by user-definable ladders or stairwells.

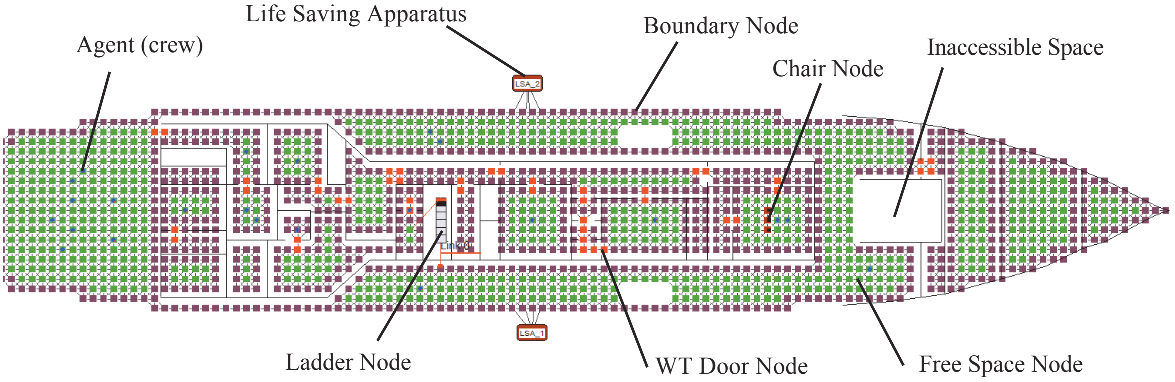


Figure 6: Example of ship geometry and associate node network

The now-recognised benefit of this approach over legacy hydraulic tools is that human abandonments are subject to uncertainty and cannot be realistically described deterministically.

The modelling of agent behaviour in mEX is probabilistic and each individual simulation will result in different predicted timings and outcomes based on the particular agent behaviour. This includes random door opening times and stair traversal times (between the maximum and minimum allowed time) and probabilistic behaviour in overtaking, congestion avoidance, etc. Consequently, simulations are run multiple times to ensure the output variables have converged to stable values.

mEX can also account for the effects of static heel and trim on agent motion, timings to open doors and transverse stairs etc.

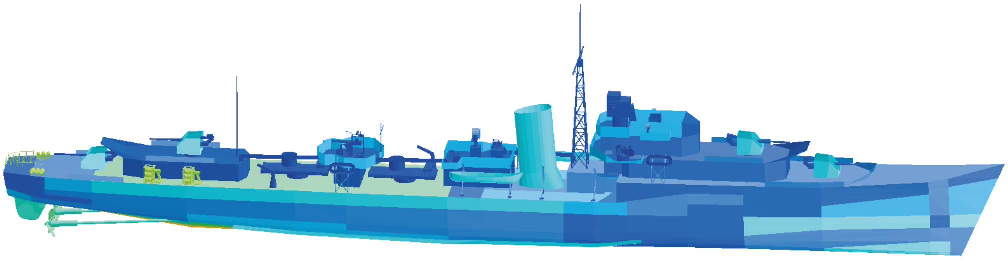
mEX also has the ability to incorporate dynamic hazards to agents as the simulation progresses. This includes pre-determined fire hazards such as heat, smoke and toxic products which are calculated from other software tools. These act to modify the agent's ability to move through the network. It can force the agents to crawl to get under the smoke or divert to alternative routes if blocked by the hazard. Finally, agents are killed if their defined thresholds are exceeded e.g. if they are overcome by smoke or toxic products.

The link is designed to automatically launch numerous mEX simulations automatically based on the details of the target model and the damage experienced by the threat. The link allows the user to:

- Automate the creation of an undamaged baseline mEX model from the vulnerability model;
- Automate the creation of battle damaged mEX models and extract timings back into the vulnerability assessment to create statistical E&E and recoverability metrics.

4.5. Historical case study: HMS Cassandra

HMS Cassandra was a WWII Emergency Class (EM) Destroyer laid down at the start of 1943 and finished in summer 1944. Its sister HMS Cavalier is still preserved in Chatham. The EM class benefited from several of the lessons learned from for first years of the war such as duplication and separation of steering gear cables, shock protection of communications aerials and had a small amount of fragment protection around the guns. The vulnerability model in Figure 7 was built using historical sources from the war and post-war trials on EM destroyers.



http://doi.org/10.24868/issn.2515-818X.2018.024

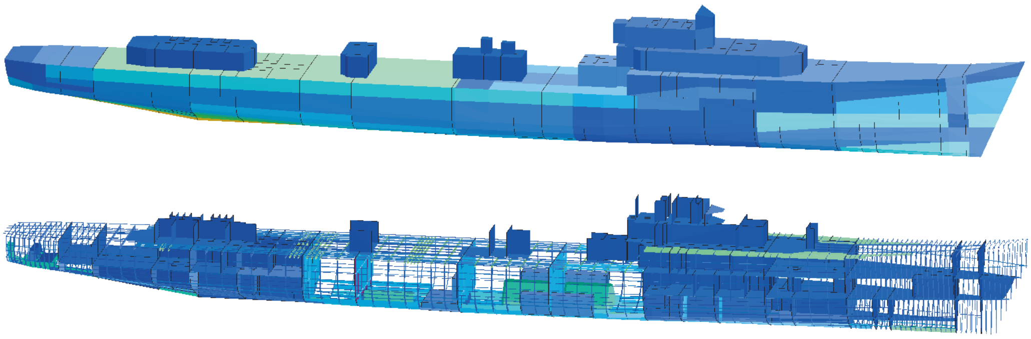


Figure 7: HMS Cassandra Structural model

At 2200 tons standard displacement, 100m length overall and with a beam of 10.9m, HMS Cassandra was small by current standards. Some would now argue that it would be too small to build in survivability features. As an illustration to the contrary, the WWII analysis of the main steering system (on the lines of Figure 1) has been revisited. Options were considered for upper and lower cable routes, with those on the starboard side visible in Figure 8.

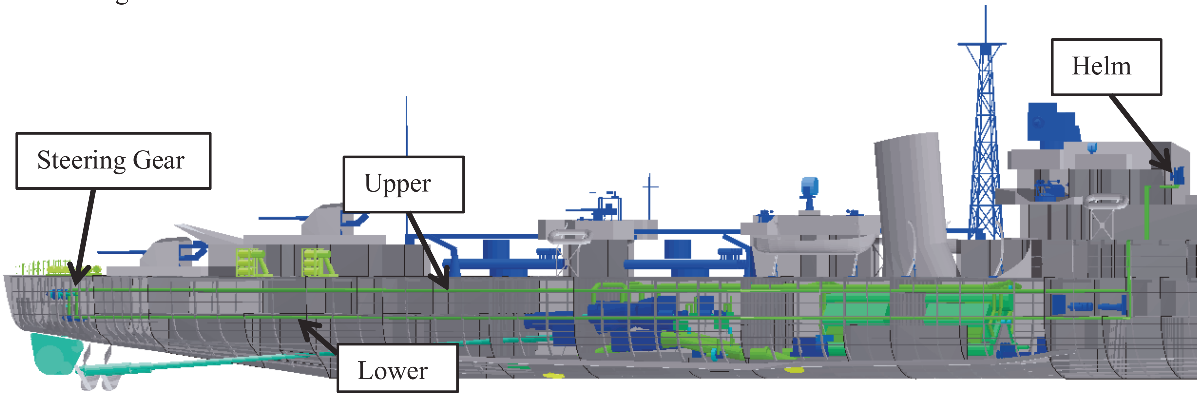


Figure 8: Starboard cables from helm to steering gear upper and lower routes

With similar positioning of cables on the port side, a total of four routes were evaluated. The availability of steering was considered assuming that either one of the routes was installed or a redundant pair of the routes was installed.

Two grids of attack points were used from port and starboard sides, the first covering the profile starboard side of the ship as shown in Figure 9 and the second being similar but set in the horizontal plane simulating bombs dropping from above, passing from starboard to port landing from 35m short of the starboard side up to the centreline.

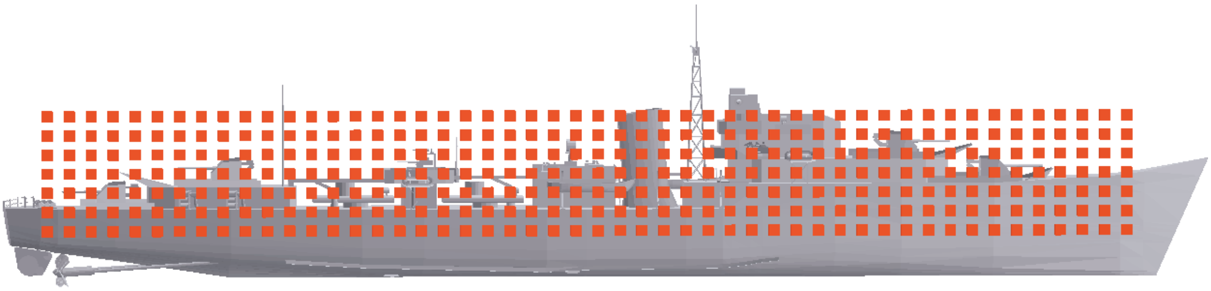


Figure 9: Profile grid used for missile/shell attacks

The weapons used were an aircraft’s 20mm high explosive (HE) cannon shell, an externally detonating 250lb HE bomb, a 5in delayed action HE shell and a small anti-ship missile from the post-war period. An individual shot of the 20mm cannon shell in Figure 10 shows that the WWII predictions in Figure 1 underestimated the angle of the initial fragmentation cone.

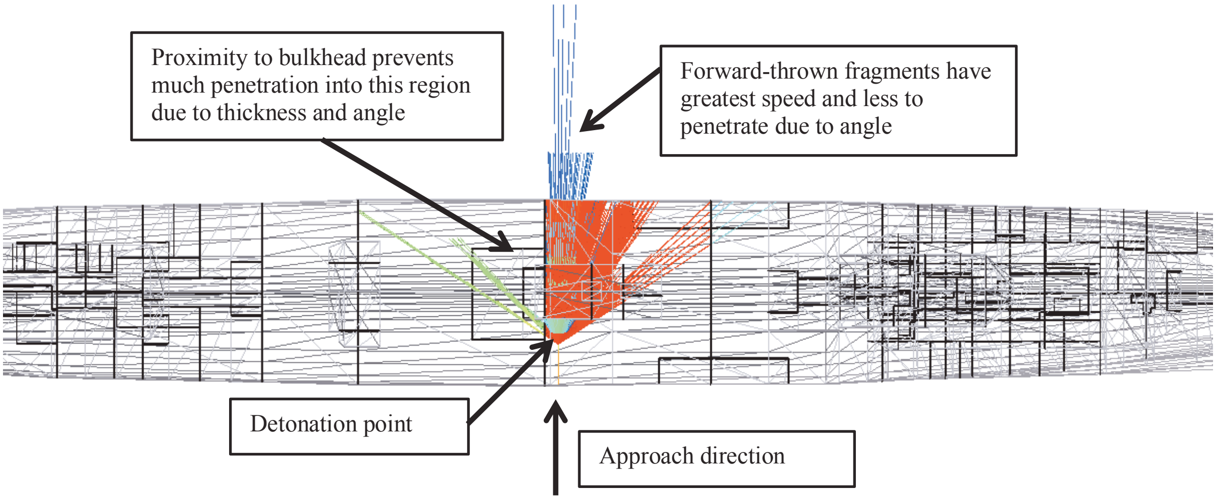

Proximity to bulkhead prevents much penetration into this region due to thickness and angle
Forward-thrown fragments have greatest speed and less to penetrate due to angle
Detonation point
Approach direction

Figure 10: Example of cannon shell fragment spread

Similarly, the bomb fused off the water in Figure 11 shows how fragments can pass through to the far side of the vessel as predicted in Figure 1.

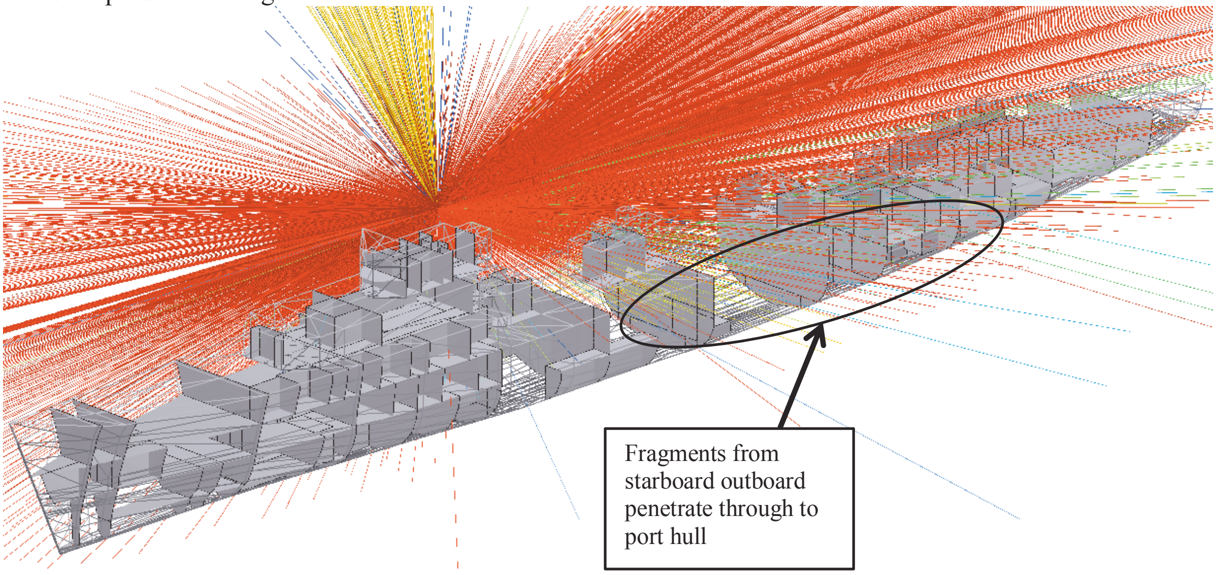

Fragments from starboard outboard penetrate through to port hull

Figure 11: 250lb bomb detonating on water alongside

Table 1 shows the percentage chance that the steering system is lost (i.e. its vulnerability) for the different design variants. The bomb shows substantial benefit from duplicated cable runs as predicted in WWII, with the change now shown to cut the steering vulnerability by a factor of four. Deeper analysis showed that a lower cable on the side closest to the detonation is the most vulnerable because it is swept by the heaviest fragments and the cables on the opposite side are less vulnerable as the internal equipment and structure soaks up the fragmentation.

Also as expected, it is the cables on the far side of the vessel that are more at risk from shells. These small weapons give much lower vulnerability to single hits (although multiple hits can also be considered) but the relative change is even greater than that for the bomb and up to a factor of ten for the 5” shell.

The anti-ship missile has a more extensive fragmentation pattern and internal blast than the bomb, therefore shows less benefit from the duplication, but nevertheless there is still a useful gain to be had, up to a factor of two between the diagonal pair and a single upper route.

Table 1: Vulnerability of steering system for different cable options

Weapon	*Upper single*	*Lower single*	*Upper pair*	*Lower pair*	*Diagonal pair*
250lb bomb	34%	31%	10%	8%	8%
20mm cannon	3.1%	1.5%	0.9%	0.5%	0.4%
5" HE shell	2.8%	2.2%	0.2%	0.2%	0.2%
Small ASM	36%	27%	26%	20%	17%

Without the benefit of modern assessment tools, the EM Class was implementing lessons from damage events to significantly reduce vulnerability for little cost.

5. Conclusions

Warship vulnerability reduction is not a new topic, having been undertaken since World War II. Historical lessons can still be relevant to modern designs, which also benefit from robust policies and procedures for requirements specification, vulnerability management and quantitative assessment. In recent years the required vulnerability/lethality assessments for new designs (including option assessments) and in-service operational analysis have required increasingly complex scenarios and parameter spaces. The Purple Fire tool has been built for efficiency of model building, preparation, simulation and analysis of such assessments.

6. References

Director of Naval Construction, “Notes on damage caused by enemy action and lessons learned during the first year of war Sept 3rd 1939-Sept 2nd 1940”, ADM 267/141, November 1940.

Director of Naval Construction, “Notes on damage caused by enemy action and lessons learned during the second year of war Sept 3rd 1940-Sept 2nd 1941”, ADM 267/142, 1941.

Director of Naval Construction, “Notes on damage caused by enemy action and lessons learned during the third year of war Sept 3rd 1941-Sept 2nd 1942”, ADM 267/143, 1942.

Director of Naval Construction, “Notes on damage caused by enemy action and lessons learned during the fourth year of war Sept 3rd 1942-Sept 2nd 1943”, ADM 267/144, 1943.

Naval Construction Research Establishment, “Underwater Explosion Trials against HMS Jervis in Lock Striven”, NCRE/R88, March 1949.

Naval Construction Research Establishment, “HMS Obdurate Report of Damage Sustained during NCRE Investigation TF13 (Bulkhead Trial)”, DGShips/XCI/IOI/C33A, October 1964.