Risk Assessment Reference Guide For Small Craft

A method for demonstrating safety for innovative vessels and products







HYDROGEN AFLOAT

HPiVS

Executive Summary

As marine technology evolves, manufacturers and designers are increasingly developing products and systems that are not covered by existing regulatory standards. From alternative propulsion technologies and advanced battery systems to hydrofoils and new materials, innovation is moving quickly, creating new challenges for those responsible for demonstrating product safety.

The industry needs a consistent, structured approach to assessing these emerging risks. This guide has been developed to help meet that need. It offers practical guidance on how established risk assessment techniques can be applied to small craft and includes templates.

Why use risk assessment?

The purpose of risk assessment is to ensure that hazards are identified and mitigated in a manner proportionate to their threat to safety. There are countless risk assessment methods in use across, not just all sectors of industry but also in society at large e.g. safety of school outings.

Many industries, for example, automotive, train and aerospace, have come together in recommending a select few risk assessment methods. They have done this so that the industry as a whole will become familiar and increasingly expert at the application of those methods. It also harmonises the language and, where appropriate, the metrics used by the industry.

The authors of this Risk Assessment Reference Guide for Small Craft are advocating the following three methods of risk assessment for the boat building industry:

1. Hazard Identification
2. Failure Modes & Effects Analysis (FMEA)
3. Bow-Tie Analysis

These methods have not been created by the authors and are well recognised in a range of industries. These tools can be useful as part of the design and construction of new craft, or when modifying existing vessels. Depending on the scope of work, one, two, or all three of the tools may be applied.

Any process should be outcome focused. It is only useful if it results in the application of measures (mitigations) or gives assurance that risks are already controlled to be as low as they reasonably can be.

Contents

1 Hazard identification (HAZID) 4
2 Risk Bow-tie Assessment 5
Reporting a Bow-tie Assessment 6
3 Failure Modes and Effects Analysis (FMEA) 7
3.2 Risk Assessment 9
Frequency of Occurrence 9
Severity of Consequence 10
Risk Acceptance 10
Post-Assessment Review & Actions 11
Risk Assessment Principles (RAP) 12
RAP 1: Code of practice 12
RAP 2: Reference system 12
RAP 3: Explicit Risk Estimation 12
Safety targets 12
ANNEX 1: HAZID Template 13
1. Project / Modification Details 13
2. HAZID Register 14
3. Summary & Sign-off 15
ANNEX 2: Bow-tie report template 16
1. General Information 16
2. Bow-tie Summary Diagram 17
3. Core Bow-tie Data Table 17
4. Threats and Preventive Barriers 18
5. Consequences and Mitigating Barriers 18
6. Escalation Factors (Optional but Recommended) 18
7. Assessment Summary 19
8. Sign-Off 19
ANNEX 3: Example Fault Tree Analysis (FTA) 20
ANNEX 4: Glossary 22
About the authors 23

1. Hazard Identification (HAZID)

HAZID is a simple process whereby a group of suitably competent and experienced people are brought together in a "workshop" to generate a list of hazards that could be relevant to a planned scope of work. Many refer to it as 'brainstorming'.

The first step is to have a clear definition of the scope: the "system boundaries". This should consider the physical asset, whether it includes any fixed infrastructure or spares, maintenance and operation. For bigger changes it may be appropriate to employ a facilitator to manage input and ensure the discussion is fully documented.

There are techniques, like the use of key words, that can help generate a list of hazards. The machinery industry's standard **ISO 12100 "*Safety of machinery – General principles for design – Risk assessment and risk reduction*"** has been developed expressly to help in this process. While this is not a marine standard, for systems and components within a boat, this standard is very well suited for a HAZID and only the relatively obvious water-related hazards are missing from this document.

A good HAZID is the starting point of a good safety assessment. See ANNEX 1: *HAZID Template*.

The purpose of the HAZID workshop is not to agree hazards or develop appropriate mitigations (something that engineers are naturally attracted to do), but to generate a full and complete list of hazards.

HAZIDs are most effective where they include a diverse group of people.

It has been shown, post-incident, that "group think" can cause some key hazards to be missed. This might occur when the clear consensus of the group is that a hazard is of so little concern that it need not be listed. It is not for the HAZID team to make this judgement. The risk assessment that follows the HAZID should be the judge of this.

Even if only one member of the HAZID team believes a hazard is applicable, it should be listed as that person might have experience that the others have not.

HAZID needs imaginative thinking of what could (not what has) occurred.

HAZIDs must apply lessons learnt from marine or other sectors/industries and not just reprint a previous report of something similar.

2. Risk Bow-tie Assessment

A risk bow-tie is a "*barrier*" risk model. The concept of barriers to prevent hazards becoming consequences is a well-established safety principle. It is also a graphical method.

At the centre of the bow-tie is a single event: usually something that happens relatively quickly and in an uncontrolled way. Care should be taken when drafting the event being considered. It needs to be broad enough to be useful, without being so high-level that it is too generic. A good example might be "sudden loss of containment" for a fuel system or "sudden loss of stability" for a vessel.

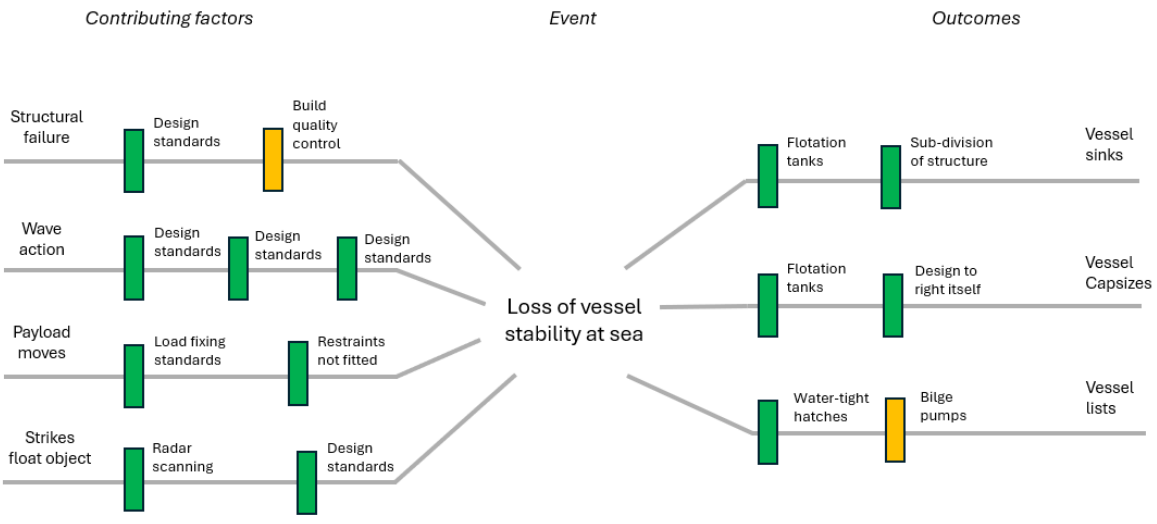
On the left-hand side of the bow-tie are the threats: the things that could contribute to the event occurring.

On the right-hand side of the bow-tie are the outcomes: the consequences of the event.

On each of these branches are the "barriers" to prevent the cause or consequence from occurring.

Barriers can take different forms (physical, design, operational controls etc) and can range in effectiveness. Sometimes colours are used to categorise the effectiveness of a barrier, with green indicating an effective barrier, through yellow to red for less effective measures. A simple example to illustrate the 'philosophy' of the assessment is given below.

Figure 1 – Illustrative example of a Bow-tie Assessment



- Start with a clear top event - it should be a single, controllable “loss of” control point (e.g., “Loss of containment”, “Loss of steering”).
- Keep barriers specific and verifiable - avoid vague phrases like “good training.”
- If working in an organisation, always identify who owns each barrier.
- Use the same matrix as in your HAZID for traceability.
- A template for recording bow-tie assessments, from initiation to conclusion, is given in ANNEX 2: *Bow-tie report template*.

The value of a bow-tie assessment is that it creates a picture of risk management, enabling people to understand the connections between mitigations and consequences. Bow-ties can also be useful when investigating safety failures and it can be useful to update bow-ties whenever significant modifications, incidents, or operational changes occur.

Reporting a Bow-tie Assessment

There are many commercial and free-to-use tools on the internet for drawing the bow-tie diagram but as it consists of simple graphics, no specialist software is necessary. The bow-tie can be used as a checklist to ensure that all mitigations and controls are in place.

3. Failure Modes and Effects Analysis (FMEA)

Understanding the relationship between the functions of things, and what the effect of their failure can have on outcomes, is at the core of FMEA. FMEA can be performed at a whole craft level, at system level, or sub-system level. It can help to identify improvements to design to reduce risk, documenting the decision made during the development of a product. It can be performed by an individual with appropriate knowledge but is best performed by a team with a range of skills and experience.

It is helpful to start with a requirement specification, a list of features that define a product, split out into discrete functions. For example, the primary function of a fuel tank is to safely store a quantity of fuel, but it may also provide support of a fuel level sensor, form connection points for fuel hoses etc, which are secondary functions. Key words can help ensure that a complete list of functions is defined. Elements may have a few key functions, and many secondary or supporting functions. The functions are best listed in a spreadsheet, with columns for primary and secondary functions for each element.

Once the functions have been defined the potential failure modes can be considered. Key words like “loss of” or “failure to” can help draw out the ways in which an element could fail to fully function. Past failures can be useful experience to inform failure modes, but this can be less effective for new technologies and can fail to identify some less frequent failure modes. Often elements are dependent on each other as part of a system. A fault tree analysis (FTA) can show this inter-relationship.

Lastly, the potential impact of those failures can be assessed; the effect they have on the system to deliver its functionality. Is the failure likely to be obvious, or could the failure be hidden? Hidden failures can lay dormant until the function is called upon, possibly as a mitigation for a risk.

A good example of a hidden failure mode is failure of a fire suppression system to operate when needed. Regular periodic testing of some elements of the system may be possible, but a full system test will not.

It can be helpful to assign a risk priority number (RPN) to each entry in an FMEA. This is simply an assessment of the likelihood and severity of an outcome and can help to focus attention to the areas that need the most risk mitigation.

If data is available, the reliability of a component to fulfil its primary functions can be added to an FMEA. Populating the analysis with failure rates for all components can be time consuming and lead to the conclusion that the system, as a whole, will be unreliable. Such assessment can identify mitigations, like ensuring dual systems are fitted, or identify the areas where system testing is needed as part of maintenance.

3.2 Risk Assessment

Once the hazards have been identified, the relationship between the components of a system is fully understood, and the effectiveness of barriers/mitigation has been considered, it is time to conduct the risk assessment.

The risk assessment is performed in three stages:

1. Frequency of occurrence
2. Severity of consequence
3. Risk acceptance

These are described in the following sections.

Frequency of Occurrence

The likelihood and frequency of occurrence of a hazard is assessed in accordance with Table 1, below.

Table 1 - Frequency of Occurrence of hazardous event quantification (based upon Table c.1 of EN50126-1)

Frequency Level	Description	Example of frequency range based on a vessel item operating 50 hours / year over 10 years	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000h / year
Frequent	Likely to occur frequently. The event will be frequently experienced	More than once within a period of approximately 6 weeks	More than about 150 times
Probable	Will occur several times. The event can be expected to occur often	Approximately once per 6 weeks to once per year	About 15 to 150 times
Occasional	Likely to occur several times. The event can be expected to occur several times.	Approximately once per year to once per 10 years	About 2 to 15 times
Rare	Likely to occur sometime in the system lifecycle. The event can reasonably be expected to occur.	Approximately once per 10 years to once per 1000 years	Perhaps once at most

Frequency Level	Description	Example of frequency range based on a vessel item operating 50 hours / year over 10 years	Example of equivalent occurrence in a 30 year lifetime of a single item operating 5000h / year
Improbable	Unlikely to occur but possible. It can be assumed that the event may exceptionally occur.	Approximately once per 1000 years to once per 100,000 years	Not expected to happen within the lifetime.
Highly improbable	Extremely unlikely to occur. It can be assumed that the event will not occur.	Once in a period of approximately 100,000 years or more	Extremely unlikely to happen within the lifetime.

Severity of Consequence

The severity of consequence is assessed in accordance with Table 2 below.

Table 2 - Severity Categories (Table C.4 of EN50126-1)

	Consequence to persons or environment	Consequence to service
Catastrophic	Affecting a large number of people and resulting in multiple fatalities, and/or Extreme damage to the environment	Any of the below consequences in presence of consequences to persons or environment
Critical	Affecting a very small number of people and resulting in at least one fatality, and/or Large damage to the environment	Loss of a major system.
Marginal	No possibility of fatality, severe or minor injuries only, and/or Minor damage to the environment	Severe system(s) damage
Insignificant	Possibly minor injury	Minor system damage

Risk Acceptance

The risk assessment brings together the likelihood and consequence of hazards into table, enabling the acceptability of risk to be quantified and shown in different zones, as shown in Table 3.

Table 3 - Risk acceptance categories (Table C.9 of EN50126-1)

Hazard frequency	Catastrophic	Critical	Marginal	Insignificant
Frequent	Intolerable	Intolerable	Intolerable	Undesirable
Probable	Intolerable	Intolerable	Undesirable	Tolerable
Occasional	Intolerable	Undesirable	Undesirable	Tolerable
Rare	Undesirable	Undesirable	Tolerable	Negligible
Improbable	Undesirable	Tolerable	Negligible	Negligible
Highly improbable	Tolerable	Negligible	Negligible	Negligible

The acceptability of the risks is identified in Table 4.

Table 4 - Risk acceptance categories (Table C.8 of EN50126-1)

	Risk acceptance categories
Intolerable	The risk shall be eliminated
Undesirable	The risk shall only be accepted if further risk reduction is impractical, and the vessel operator positively confirms knowledge and acceptance of the risk
Tolerable	The risk can be accepted with adequate controls (e.g. maintenance procures and operating rules) with the agreement of the vessel operator
Negligible	The risk is accepted without the agreement of the operator.

The risk assessment is best to be recorded in a spreadsheet. One or more mitigations can be identified against each risk that is not negligible.

Post-Assessment Review & Actions

The mitigations identified from the risk assessment above, will form a list of actions that need to be incorporated into the design, testing or operation of the product/system being assessed. The operational aspects need to be shared with the operators. These “exported” mitigations need to be documented, and it is good practice to ensure that the operator acknowledges their role in managing these risks. This might be achieved, for example, by demonstrating that they have incorporated controls into staff training or competence assessment.

It can be useful to re-assess the risk “post mitigation”, considering the revised likelihood or consequence to check that it has been adequately reduced.

When considering mitigations, it can be useful to consider risk acceptance principles as described in the following section.

Risk Assessment Principles (RAP)

RAP can help to set the context of accepting the risk into what is broadly accepted elsewhere. There are three RAPs:

RAP 1: Code of practice

The equipment / change is compliant with an industry standard, code of practice, international standards, or standards that apply to a different industry sector where the differences in operating environment have been considered

RAP 2: Reference system

The equipment / change is like other equipment in use in a similar duty and environment, where an acceptable level of safety has been proven over a period of time.

RAP 3: Explicit Risk Estimation

Where a quantitative or qualitative assessment is undertaken that assesses the likelihood and consequence of the hazard or hazardous event causing harm. This assessment can compare the calculated risk to safety targets.

Safety targets

A safety target is a level of safety that if attained, it is widely agreed that no further work is required to reduce the safety risk further. Safety targets tend to be aspirational, and it is difficult to state with any certainty whether they have been achieved over a short period. If the risk is 1-in-a-1,000 years, the incident would occur once in that period, but it could occur on any specific year, and not achieving the target is only evident when a second incident occurs within the 1,000-year period.

There are two generally accepted safety targets, each related to different levels of consequence. For a catastrophic consequence (see table 2), the value is $1x10^{9}$ incidents per operating hour. For a critical consequence the value is $1x10^{7}$. For one vessel being operated continuously, these correspond to 11,439 years and 114 years.

ANNEX 1: HAZID Template

In this section is a template that may be used for a clean, practical **HAZID.**

It can be amended to suit specific applications as required. It is designed to be simple enough for workshop use but detailed enough for regulatory or assurance purposes.

Excel versions of these templates are also available to download at www.hpivs.com/risk-assessment-guide

---

HAZID (Hazard Identification) Record

1. Project / Modification Details

Field	Description
Project / Modification Title	
System / Location	
Date of HAZID	
Facilitator	
Recorder	
Participants / Roles	(e.g., naval architect, electrical engineer, operations representative, maintainer, safety specialist)
Reference Documents	(Drawings, system descriptions, change request, procedures, etc.)
Related Safety Studies	(e.g., previous HAZOPs, risk assessments, incident reviews)

Continued...

2. HAZID Register

No.	System / Subsystem	Hazard Description	Causes	Potential Consequences	Existing Controls	Status / Comments
1						
2						
3						
4						
5						
6						

Notes:

- **Hazard Description** – State the undesired event (e.g. “Loss of steering control”).
- **Causes** – Identify initiating events (e.g. “Electrical fault”, “Software crash”).
- **Consequences** – Describe the worst credible outcome (e.g. “Grounding or collision”).
- **Existing Controls** – List design or procedural safeguards already in place.
- **Status / Comments** – Track whether actions are open, closed, or require review.

Continued...

3. Summary & Sign-off

Item	Detail
Total hazards identified	
Key recommendations	
Next steps / linked studies	(e.g., detailed HAZOP, FMEA, Bow-tie assessment)
HAZID Facilitator	Signature / Date
Project Manager / Safety Authority Approval	Signature / Date

4. Optional Attachments

- P&IDs, diagrams, system architecture sketches
- Photos or design schematics
- Copies of existing risk assessments
- Workshop attendance sheet

ANNEX 2: Bow-tie report template

1. General Information

Field	Description
Project / Vessel / System	
Assessment Title	(e.g. “Loss of Propulsion Bow-tie”)
Date of Assessment	
Facilitator	
Recorder	
Participants / Roles	(e.g., Master, Chief Engineer, Naval Architect, Safety Officer, Operations Manager)
Reference Documents	(e.g., Design specs, procedures, incident reports)
Linked Safety Studies	(e.g., HAZID, FMEA, safety case)

2. Bow-tie Summary Diagram

(A visual bow-tie diagram shall be added here — "Threats" on the left, "Consequences" on the right, "Top Event" in the centre, and barriers above/below.
If created in software (e.g., BowTieXP, Visio, Power BI), attach or embed a screenshot.)

---

3. Core Bowtie Data Table

Section	Details
Hazard	(What source of danger exists? e.g., Stored energy in propulsion system)
Top Event	(The point of loss of control — the event you want to prevent. e.g., "Loss of Propulsion")
Potential Consequences	(What could happen if the top event occurs? e.g., "Grounding," "Collision," "Loss of manoeuvrability in confined waters")

4. Threats and Preventive Barriers

Threat (What could cause the top event?)	**Preventive Barriers** (What controls prevent or reduce the chance of the top event?)	**Barrier Type** (Technical / Procedural / Human / Organisational)	**Barrier Effectiveness** (High / Medium / Low)	**Owner / Responsible Party**	**Remarks / Actions**
1. e.g. Fuel leakage from hoses	*Compliant fuel-grade hoses fitted & inspected at prescribed intervals*	*Technical*	*High*	*Boat owner*	*Note in Owner's Manual*
…					

5. Consequences and Mitigating Barriers

Consequence (What happens if the top event occurs?)	**Mitigating Barriers / Controls** (What reduces the severity or escalation?)	**Barrier Type**	**Barrier Effectiveness**	**Owner / Responsible Party**	**Remarks / Actions**
1. e.g. Sinking	*Foam-filled flotation voids*	*Technical*	*High*	*Manufacturer*	*Note in Owner's Manual to check integrity*
…					

6. Escalation Factors (Optional but Recommended)

Escalation Factor (What could weaken a barrier?)	**Escalation Control** (How is that factor managed?) …	**Owner / Responsible Party**	**Status / Actions**
E.g. Poor maintenance	*Planned maintenance inspection schedule in Owner's Manual*	*OEM to supply boat manufacturer with manual to be included with the boat / OEM Compliance Team*	

7. Assessment Summary

Risk Summary	Details
Most credible threats	
Most severe consequences	
Barriers identified as weak or missing	
Recommended improvements	
Responsible persons and target dates	
Review frequency / trigger	(e.g., annual, post-modification, post-incident)

---

8. Sign-Off

Role	Name	Signature	Date
Facilitator			
Project Manager / Vessel Master			
Safety Authority / Reviewer			

ANNEX 3: Example Fault Tree Analysis (FTA)

The following is a worked example of a fault tree in table form, for a boat's electric propulsion system.

The columns are organised as follows:

- **Description** – what physically happens
- **Subsystem / location** – where it originates
- **Possible causes** – failure mechanisms or triggers
- **Example failure rate (λ)** – per hour, illustrative typical values based on IEC 61508 data from the automotive industry
- **Primary detection / protection** – how the system can sense or mitigate
- **Recommended mitigation** – design or maintenance control

ID	Description	Subsystem / Location	Possible Causes	Example Failure Rate (λ/hr)	Detection / Protection	Recommended Mitigation
A	Battery internal short / cell thermal runaway	Battery pack	Manufacturing defect, dendrite growth, overcharge, contamination	1×10^{-5}	BMS cell voltage/temp monitoring, pack fuses	Cell screening, pack venting, BMS cutoff, physical partitioning
B	Main contactor fails to open (welded contacts)	HV isolation system	Arcing from high current, wear, coil driver fault	1×10^{-3} (per demand)	Contactor health test, current decay check	Dual series contactors, arc suppression, scheduled replacement
C	DC bus insulation breakdown / water ingress	HV cabling / connectors	Salt spray, condensation, abrasion, corrosion	5×10^{-6}	Insulation monitoring device (IMD), IR test	Sealed connectors (IP67+), routing protection, periodic IR check
D	Insulation monitor / HV interlock fails	Protection / control	Software freeze, loose interlock loop, calibration drift	1×10^{-4}	Self-test on power-up, BMS diagnostics	Redundant IMD, periodic test, watchdog supervision

ID	Description	Subsystem / Location	Possible Causes	Example Failure Rate (λ/hr)	Detection / Protection	Recommended Mitigation
E	Motor winding short / insulation failure	Propulsion motor	Overheating, vibration, water ingress, aging	2×10^{-5}	Motor current imbalance, insulation monitoring	High-grade insulation, temperature sensors, periodic IR test
F	Inverter fails to isolate fault (hardware or firmware)	Power electronics drive	MOSFET/IGBT short, gate driver failure, firmware crash	2×10^{-3}	Hardware overcurrent trip, watchdog, BMS isolation	Hardware cutoff path, software FMEA validation, redundant drivers
G	Cooling system failure (loss of flow or coolant)	Thermal management	Pump seizure, leak, blockage, airlock	5×10^{-4}	Flow sensor, temp sensors, BMS overtemp	Dual pumps, periodic bleed/test, overtemp shutdown
H	Temperature sensor / alarm failure	Thermal management / BMS	Open circuit, miscalibration, software filtering	1×10^{-4}	Sensor cross-check, plausibility check	Dual sensors, independent overtemp trip
I	Human maintenance error (HV connector live, bypassed isolation)	Maintenance / operations	Procedure non-compliance, poor training	1×10^{-3} (per task)	Interlocks, voltage presence indicator	LOTO procedures, training, physical barriers
J	HV fuse or breaker fails to clear fault	Protection device	Mechanical defect, arc quenching failure, rating exceeded	1×10^{-4} (per demand)	Fault current sensor, thermal trip	Proper derating, verified interrupt capacity, testing
K	Communication loss / unsafe control command	Control / CAN bus	EMI, software fault, connector corrosion	1×10^{-4}	Timeout watchdogs, redundant bus	EMI shielding, redundancy, health monitoring
L	Battery Management System (BMS) failure	Battery pack / control	Software crash, power supply fault, CAN loss	1×10^{-4}	Watchdog, redundancy, diagnostics	Dual microcontrollers, safety-certified software (ISO 26262 ASIL C/D)

ANNEX 4: Glossary

European Recreational Craft Directive
Legislation in force in the European Economic Area that sets safety and environmental requirements for small craft, their engines, and their critical components.

Major Craft Conversion
The EU Recreational Craft Directive defines a Major Craft Conversion as a modification of a watercraft which alters it to such an extent that it may not meet the requirements laid down in this Directive. It requires formal certification by a Notified Body.

Notified Body
An accredited certification body authorised by the EU Commission to certify products to one or more EU Directives.

Post Construction Assessment
PCA is defined in the EU Recreational Craft Directive and describes the process where a Notified Body assesses a watercraft after it has been manufactured. It requires certification by a Notified Body.

About the authors:

Alasdair Reay, HPiVS

HPiVS provides independent verification, inspection and certification services to the marine and industrial sectors. With expertise spanning recreational craft certification, marine equipment, pressure equipment, welding and quality assurance, HPiVS works with manufacturers and innovators to help demonstrate regulatory compliance, product safety, and technical integrity. For further information, visit **www.hpivs.com** or email: enquiries@hpivs.com

Nick Swift, Hydrogen Afloat

Hydrogen Afloat develops near-silent, zero-emission hydrogen fuel cell systems to provide clean off-grid electricity for narrowboats and inland waterway vessels. For further information, visit **www.hydrogenafloat.com** or email: nick@hydrogenafloat.com

"Our hope is that this document will be a seed for the industry to develop and publish its own guidance, shaped by the people who build, fit and maintain these boats every day. To encourage that, we are making the guide available free of charge on our website.

"Better risk assessment will make boats safer for the people who use them, and I would encourage everyone in the sector to read the guide, use it, challenge it, and help improve it."
Alasdair Reay, CEO HPiVS

Disclaimer: *The information contained in this Risk Assessment Guide is intended as a general guide for best practice within the recreational marine industry. It does not constitute legal, safety, or technical advice and should not replace independent professional evaluation or consultation. Contributors disclaim all liability for any direct or indirect consequences arising from reliance on using this voluntary guide. Users are responsible for ensuring that their own best practices comply with all relevant national statutory and regulatory requirements and it must not be considered or intended as a legally binding text for any reason whatsoever.*