Naval Safety Command

Safe to Operate and Operating Safely: How the 4Ps Support Risk Resilience

What is Resilience?

Resilience is a system's ability to adjust and sustain normal functioning in the face of disturbances.

Characteristics of a resilient system include: Defense-in-Depth, processes designed for both issue prevention and resulting recovery when an issue occurs, and processes to verify the effectiveness of the system.

Defense-in-Depth *is an approach to designing a system that prevents accidents and mitigates the severity of smaller events. The key is creating multiple independent and redundant layers of defense to compensate for potential human and mechanical failures so that no single layer, no matter how robust, is exclusively relied upon to prevent an accident. This approach defends against latent, unrealized weaknesses in a system that can be triggered by active errors (unsafe behaviors carried out by individual parties).*

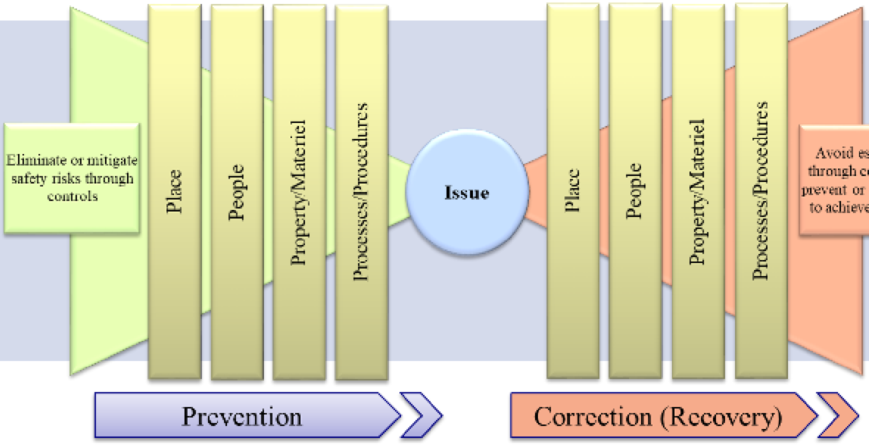
Risk resilience is a systems view of risk controls that protects people and materiel and also effectively prevents or de-escalates issues leading to increased severity of harm such as an effective emergency response and actions that correct smaller issues before they become larger issues. Effective self-assessment and self-correction improves risk resilience.

No one goes to work intending to cause a mishap, but error is a normal by-product of human performance especially in the demanding, repetitive, dynamic and complex operating environments associated with naval and industrial activities. Post-mishap investigation and analysis results repeatedly show how overlapping and complex paths of system failures could be linked back to organizational factors, the competence of personnel and local conditions, and are ultimately responsible for promoting unsafe behaviors in every type of operating environment.

System failures occur when risk controls are absent, disregarded, ineffective or fail to account for the inevitability of human error. The mishap therefore, often comes as a complete surprise, as the organization was likely unaware of its actual cumulative risk level. The lack of resilience is evident in the findings from mishap investigations, which more often than not, reveal weaknesses in the organization's ability to identify, assess or control risks.

The Resilience Model

Ensuring an organization meets safe-to-operate standards so it is operating safely is a way to prevent mishaps from occurring **(Prevention)**, and/or reduce the severity when they do occur. The 4Ps are controls to reduce and prevent risk.



When something does happen outside normal operations, the health of those controls together impact the effectiveness of the response and reduce the adverse effects when a mishap occurs. **(Correction Recovery)**

What does it mean to be Safe to Operate and Operating Safely?

Everyone has an obligation and duty to Operate Safely by preserving Safe-to-Operate conditions. Echelon commanders must ensure their commands are Safe to Operate through their management of people, policy and resources, and transparent communication of risk up and down the chain of command.

Per OPNAV M-5100.23 CH-2:
"Safe to Operate" *refers to the as-designed safety for places, property/materiel, people and processes/procedures. It is the defining design, policy, engineering, resourcing and expectation management that sets the safety risk envelope for the hazardous activity or activities for a given operating environment. Original Equipment Manufacturers, Systems Commands, Program Offices and upper echelon commands are primarily responsible for the Safe-to-Operate criteria.* Typically, we see the Safe-to-Operate envelope defined by technical manuals, policies and procedures.

***"Operate Safely"** is executing the mission within the designed safety envelope. The safety envelope is normally maintained by operating within established procedures. When unplanned or unforeseen safety risks manifest outside of the approved Safety Case and the military benefit (operationally defined objective) of taking the risk outweighs the cost of the risk exposure, then commands should apply the principles of operational risk management to control risk.*

The 4Ps are the desired and goal outcomes of the Navy SMS. When an organization's **Place** (workplace or operating environment), **People** (military and civilian employees), **Property and Materiel** (equipment, systems, tools, assets, etc.), and **Processes and Procedures**, meet the requirements established by its governing authorities - the DoD, DON, or echelon commander, for example - to be "Safe to Operate," that organization is "Operating Safely."

The 4Ps per OPNAVINST M-5100.23 CH-2, 5 SEP 2022

Safe Place (ECH III-Unit level)
The condition of the physical operating (and operational) environment. A safe place is a workplace that is free from unnecessary hazards. The chain of command (Echelon II through Unit-Level) must ensure a safe place, equipment and practices are in place and effective to control risks in the workplace, which includes working in warfighting and crisis conditions. The workplace should have the sufficient number of competent personnel needed to maintain designed workplace safety. Commands need to evaluate the entire system to ensure resources are correct to safely complete tasking.

Safe People (ECH III-Unit level)
The absolute safety-critical need for individuals and teams to behave safely. To facilitate this, the organization must ensure enough appropriately trained personnel are qualified, experienced and current for the tasks required of them; that they are also physically, psychologically and mentally prepared (akin to warrior toughness program); and human limitations are accounted for (anthropometric reach, vision, hearing, etc.).

Safe Property/Materiel (ECH I-III)
The high-level management of safety includes resourcing to ensure compliance with Federal Law, DoD and DON policy. Organizational factors also include, deciding on the mission, structure of the organization, provision, allocation of resources and risk appetite. This category encompasses all factors needed for a safe workplace (applicable to the entire spectrum of workplaces from the office environment through frontline warfighting in a ship, submarine or other forward deployed operating base).

Safe Procedures (Unit Level)
This condition supports resilience at the 'sharp-end' of naval operations by prompting safe behaviors in the work environment. Safe actions are dependent on effective leadership and supervision so that personnel routinely work safely and are resourced and empowered to respond to emergent risks and issues. At this level, it is about individuals and teams working within a safety system's boundaries as defined by established standards and procedures. Risks and issues requiring mitigation beyond unit-level resources are elevated to the next higher Accountable Person (AP).

Operating Safely covers all procedures, requirements and conditions for all activities, including routine, day-to-day operations; high-hazard or special operations; or crisis and emergency event operations. To **Operate Safely** is to operate within established procedures, also known as the "safety envelope."

When it comes to Resilience, organizations that preserve the Safe-to-Operate envelope are better able to respond and manage events occurring outside of normal operations, such as a shipboard fire, engine loss in an aircraft or when an amphibious assault vehicle (AAV) starts taking on water halfway between the ship and shore. For example, Marines not properly trained in AAV egress procedures are at a higher risk if an AAV starts to sink, than those who know exactly what to do, when and how. If a fire breaks out on a ship and firefighting systems and equipment are degraded or offline, firefighting efforts are significantly hampered, even if the crew is properly trained and qualified.

Accountability

Everyone has a duty and responsiblity to communicate risk up and down the chain of command, but echelon commanders are ultimately **Accountable** and responsible for ensuring Safe to Operate conditions across the 4Ps and that their activities are Operating Safely. ECH II/III commanders ultimately own the risk for the 4Ps.

ECH II/III commanders are accountable for ensuring their subordinate commands have the available resources to meet the requirements to operate safely. This includes resources such as personnel, training and ensuring availability of the proper tools and equipment, etc., to perform their work safely, to include a safe working environment.

ECH IV/V commanders and unit-level commanding officers and officers-in-charge are responsible for self-assessing and identifying risk at their levels, and *must* elevate risk factors beyond their control to the next appropriate level, i.e., their echelon commander, to evaluate for action or mitigation.

All Navy personnel are accountable for risk communication and must raise all known, discovered or perceived risks and issues to their immediate supervisor or chain of command.

See OPNAV M-5100.23 CH-2 at www.secnav.navy.mil/doni/SECNAV%20Manuals1/5100.23%20CH-2.pdf