Black&McDonald

Safety Bulletin

The ‘Fail-Safe’ Approach

Fail-Safe design is an approach to working in such a way that you can ‘fail’ without causing excessive damage or putting people at risk.

While, preventing error from occurring altogether would be a preferrable outcome, fail-safe design recognizes that this is an impossible goal as people are fallible and even the best can make mistakes. Rather than simply attempting to avoid all failures, fail-safe design plans for the possible failure by finding ways to minimize the adverse effects.

The Fail-Safe Approach aims to ensure that a system has enough integrity to remain safe even when a part of that system fails.

Types of Fail-Safe work designs include:

- **Redundancies** – which essentially build additional capacities into the system that will take over if the primary components fail.
- **Intentional Weak Links** – are cheap and easily replaceable component that can fail first, thereby acting as a shield to prevent damage to more complex or expensive parts of the system.
- **Physical Law** – uses the way certain materials respond to stress and pressure to make components that will fail without catastrophic outcomes.
- **Early Detection** – makes smaller issues and early warning signs easily detectable so they can be addressed before they result in more significant risks.

Can you think of why the objects below are considered part of a ‘Fail-Safe’ approach?