DESIGNING FOR SUCCESS AND THE MITIGATION OF SINGLE POINT FAILURES

22 August 2023

In the world of product design, ensuring the success and reliability of a product is of paramount importance. While designers strive to create innovative and functional products, the risk of single point failures can potentially undermine all their efforts. A single point failure occurs when a critical component or feature fails, causing the entire product to malfunction or become unusable. In this article, we will delve into the significance of assessing single point failures in the design process and explore strategies to mitigate their impact, ultimately leading to better-designed and more robust products.

A single point failure is a weak link in the design that can result in catastrophic consequences. Imagine a smartphone with a faulty battery that renders the entire device useless or a car with a flawed braking system that jeopardizes the safety of passengers. Such failures can lead to financial losses, reputational damage, and, more importantly, endangering users' well-being.

Identifying Potential Single Point Failures:

To effectively assess and address single point failures, designers must identify potential weak points in their product designs. This involves a meticulous evaluation of every component, system, and interaction. Some common areas to watch out for include:

Critical Components: Identify components that are vital to the product's functionality and performance. These components should be analysed for their reliability, durability, and potential points of failure.
User Experience: Examine the product from the perspective of the end-users. Identify areas where usability issues could lead to failures or user dissatisfaction.
External Factors: Consider the product's environment and the external factors it will encounter during its lifecycle. Evaluate how these factors could impact the product's performance and lead to failures.
Interfaces and Connections: Assess the points where different components or systems interface with each other. Weak connections can lead to failures in overall system integration.

One ambitious project with an extreme number of single point failures was the launch of the James Web Space Telescope (JWST), with a staggering 344 single points of failure to address. From intricate mechanisms to deploy mirrors and release pins to various critical functions, the JWST faced a daunting list of potential weak points. In comparison, past missions like the Galileo probe to Jupiter in the 1980s had 30 single point failures, and Mars landings could have over 100. The odds might have seemed stacked against the JWST, but its successful launch demonstrated that single point failures don't necessarily equate to failure.

Mitigating single point failures was the primary focus of the JWST's engineering team. While the lengthy list of potential failures could raise concerns, it also spurred the team to work diligently on enhancing the design's reliability. Despite cost and logistical constraints, the dedicated engineers and technicians spent years subjecting each component to rigorous

testing, envisioning possible scenarios, and conducting meticulous simulations to bolster the reliability of every single point of failure.

The JWST's successful launch was not a stroke of luck; rather, it was the result of meticulous planning and proactive problem-solving. The engineering team strived to maximize the telescope's chances of success, embracing redundancy, implementing fail-safe mechanisms, and continuously refining the design to minimize risks. While uncertainties lingered, the commitment to creating a robust and reliable spacecraft paid off.

"What looks much like craggy mountains on a moonlit evening is actually the edge of a nearby, young, star-forming region NGC 3324 in the Carina Nebula. Captured in infrared light by the Near-Infrared Camera (NIRCam) on NASA's James Webb Space Telescope, this image reveals previously obscured areas of star birth." – Webb Space Telescope

Strategies to Mitigate Single Point Failures:

Once potential single point failures are identified, designers can implement various strategies to mitigate their impact and enhance the product's overall reliability:

Redundancy and Backup Systems: Introduce redundancy by duplicating critical components or creating backup systems. This way, if one component fails, the backup can seamlessly take over, preventing the entire product from failing.
Testing and Prototyping: Rigorous testing and prototyping are crucial steps to identify weaknesses in the design. Real-world simulations and stress tests help expose potential single point failures and provide opportunities for improvement.
Safety Margins and Tolerance: Incorporate safety margins and tolerance levels to allow the product to withstand unexpected stresses or variations without failing.
User Feedback and Iteration: Involve end-users in the design process and gather their feedback. User insights can highlight usability issues and areas of improvement, reducing the likelihood of single point failures.
Fail-Safe Mechanisms: Integrate fail-safe mechanisms that automatically activate in the event of a failure. These mechanisms can prevent or minimize the impact of single point failures on the product's overall functionality.

Diving into another ambitious project, we encounter the OceanGate Titan Submersible, which faced a significant number of single point failures during its ill-fated exhibition to the Titanic on June 18th. While the exact count of single point failures remains uncertain, what is clear is the lack of strategies employed to mitigate these potential risks. Unlike the meticulous attention to detail and precautionary measures seen in the James Webb Space Telescope, the Titan Submersible's design decisions were highly controversial, leading to numerous safety concerns and avoidable points of failure.

OceanGate, the company behind the Titan Submersible, opted not to seek certification from safety organizations overseeing deep-diving crafts, citing that certification might stifle innovation. However, this approach led to critical oversights that compromised the submersible's safety. One such issue was the decision to use a pill-shaped hull made from carbon fibre, instead of the more common and pressure-resistant spherical-shaped hull made from titanium. The pill-shaped hull was chosen to accommodate more occupants,

but its design lacked the even distribution of stresses that a spherical hull provides, leaving it susceptible to weaknesses and potential failures.

Furthermore, the choice of carbon fibre over titanium was driven by cost-saving motives, disregarding the fact that carbon fibre performs better under tensile stress rather than compression despite the fact compression is the force that a submersible must be able to withstand. The integration of titanium hemispheres with the carbon fibre hull introduced additional points of failure at their joints. The Titan experienced numerous pressurization cycles throughout all the tests, potentially leading to defects in the carbon fibre that are near impossible to measure due to the nature of carbon fibre, unlike metallurgy which can be monitored. As the hull was composed of two different materials, during these pressurization cycles each material may have undergone distinct deformations. This could have resulted in permanent deformations or misalignment between the two parts, compounding the complexity of the issue.

Numerous safety warnings were raised, including concerns voiced by David Lochridge, a pilot for a previous OceanGate submersible, saying that Titan was not equipped to reach the depths of the Titanic around 13,123 feet. Before the launch of Titan, Rob McCallum, an experienced expert in submersibles, also issued warnings. Including that unlike every other submersible that uses hard-wired controls, Titan’s control system relied on Bluetooth. This raised concerns because hard-wired controls ensure continued control even if the signal drops, whereas Bluetooth may lead to loss of control under certain circumstances. Unfortunately, these warnings fell on deaf ears, and Lochridge was even dismissed from the company for expressing his safety concerns. OceanGate’s management exhibited a significant deficiency in establishing a proper system for listening to their technical experts, which particularly on a project as unique and high-risk as this, is extremely negligent.

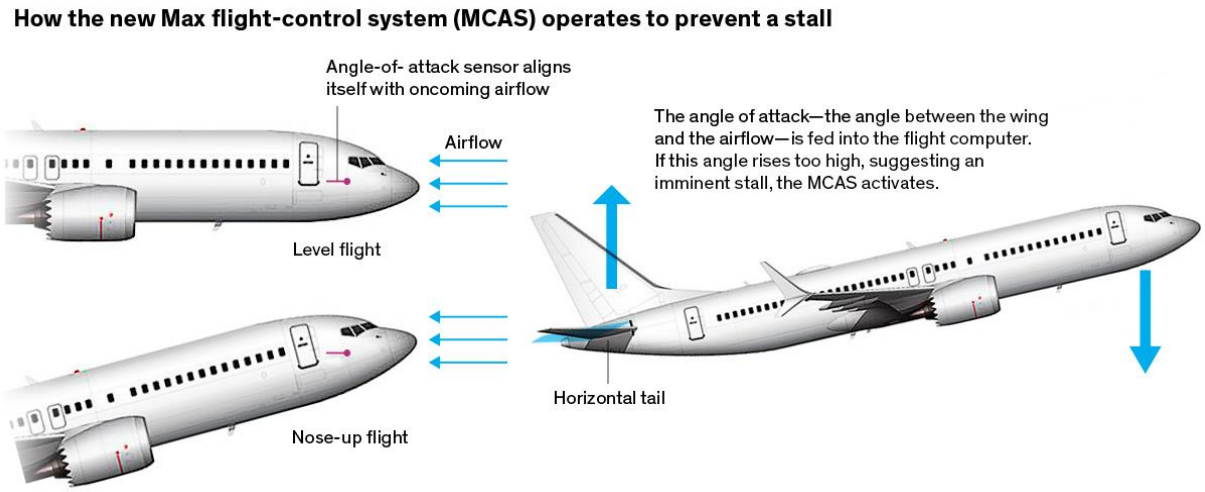
OceanGate’s Titan Submersible serves as a stark example of the consequences that can arise when proper testing, safety measures, and

reliability are compromised in the pursuit of rushing innovation. The unfortunate outcome of the Titanic exhibition was, in part, a result of overlooking essential safety protocols and choosing shortcuts over thoroughness. Such incidents underscore the importance of prioritizing safety and the need for collaborative efforts among designers, engineers, and safety experts to ensure the success and security of ambitious projects like deep-diving crafts. If the designers and engineers involved in the project had been granted greater authority in making design choices, it is highly probable that the product development path would have taken a more favourable and successful direction.

There are instances where companies have tried to address single point failures by implementing failsafe mechanisms, only to find that these very mechanisms become the cause of failure. An example of this occurred with the Boeing 737 MAX, which introduced a new system called MCAS. The purpose of MCAS was to automatically adjust the horizontal stabilizer and trim tab, pushing down the aircraft nose from an elevated angle of attack (AoA) to prevent potential stalls.

However, unlike previous versions of this system, on the 737 MAX, movement of the control column by the pilots did not disable MCAS. Boeing

sought and received approval from the FAA to omit a description of MCAS from the aircraft manual, leaving pilots unaware of the system when the airplane entered service in 2017. This critical information, which highlighted the system's limitations, was withheld by Boeing for at least a year. Tragically, this resulted in pilots being unaware of how to override the MCAS system when it malfunctioned, leading to the plane nosediving uncontrollably and causing fatal crashes. Two such devastating incidents occurred with Lion Air Flight 610 in 2018 and Ethiopian Airlines Flight 302 in 2019, leading to a total of 346 lives lost.



Source: https://spectrum.ieee.org/

The assessment of single point failures is a critical aspect of the product design process. Designers must proactively identify potential weak points and implement strategies to mitigate their impact. By incorporating redundancy, conducting thorough testing, considering user feedback, and integrating fail-safe mechanisms, designers can create more reliable and robust products. Designers bear a significant responsibility in ensuring that the products they create enhance the lives of users rather than endanger them. The pursuit of excellence in product design lies in the continuous effort to identify and address single point failures, ultimately leading to safer, more reliable, and successful products in the market.

*Flynn Product Design offers **product design consultancy**, **industrial design**, **prototype design**, and related services, to ambitious companies.*

SET US A CHALLENGE **BOOK YOUR FREE MEETING** TODAY !