

An electronic glitch can lead to large claims

Automation, digitalization and the use of ships' data is today having a big impact on the maritime industry. While there is no doubt that cyber is a major growing risk in this area, there is, however, still a more common, less hyped and maybe growing type of shipboard technology related risk that should not be forgotten - the reliability, breakdown and [no fault found failure](<https://en.wikipedia.org/wiki/Nofaultfound>) of electronics.

Published 10 March 2020

The information provided in this article is intended for general information only. While every effort has been made to ensure the accuracy of the information at the time of publication, no warranty or representation is made regarding its completeness or timeliness. The content in this article does not constitute professional advice, and any reliance on such information is strictly at your own risk. Gard AS, including its affiliated companies, agents and employees, shall not be held liable for any loss, expense, or damage of any kind whatsoever arising from reliance on the information provided, irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.

The digital data flow on today's ships and the push towards more automation of onboard processes and functions, can have a positive impact on safety, and the commercial, and environmental performance. Combining the data stream from multiple digital sensors allows the maritime industry to make better-informed decisions more quickly, and in turn creating more efficient and responsive organizations. The technology progress has even enabled the development of fully electrically powered and autonomous ships for commercial operations.

Although there are some immediate benefits of using digital technology onboard, there are some important points to consider from a risk management perspective. Cyber threat is a major risk, because cyber incidents can corrupt data that needs to be processed for the ship to operate and can also paralyze a fleet management system. Also, the recovery from a cyber incident will most likely incur considerable costs and stretch the shipowner's business operations.

In future ships, the automation system will play the role of the crew, so the reliability of the onboard electronics is even more essential if it is to replace the crew's crucial role in the safety and maintenance of the ship and its cargo. The insurance market has some concerns about advances made in the use of digital applications and control systems in the operation of ships – particularly crew training and their ability to manage cutting edge technology with the corresponding large amounts of data. Evidence suggests that the frequency of collisions is increasing, possibly as a result of the introduction of new digital technology.

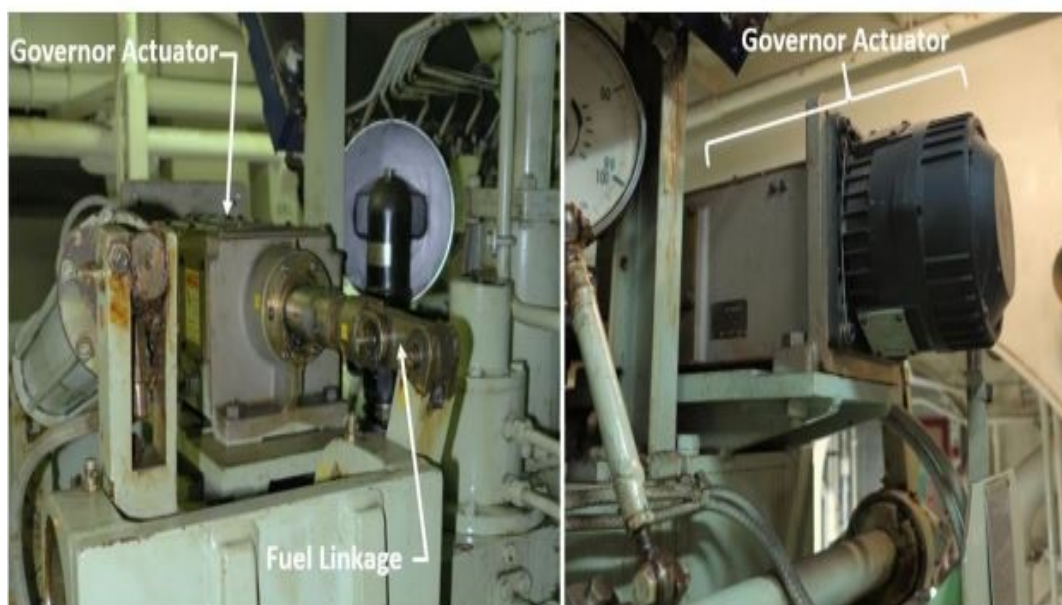
It is unknown how many incidents at sea are related to electronic failures. This may be because the casualties triggered by electronic failures are not significant or because of the difficulty in finding the root cause of the incident in terms of electronic failure. Electronic devices malfunctioning whilst the ship is underway have led to significant casualties, particularly when essential operational equipment have broken down while entering or leaving port.

Collision and fire due to a momentary abnormality



Shortly after midnight on 6 September 2016 in the Houston Ship Channel the tanker “Aframax River” experienced a sudden failure of its main engine that resulted in loss of control and led to the ship striking two mooring dolphins. A fuel tank was ruptured, causing fuel oil to leak into the river and the fuel quickly ignited. The ship was engulfed in flames and the fire quickly spread across the channel, threatening other ships and nearby waterfront facilities. It also enveloped the area in thick toxic smoke. There were only minor injuries, but there was also damage to the tanker and other ships. So, what happened?

The tanker departed the terminal in ballast condition, with two pilots aboard and two assisting tugs. A dead slow astern order was given on the bridge. Thereafter, an all stop order was given by the bridge, but the engine did not respond. A dead slow ahead order was then given, then half ahead, then full ahead – but the engine did not respond. The tugs tried to stop the astern movement, to no avail. The emergency stop button was engaged and responded, but not in time to avoid the ship collision and the following fuel tank rupture and fire. Why did the engine not respond to the orders given from the bridge?

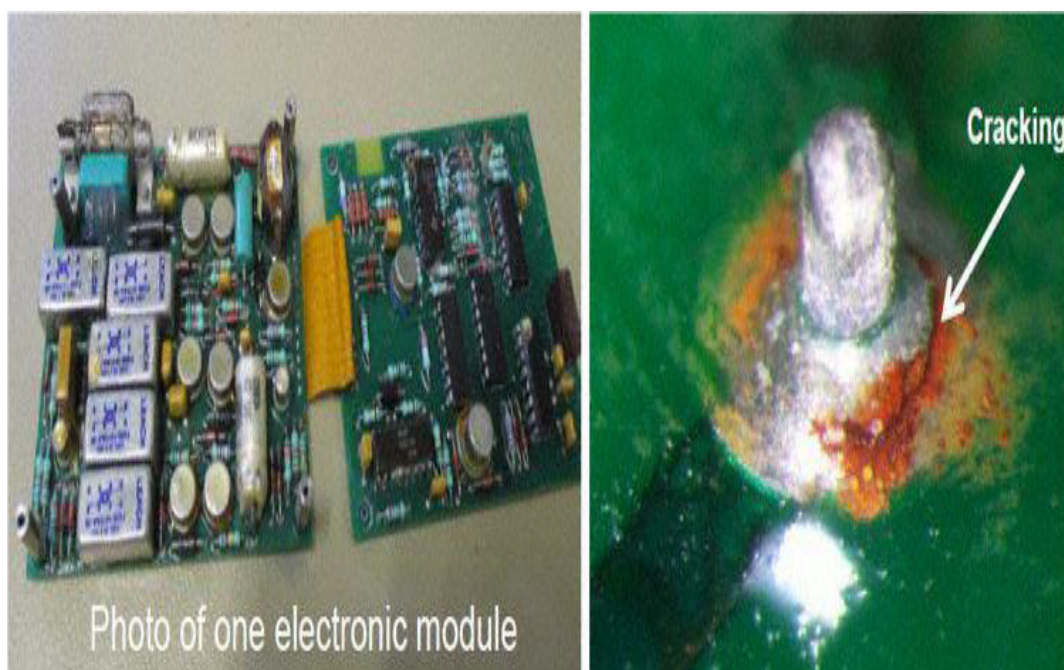


Front and back of the main engine governor actuator and mechanical fuel linkage.

The [US National Transportation Safety Board report](#) concluded that the probable cause of the ship’s collision with mooring dolphins and the subsequent fire in the waterway was a momentary abnormality of the main engine governor actuator system (electronic unit inside) in responding to command inputs from the bridge.

On 28 December 2014, AirAsia flight QZ8501, departed the Indonesian city of Surabaya for Singapore and its communication with air traffic control was cut off just 42 minutes after it took off. The aircraft was later found crashed into the Java sea, and all 162 passengers and crew onboard were killed in the crash.

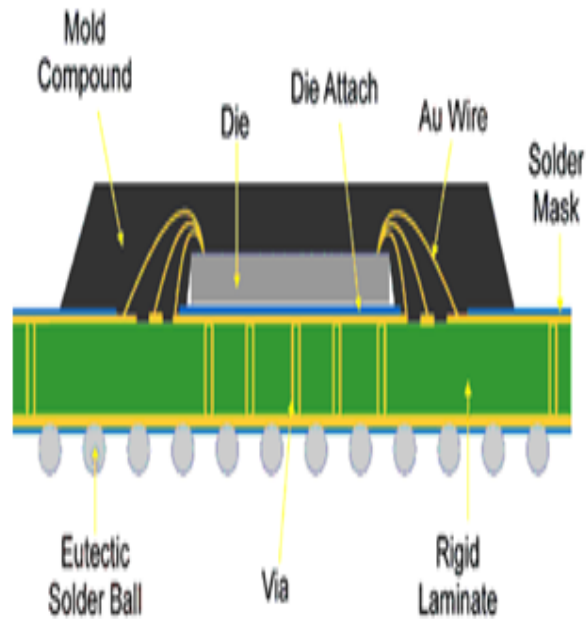
[The Indonesian National Transportation Safety Committee investigation report](#) showed cracked soldering on the electronic module called the Rudder Travel Limiter Unit (RTLU). The cracked solder resulted in the intermittent failure of the RTLU and four warning signals were given throughout the flight. When the pilot powered off the circuit breaker to reset the system to resolve the issue, the autopilot mode turned off and the plane crashed due to the inability to control the aircraft. The maintenance record showed that the RTLU had malfunctioned 23 times over the previous 12 months and investigators concluded that the plane crash was initiated by cracked soldering within the electronic module.



Electronic modules (left) and cracked solder joint (right)

Common causes of failures of electronic modules

There are many different types of failures in electronic modules. Below we list some examples:



Printed circuit board through solder by surface mount technology (left) and semiconductor plastic package (right)

Failure due to manufacturing, material or use

Electronic modules and printed circuit boards (PCB) are put together by interconnecting chips and other small electronic components into a circuit board. The effectiveness and reliability of these circuit boards are determined by the quality under which they are initially manufactured (printed).

The quality and reliability of solder joints are two of the more critical issues. The solder supplies electrical, thermal, and mechanical connections on the PCB. As semiconductors become smaller and denser in design, the PCB assembly is reduced in size and challenges the quality of the manufacturing. Some signs and symptoms of poorly manufactured electronic modules and PCBs include, connection issues, bad solder or premature failures, etc.

Electronic modules and PCBs may be affected by different environmental conditions such as temperature, humidity, dust, shock and vibration, which can all contribute to the aging and failure of the electronics.

Changes in temperature and expansion and contraction of the PCB may potentially risk a warped board with consequential damaged soldering joints and damaged internal bonding wires inside the semiconductors (“au wire”). It is also common for PCBs to overheat due to the high temperatures they are exposed to, especially if there is insufficient space around the component.

Electronic packages can also fail under dynamic loads such as shock or drop impacts and solder joints between chips and PCBs can become brittle and fail. The failure of these solder joints under thermal and dynamic loads can lead to an open circuit in electronics.

Lastly, the electronic packages can fail by material. The EU directive on the restriction in the use of hazardous substances in electrical and electronic equipment (RoHS Directive) restricts the use of lead, mercury, cadmium, chromium and brominated flame retardants in such electrical equipment. The transition into lead-free electronic packages impacted the industry. In 2006, a large batch of Swatch watches were recalled and the Microsoft Xbox360, a video game console device, suffered a high failure rate.

Failure by No Fault Found (NFF)

NFF is a common failure mode represented by symptoms such as intermittent failures. Failures do occur, but the device works again if rebooted. This instance is called NFF. The two case studies mentioned above can both be categorized as NFF combined with other types of failure. Broadly, NFF is found in applications such as automotive, avionics, computers, telecom, mobile phones, etc. NFF can be caused by a number of factors such as sneak circuits, printed circuit boards, connector issues, component-PCB interconnect failures, component failures, manufacturing issues, etc.

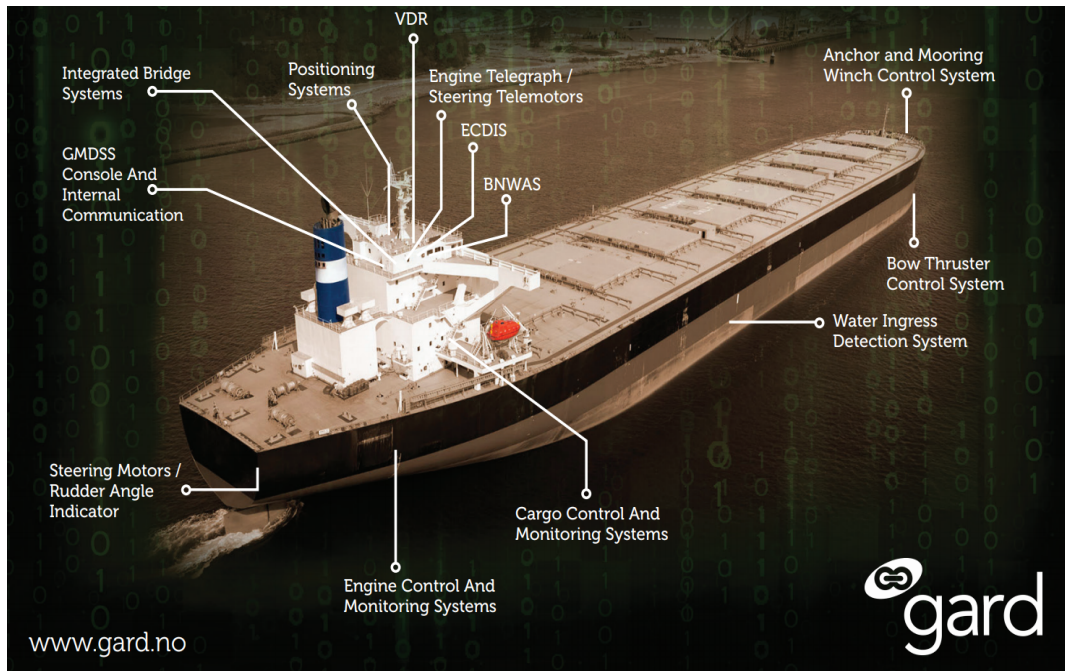
Failure by supply chain management

Changing consumer tastes are pushing products towards shorter life spans, lower costs, and faster time-to-market. Supply chain management has become an important facet of many companies' operation as it involves outsourcing parts of a global supply channel.

Effective supply chain management can be achieved not only by the purchasing team outsourcing parts, but by a strong lean organization of cross-functional teams where each team deliver different tasks such as: designing products, qualifying parts, testing products, finding the root cause of the failures from prototypes and the field, manufacturing products, reflecting market changes, auditing suppliers, outsourcing to reduce costs, handling logistics to meet lead-time, etc. The end goal of supply chain management is to meet customers' needs by bringing functional and reliable products to the market.

Manufacturing of electronic products is challenging as electronics use many outsourced parts and services such as contract manufacturers. Supply chain management, which includes processes to screen out poor quality parts and sufficient development time through prototyping and redesigning loops, is needed to ensure a fully functional and reliable product. Poor supply chain management, due to pressure from quick time-to-market, will lead to a loss of the reliability of such electronic products.

Recommendations



The operational technology onboard, such as navigation, communication, machinery and cargo systems, are today digitally connected to the bridge and engine control room and even digitally connected via satellite to onshore operation centers located far away from the ship.

It may be easy to assume that new digital equipment as reliable or to view their malfunctions as not serious. However, if digital or electrical equipment should fail, there may be no easy or quick fixes available and a variety of factors can prevent prompt repairs. For example, it may be too complex for the ship's crew to repair, or an authorized technician is far away and too expensive, or the crew can repair it, because if they do, it may void the manufacturer's warranty.

Experience has shown that operational technology and its electric and digital components onboard ships are not permanently reliable and can fail when exposed to harsh conditions, fatigue, or latent defects caused by poor design or manufacturing. Finding the root-cause of the failure of electronics is not always straightforward. The reliability and defects present in electronics also impact the maritime legal system as we try to find answers to the legal implication of a 'glitch'.

Gard is of the view that it may be beneficial if the maritime industry put more efforts into reporting and finding the root-causes behind cyber, software, and electronic incidents and failures. Doing so would enable the industry to learn how to avoid errors in the future.

As a major insurer, we are interested in finding answers to:

- When did the glitch happen? Before the ship broke ground, or after?
- The origins of the flaw? Negligence? Unseaworthiness?
- Products Liability: Manufacturing or design defect? Could the enhancement of internal diagnostic features in systems/devices help avoid 'glitches', or detect them and alert the ship operator, before an accident occurs due to the 'glitch'?
- Does this 'probable cause' have impacts on Limitation of Liability? Fire Defense? Other legal and contractual liabilities?
- Is the concept of 'glitch' going to be our future explanation for such technical failures? Will there always exist a sub-set of technical failures that will defy an objective, precise causal explanation?

Gard would like to thank our correspondent in South Korea, Dr. Dong Hyun Kim, CEO of KOMOS for his valuable insight and contribution to this article.

Dr. Kim has over 10 publications on the reliability of electronics and a PhD degree from the study of electronics reliability within the mechanical engineering department of the University of Texas at Austin. Prior to joining KOMOS, he worked for Cisco Systems in Silicon Valley for seven years, as a manufacturing engineer and supply chain manager.

The information provided in this article is intended for general information only. While every effort has been made to ensure the accuracy of the information at the time of publication, no warranty or representation is made regarding its completeness or timeliness. The content in this article does not constitute professional advice, and any reliance on such information is strictly at your own risk. Gard AS, including its affiliated companies, agents and employees, shall not be held liable for any loss, expense, or damage of any kind whatsoever arising from reliance on the information provided, irrespective of whether it is sourced from Gard AS, its shareholders, correspondents, or other contributors.