Emre AY

040100675

FAIL-SAFE

ABSTRACT: This is a century that almost anything relies on complex systems. From a fire alarm system to a nuclear plant, every system has a possibility to failure. Reducing this chance is a vital step, but not enough in the systems that can endanger human life. This is the point where a plan steps in, in case of a failure.

KEY WORDS: Redundancy, fail-deadly, fail-secure, control system, relay, complacency, jolt, free-return trajectory, propulsion, scaremonger

Every system can fail. From the most harmless ones to the critical ones, this is a prudent approach. As many systems have crucial *–and also not so crucial–* roles in humans' lives, stability and safety of the systems takes most of the time in the design process.

A fail-safe system is a system that in case of failure, it responds as safely as possible – i.e. no harm or minimum harm. Fail-safe systems designed that a failure would result in to default its safest possible state [1]. The word 'fail-safe' has its first known use back in 1945-1950 [2].

Fail-safe concept usually gets confused with fail-proof. Fail-safe does not mean that the system won't fail. It means it can fail securely. Any predictable failure must result in a safe situation [3]. Also fail-safe and fail-secure are not the same concepts. A fail-secure system is defined as a system that is secured in case of a failure, an ingress-egress system is an example.

A lot of dangerous devices, machines and systems exists, and the world is full of them: nuclear plants, fast trains, huge electrical transformers and turbines, power lines. Each of them has to be stable and safe. Most of these systems have a control system which controls their behavior in a desired way. But control systems can fail, so they must be designed and built as fail-safe systems.

To explain fail-safe concept better and how it works, an example would be clear enough. Think about a fire alarm system [4]. In a building, there are several alarm switches which triggers the alarm. Think these normally open switches as parallel connected with each other and in series with the alarm siren. (*Figure 1*)

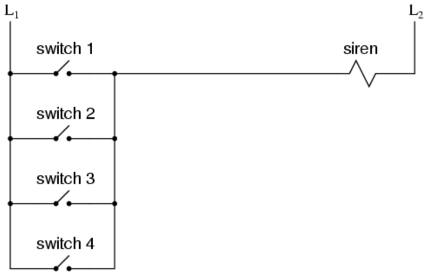

Figure 2 [4]

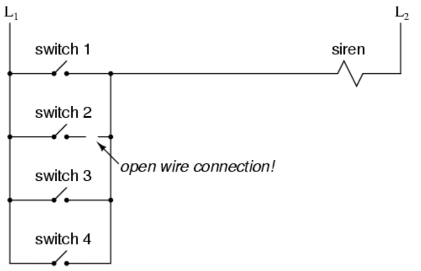

Figure 1 [4]

The logic is quite simple; once an alarm switch is pushed, the circuit will be connected and the alarm will be triggered. But, in electrical circuits the most common failures are ‘open’ failures, which mean there is a connection problem somewhere in the circuit that it’s an open circuit, there is no electrical conduction. It can be caused by a physical damage, over heat, blown fuses etc. What we wanted to do is, design the system that can reduce the harm in case of failure. Broken wire (*Figure 2*) failure results in disability to alarm the siren in case of fire, so this system is not fail-safe. The desired system is a working system in failure. If we change our design as in *Figure 3,* and add a control relay to the system, when all switches are unactuated, the relay is energized and it keeps the contact of the siren open. If one of the switches is pushed or there happened an open connection *–a fail–* the relay would be no longer energized and its contact will be closed. This will trigger the alarm siren.

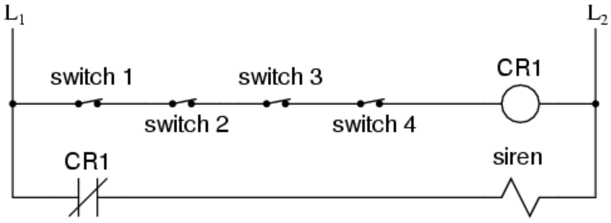

Figure 3 [4]

In this example, the state in case of failure is changed between two designs. In first design, the failure caused the alarm not to be triggered in time of need which can possibly harm a lot of people and/or objects. However, the failure cause only a false alarm in the second design, which is a way more harmless to be compared with the first one. The system can still be fail if the connection between the contact and siren is broken, but it’s safer than the first one.

To design a fail-safe system there are two important criterion. First, to find the most likely failures and second to find the safest mode. The cooler system of a machine for example, has electrical valves which controls the flow rate of cooling water –on an off- . The most likely failure would be the breakdown of the valve. The safest mode is to turning on the cooling water. So the design would be based on this default mode, a spring will return the valve to its default position when the valve is de-energized.

The systems which have critical roles on human life results in to design and built fail-safe systems. As the technology is developed, more crucial needs such as electricity, energy, transportation, agriculture, communication etc. have become depended on the technology and thus, these complex systems became more vital to be controlled.

In modern technology, it is absolutely vital to design systems as fail-safe. In 1962, The Bay Area Rapid Transit system (BART) project was begun which was to serve a rapid transit system in San Francisco Bay Area. In this project, an innovative method ATC (Automatic Train Control) system was to use [5]. ATC is a system that relies on onboard sensors that determines the position of the train and the location of the other trains. The speed was automatically maintained by the position information that the sensors provide. The problem of this system was, there were no fail-safe methods, all control was based on redundancy [6]. Three BART engineers found this problem but their attention to tell the managers was eventually resulted in to lose their jobs. This is a very frequent problem in many companies and projects when some contrary ideas have heard. Usually the bosses or team leaders don't want to hear the contradictory thoughts and they just ignore and act them as scaremongers. This complacency usually costs time, money and/or human life.

On October 2, 1972 a BART train overshot the station and five people have injured. This was an avoidable accident and it was predicted and warned. If the case was about a nuclear reactor or a weapon, this complacency would be caused a disaster.

In December 3, 1999 NASA's robotic spacecraft Mars Polar Lander crashed on Mars. The reason was the sensors in the gear sensed the jolts while landing and the software mistake caused the spacecraft to misinterpret that it has landed and it turned off the engines.[7] The software actually, was designed to ignore these signals that caused from the jolt while landing. [8] But the error was not realized in the tests before launch because the sensors on the tests were wired incorrectly. As a result of this failure, the engines stopped working at an altitude of 40 meters and crashed into the Mars surface.

Apollo 13, on the other hand, has good and bad examples of failsafe. In April 13, 1970 Apollo 13 had an Oxygen Tank incident. The liquid oxygen tank was damaged in the factory and also the thermostat was rated less voltage [7]. This damage emptied oxygen tanks and this resulted in a big problem. But the returning back of the crew was also a failsafe system. They have used a free-return trajectory which is the trajectory that in absence of propulsion the spacecraft would return to Earth. Within hours after the accident, Apollo 13 used the lunar module to maneuver from its planned lunar orbit insertion trajectory to a free-return trajectory [9] and became the only Apollo mission that really used the free-return trajectory to turn around Moon.

Today, many precautions for failure considered in systems while they're designed. Without the fail-safe concept, it would not be possible to have stable, sustainable and reliable systems and thus their outputs. But even the fail-safe system of a fail-safe system can be fail, so a system can't be 100% fail-safe. But the failure can be under control.

REFERENCES:

[1] http://tvtropes.org/pmwiki/pmwiki.php/Main/FailsafeFailure

[2] http://dictionary.reference.com/browse/fail-safe

[3] http://www.steamesteem.com/?control-fail-safe

[4] http://www.allaboutcircuits.com/vol_4/chpt_6/5.html

[5] http://eng-web.engineering.cornell.edu/EngrWords/cases/BART_case.cfm

[6] Friedlander, Gordon D. 1974. The case of the three engineers vs. BART. *IEEE Spectrum* October: 69-76.

[7] Chiles, R. James. *Inviting Disaster ,* first edition.

[8] http://www.spaceref.com/news/viewnews.html?id=105

[9] Stephen Cass, "Apollo 13, We Have a Solution," *IEEE Spectrum,* APRIL 2005