Lectio Precursoria

Alessandro Mancuso

September 18, 2020

Dr. Custos, Dr. Opponent, ladies and gentlemen.

Everyday, we are surrounded by safety-critical systems, starting from your coffee maker in the morning to the public (or non-public) transportation you take to go to work. If you work in a factory, you are probably working closely to heavy machinery. If you work in offices, you strongly rely on safety-critical systems that provide you with a reliable source of heating and electricity.

Let's take for example a metro line. Nowadays, I see more and more metro stations with safety panels to avoid people to fall onto the railway; that is only one (and one of the more evident) safety measures to protect the passengers, but many other safety measures are installed on the metro to ensure a safe and reliable ride for all of us. A metro line is composed of thousands of components that are interconnected together to make sure that the metro takes you to the right stop at the right time. If such components are not working correctly, the metro will stop (hopefully at the right station, but often that's not the case). Not only that, if the components are not working correctly together, the metro will stop, you will miss that important meeting at work or a special date. In some cases, the failure of a component may not cause an immediate stop of the metro line, but could generate a cascading sequence of failures throughout time which will finally cause the failure of the metro. All these failure scenarios can be modelled through a common framework, which allows the risk analysis of the safety-critical system.

Still considering the metro line as an example, let's think about the possible outcomes from metro failure scenarios: (1) the metro stops irreversibly, (2) the metro stops with injuries, (3) the metro reaches its destinations late due to temporary stops and (4) the metro reaches its destinations on time with no accidents. Of course, we do hope that the latest outcome is the most likely, but how to define how likely a scenario is? Luckily, mathematics comes handy here by setting the most likely scenarios with higher probabilities. Not only that, mathematics helps us to quantify the impact of such scenarios (meaning economical, safety and environmental consequences). The product of probabilities and impacts is the risk!

To reduce the probability of negative scenarios, we can deploy different mitigation actions: inspections, maintenance activities, replacement of components, personnel training, and so on. To reduce the impact of negative scenarios, we can deploy other mitigation actions, for instance insurance contracts for economical consequences. So what is the best possible strategy to minimize such risks? Well, this thesis is all about that!

First we list all possible accident scenarios, then we quantify how likely and how severe each scenario is, finally we optimize the selection of actions to minimize the failure risks. The best strategy can be a combination of maintenance activities, frequent inspections and insurance contracts.

Nowadays, we live in a connected world where all components can be constantly monitored in order to detect failures before they actually happen, by

(i) activating monitoring devices to check the condition of the components, (ii) tracking down possible upcoming failures and (iii) act on time to avoid system failure. This way, maintenance activities can be planned in due time such that the predicted failure does not happen. Connectivity enables us to be more proactive in maintenance, instead of reactive. This has proven to be very effective in anticipating system failures and avoid the consequences of such failures. For instance, the 24/7 Connected Services by KONE strongly relies on the monitoring information of the elevator to schedule maintenance activities on each equipment. However, this novel advances lead us to new interesting challenges for the future society, beside leading us to safer and more reliable systems. These challenges include: how reliable are the monitoring devices? Are they actually secure from malicious and non-malicious threats? This Dissertation tries to answer also these questions.

To clarify the challenges we face in our society, I want to share with you a piece of ancient Greek mythology. In ancient Greece, sailors would occasionally brave a sail through the Strait of Messina, that separates Sicily from the Italian mainland. According to the myth, on one side was Scylla, a terrifying sea monster that caught any ship that sailed too close. However, attempting to steer clear from Scylla would take the ship close to an equally dangerous hazard on the other side of the strait, a deadly whirlpool called Charybdis. In the same way, the more we empower our systems with connected services for monitoring and controlling, the more we make our systems safe and reliable (sailing away from Scylla). But at the same time, the more we are leading the way to cybersecurity issues (sailing closer to Charybdis), therefore we need to consider new possible hazards, both accidental and malicious.

To conclude, safety is not defined by the absence of accidents (the concept of “zero accidents” in a working environment is a utopia, still it must be the main vision in safety management), but by the capacity to cope with possible accidents.

I ask you professor Lesley Walls, as the opponent appointed by Aalto University School of Science and Politecnico di Milano, to make any observations on the thesis which you consider appropriate.

[redacted]

I kindly thank you, professor Walls, for your observations on my doctoral thesis. Ladies and gentlemen, if you have observations you would like to make on my dissertation, please ask the custos for the floor.