University of Glasgow

Safety Critical Systems 4

Safety Analysis Tool for a Formula 1 Race

Author:
Garry Sharp
0801585s

Course Co-Ordinator:
Dr. Chris Johnson

19th of November 2012

Abstract

Formula 1 has always been a sport in which tragedy has had the misfortune to echo throughout its history. The often fervent debate surrounding the sport's safety has lead to much increased safety standards within the past 30 years as there has not been a death in the sport for many years now (although there have been recent deaths in similar sports MotoGP and Indy 500). However, the sport transitioning into a new era has brought about new threats and concerns to both drivers and members of the public. A good example of this could be the terrorist threats this year in advance of the Bahrain GP.

After the infamous death of Aryton Senna in Imola on the 1st of May 1994 (and Roland Ratzenberger in qualifying the day before), many pioneered for increased standards within the sport. Although the actual rate of innovation in safety after this did not increase at all. Innovations continued to be made before the deaths of Senna and Ratzenberger (such as mandatory fire proof clothing for all pit crew and the introduction of a safety car after crashes). The generally acc

This tool aims to objectively quantify the risks involved at any specific race by accepting an array of conditions as an input and then contrasting the likelihood of these conditions to occur and cause an accident with that of the presumed and generally accepted effectiveness of the measures designed to counteract them. The focal point of safety will be on that of the drivers, although, there will invariably be some cross over with other people included in a formula 1 event, this will be especially highlighted when this impacts on the driver in some way.

Contents

1 Introduction to Safety in Formula 1

We will examine what has happened in previous Formula 1 events, the consequences of some of these events as well as continuing innovations in safety in the sport. The governing body of Formula 1 is the FIA (Federation Internationale de l'Automobile), who are a very well known name in Formula 1 and all motorsport throughout the world. The responsibility of the safety of the drivers and other members of the Formula 1 team is their responsibility. Nowadays, and all of their regulations for the current season can be found on their website **FIA reference**. Example citation [Figueredo and Wolf, 2009].

1.1 Summary of Previous Diasters

Formula 1 has had the misfortune of being littered with disastrous past events, a look at a list of fatalities illustrates how fierce the sport can be (see appendix A). It should be noted that in modern Formula 1 events, safety is something that is taken very seriously. The FIA have an ever expanding list of regulations to ensure that the safety of their events is the best it can be.

1.2 Preventative Measures Taken

1.2.1 In General

1.2.2 For the 2012 Season

Figure 1: Example image.

2 Safety Analysis

Any seasoned formula 1 fan will tell you that no two races are ever the same, this of course is true for many sporting event, however, where formula 1 (and motorsport in general) differ is that each driver is in command of a machine that can cause immense damage to other drivers.

2.1 Tool Description

I've elected to use the FMECA technique in the development of the tool, the tool will examine a series of failure modes and after entering certain values, output to a risk matrix the Risk Probability Number. The values required to calculate the RPN (The severity, occurrence and detection rates) will be acquired by calculating user input. There will also be a slight amount of cross over between failure modes (for instance if one of the Electronica Control Units or ECUs breaks in a formula 1 car, then the chances of being forewarned of catastrophic engine failure is drastically reduced), for this reason an overall rating will be given which better reflects the probability of an overall accident. The tool also features an ability to view all of the FIA regulations relating to a microcosm of Formula 1 safety, such a pit lane regulations.

2.2 Block Diagrams

Block diagrams are a very good tool for determining the weak aspects of a system that may be instrumatal in realising a failure mode. However, for the tool that I developed I decided to omit the diagrams as I felt that the tool is too general to make any substantial gains from the inclusion of the diagrams. In my evaluation section, I discuss the concept of further development of the system to include more failure modes and better numerical analysis in determining the RPN. Should the failure modes be further developed. In this scenario when trying to identify ALL of the safety concerns and failure modes, the usage of block diagrams would aid greatly, however, as I am merely trying to encapsulate a broader spectrum of the main failure modes, the usage of block diagrams seems inapproapriate.

2.3 Failure modes

Please refer to the appendices to see a full list of Failure Modes and Effects that have been incorporated into the tool.

2.4 Unpredictable Events & Human Factors

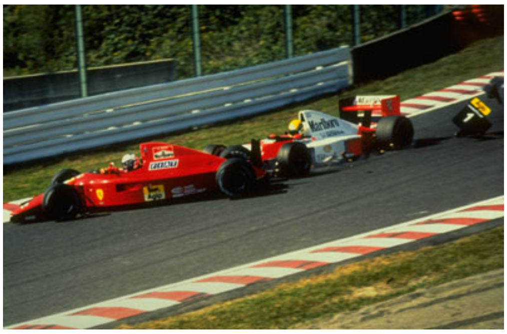


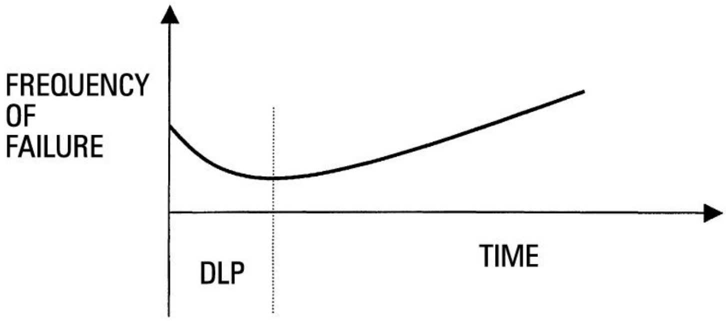
Figure 2: Aryton Senna deliberately runs Alain Prost off the track at Suzuka in the 1990 Japan Grand Prix

It is not always the case in Formula 1 events that the drivers necessarily reflect the risks involved in their racing style. Even after performing a thorough FMECA risk assessment, should a driver or a member of the public exercise a pre-mediated stunt (or simply do something entirely stupid) then there are only certain provisions that can be put in place to handle the resulting events. Figure 2 famously shows Aryton Senna crashing into Alain Prost after feeling cheated that he did not start on the correct side of the track. Although neither driver was injured and safety provisions had been put in place, other than the FIA changing the grid block positions, their is not a lot that they could have done to have prevented the crash. This level of recklessness is not uncommon in formula 1. Indeed a false start by Romain Grojean at Spa this season created a similar crash where he instantly caused three cars (including his own) to be retired straight away. The FIA punished him accordingly and he received a race ban.

2.5 Further Information

2.5.1 Team Responsibility

In addition to the regulations that the FIA produce, each of the teams is expected to perform their own safety analysis and fully test their cars before driving, this, however, does not always mean that the vehicle is safe. For instance, this season Lewis Hamilton's McLaren MP4-27 broke unexpectedly 3 times causing him to retire from the races. It is, therefore, very important to understand that despite extensive testing from teams, that there is still (an albeit reduced) risk of unexpected failure.



Bathtub model showing hardware life cycle as a function of time

3 Evaluation

Due to the scale and nature of Formula 1 events, it would be extremely difficult to do any practical testing of the system. That does not, however, not mean that general testing regarding the method and techniques cannot be performed. A reasonable way of going about the evaluation of the system would be to compare and contrast it to existing systems, and by careful examination of results, make a conclusion based on the accuracy of the system. It should be noted that initial sanity testing against a similar system resulted in a significant change of code, meaning that the version submitted is actually version 3 (with two major re-writes prior to this version), this means that some of the points made in this system have already been changed and will not be visible for

3.0.2 The bathtub failure model

There are restrictions placed on the number of cars, engines and gearboxes that each driver may use, this can have an impact on the stability of the car. Each team is allowed no more than two cars at a time and should a new car be used between qualifying and the race, the driver of that car will start the race from the pit lane.

Each driver is allowed at most eight engines per season and one gearbox per five races. The bathtub failure model (also known as the bathtub curve) is a model that explains the failure rate of hardware as a function of time illustrating that there is a high failure rate at the start of usage (known as the break in phase) and also towards the end of its life (known as the wear out phase). The tool that has been developed does not account for the changes in gearboxes or engines during the season due to time constraints.

3.0.3 Significant Changes to the System

After the initial implementation (along with basic sanity testing and comparison to a peer's model) it became apparent that a few things needed to be drastically changed, some of these changes can be documented below

Previous Item	Revision
Interface & Interactivity	My initial system had been entirely paper based, it basically operated in a traditional paper based FMECA manner (a simple worksheet). I very quickly realised that making the system more interactive would allow for better, more personalised feedback to be given. I therefore started on a simple HTML mockup of the worksheet. This later changed again to be reflected in a risk matrix.
Criticality Analysis	The initial system also did not feature any criticality analysis (this was mostly so that I could see what a more basic mock up of the system would look like before adding functionality), the addition of the criticality analysis feature was not something that I considered would pose that much more of a problem given the scope that I was working in, this was the major inspiration behind the development of the risk matrix.

3.0.4 Effectiveness of the Tool

The tool in general seems to function as desired (basic black box testing showed that it output the correct values when given an input certain input set). What still remains unclear is how well the system would function should it be employed in the safety critical analysis of a Formula 1 event. As this system focusses on the broader idea of Formula 1 driver safety and not a particular aspect of it, it has been very difficult to go into detail that, in a real race, would be sufficient enough to perform a serious and accurate test. The current list of FIA regulations spans many pages, with each racing team adhering to these instructions as well as taking their own safety precautions. Although my tool addresses a subset of each of the safety aspects of a formula 1 race (spectator positioning, pit lane procedures, racing maneuvers etc), it does not go as deep as to asses the criticality of each FIA regulation, and as such, cannot possibly claim to be more substantial than the already existing system. That said, in terms of providing a summary (which could be used when presenting a general and overall danger at an event) I would claim that my tool is quite effective. I think its greatest strength is when used in conjunction with another tool or the general regulatory FIA risk assessment, but not as the primary tool in safety analysis.

Another factor to consider is that lots of the numbers used to generate the RPNs are constructed using intuition and research where available. For instance, it would be very logical to presume that the detectability of a brake failure would be more likely should the brakes be checked before the race. However, as a system which attempts to output quantitative data, it is very difficult to say indefinitely that this increases the detectability by a factor of x. As a fan of Formula 1 I have used values (where applicable) that I believe to be close to what the actual values would be. This means that any RPN that is output to the risk matrix is not entirely accurate, rather, an approximation of the likelihood of an event against its detectability.

4 Findings & Conclusions

4.1 Further Development

In my opinion, there are two ways in which the system can be made to be more accurate. Firstly, the inclusion of more failure modes would allow for more in-depth analysis and would almost certainly highlight new safety concerns. Secondly the addition of real statistical data in the RPN engine would make the values calculated much more accurate. Due to time constraints, mining this data proved insurmountable to the functioning of the system, so intuitive values were used.

4.2 Conclusive Summary

Overall, testers found that the system does a good job of illustrating the safety concerns of a Formula 1 race along with providing insight as to how performing certain actions or adding certain failsafe measures, can mitigate the risks. In this regard they system is a complete success (see above for how it could be further improved). However, I do not feel that by today's strict Formula 1 standards, that my tool would aid organisers of an event. Whilst researching safety and safety history in Formula 1. I very quickly learned what a large field it is

References

[Figueredo and Wolf, 2009] Figueredo, A. J. and Wolf, P. S. A. (2009). Assortative pairing and life history strategy - a cross-cultural study. *Human Nature*, 20:317–330.

A Formula 1 Deaths

Name	Date of Death
Cameron Earl (UK)	June 18, 1952
Chet Miller (USA)	May 15, 1953
Charles de Tornaco (BEL)	September 18, 1953
Onofre Marimn (ARG)	July 31, 1954
Mario Alborghetti (ITA)	April 11, 1955
Manny Ayulo (USA)	May 16, 1955
Bill Vukovich (USA)	May 30, 1955
Eugenio Castellotti (ITA)	March 14, 1957
Keith Andrews (USA)	May 15, 1957
Pat O'Connor (USA)	May 30, 1958
Luigi Musso (ITA)	July 6, 1958
Peter Collins (UK)	August 3, 1958
Stuart Lewis-Evans (UK)	September 19, 1958
Jerry Unser, Jr. (USA)	May 17, 1959
Bob Cortner (USA)	May 19, 1959
Harry Schell (USA)	May 13, 1960
Chris Bristow (UK)	June 19, 1960
Alan Stacey (UK)	June 19, 1960
Shane Summers (UK)	June 1, 1961
Giulio Cabianca (ITA)	June 15, 1961
Wolfgang von Trips (GER)	September 10, 1961
Ricardo Rodrguez (MEX)	November 1, 1962
Gary Hocking (Rhodesia and Nyasaland)	December 21, 1962
Carel Godin de Beaufort (NED)	August 2, 1964
John Taylor (UK)[C]	August 7, 1966
Lorenzo Bandini (ITA)[D]	May 7, 1967
Bob Anderson (UK)	August 14, 1967
Jo Schlesser (FRA)	July 7, 1968
Gerhard Mitter (GER)	August 2, 1969
Martin Brain (UK)	May 25, 1970

Piers Courage (UK)	June 7, 1970
Jochen Rindt (AUT)	September 5, 1970
Jo Siffert (SUI)	October 24, 1971
Roger Williamson (UK)	July 29, 1973
Franois Cevert (FRA)	October 6, 1973
Peter Revson (USA)	March 30, 1974
Helmuth Koinigg (AUT)	October 6, 1974
Mark Donohue (USA)	August 19, 1975
Tom Pryce (UK)[E]	March 5, 1977
Brian McGuire (AUS)	August 29, 1977
Ronnie Peterson (SWE)[F]	September 10, 1978
Patrick Depailler (FRA)	August 1, 1980
Gilles Villeneuve (CAN)	May 8, 1982
Riccardo Paletti (ITA)	June 13, 1982
Elio de Angelis (ITA)	May 15, 1986
Roland Ratzenberger (AUT)	April 30, 1994
Ayrton Senna (BRA)	May 1, 1994
John Dawson-Damer (UK)	June 24, 2000
Fritz Glatz (AUT)	July 14, 2002