ISO26262 and a generalization of the FTTI concept

Jesper Adolfsson | Follow
Safety Manager and Systems De...

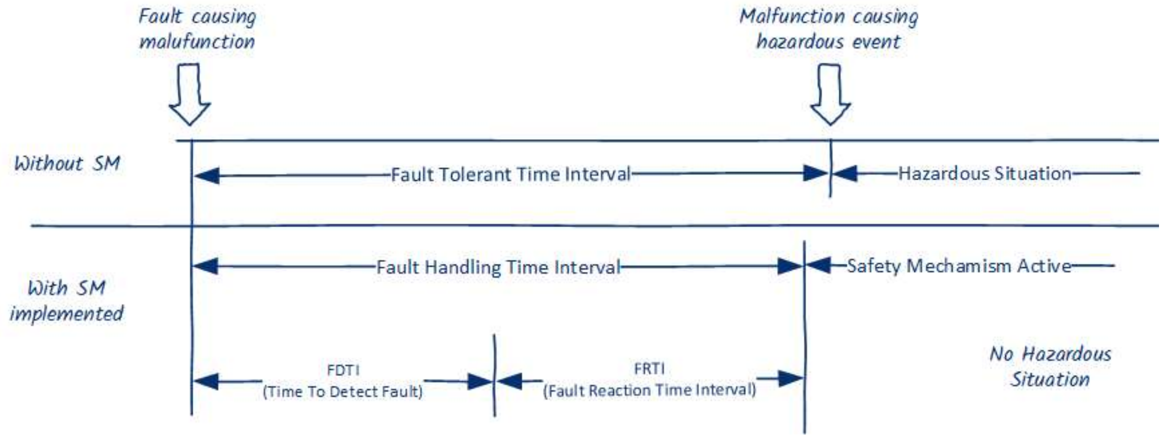
44 2 0

Introduction

According to ISO26262 Part 1 the FTTI (Fault Tolerant Time Interval) is defined as the "minimum time-span from the occurrence of a fault in an item to a possible occurrence of a hazardous event, if the safety mechanisms are not activated". However in real life applications it is not always a minimum time-span that quantifies if a fault in an item leads to a possible occurence of a hazardous event. More specific it might be different time-spans that leads to a possible occurence of a hazardous event depending on the operating point of the vehicle. Therefore we at Inmotion Technologies has generalized the FTTI concept into something we call FTQI (Fault Tolerant **Quantity** Interval) which we define as "minimum **quantity-span** from the occurrence of a fault in an item to a possible occurrence of a hazardous event, if the safety mechanisms are not activated". In this definition the quantity can be anything that is relevant to the hazardous event such as a change in speed or a change in distance. However this introduces some definition problems when translating the different parts that the FTTI consists of. This article will try to provide one possible solution that resolves this problem. It is assumed that the reader has some familiarity with ISO26262 and the definitions of the various fault timings.

Details

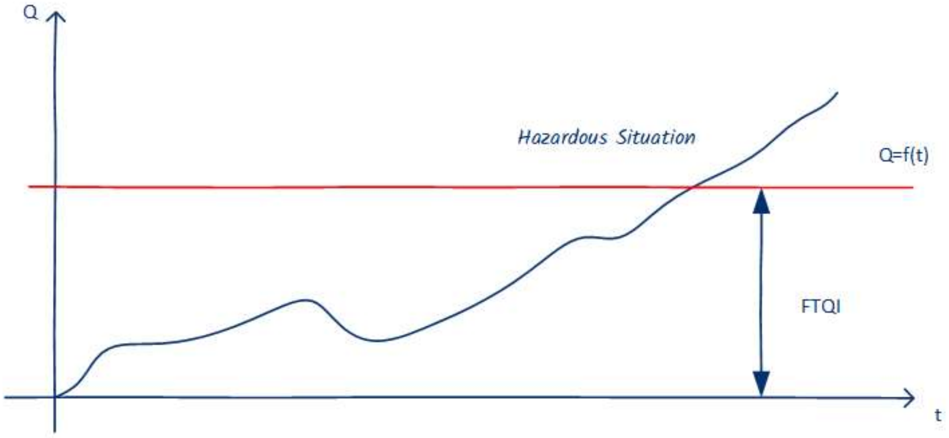
In the figure below it can be seen that to prevent a fault to turn into a hazardous situation the fault needs to be handled within the FHTI (Fault Handling Time Interval) which is less than the FTTI. The FHTI consists of two parts, the FDTI (Fault Detection Time Interval) and the FRTI (Fault Reaction Time Interval) where FDTI+FRTI=FHTI which shall be less than the FTTI.


Fault causing malufunction
Malfunction causing hazardous event
Without SM
Fault Tolerant Time Interval
Hazardous Situation
With SM implemented
Fault Handling Time Interval
Safety Mechamism Active
FDTI (Time To Detect Fault)
FRTI (Fault Reaction Time Interval)
No Hazardous Situation

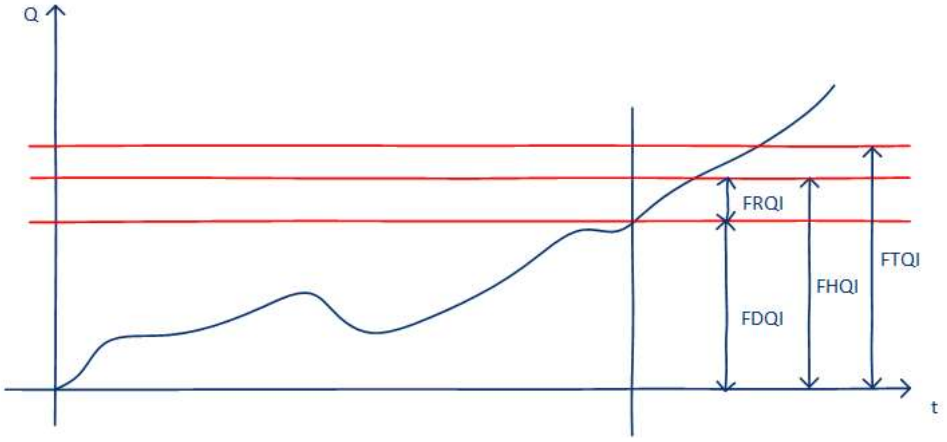
We will now replace the Time with the new Quantity by replacing the FHTI with FTQI, FDTI with FDQI and FRTI with FRQI. It could now be good to get a more intuitive feeling for what the Quantity could be in a real application. For example if we have a vehicle that is driven by an engine we might have concluded in our Hazard Analysis that unwanted acceleration is to be avoided and we have turned that into a Safety Goal. However, an unwanted acceleration typically needs time to develop into something hazardous so actually what we want to prevent is unwanted speed change. Imagine that the vehicle is at a pedestrian crossing and the engine system all by itself starts producing torque that accelerates the vehicle without driver input. This could potentially result in hitting a pedestrian with injuries as a result. Here vehicle, error torque, time interval etc... We could of course define a variable Time interval but that is not so intuitive so let us as an example make the Quantity equal to the time integral of an assumed ErrorTorque divided by the minimum inertia of the vehicle according to the formula below (don't bother too much about the units in the formula below because it should be viewed conceptually).

$$Q = \int \frac{ErrorTorque}{MinVehicleInertia}dt$$

In reality the integral above will actually have to be implemented more algorithmically and I haven't really defined what the ErrorTorque is here but as a concept I think it suffices. This quantity now reflects a speed change of the vehicle (assuming no slip of the wheels). Then if we look at this Quantity as a function of time it might behave according to the figure below.



The hazardous situation is then that an unwanted acceleration has resulted in a speed change that the driver can't control and we potentially hit a pedestrian.
Now we need to look at the parts that make up the FHQI=FDQI+FRQI (remember FHQI is the quantity that needs to be less than FTQI).



It is fairly easy to realize how to calculate and monitor Q(t) in relation to FDQI by just checking that Q(t) doesn't get larger than FDQI but what about FRQI which is related to reaction time to activate Safe State. From a system point of view we would like to express that in time since FRTI usually relates to the reaction time of HW/SW and actuation of Safe State. But if we do that we will mix two quantities, namely FDQI with arbitrary unit multiplied by time and FRTI with time as unit. The idea here is that we then go back to our system and look at the maximum possible value of the time derivative of Q. In our example above it is fairly easy to realize what Qdot_max is, the maximum torque produced by the engine divided by the minimum inertia of the vehicle. Thus we now have a conversion factor between time and Q. This is illustrated in figure below
No alt text provided for this image
Hence the FRTI is equal to dt in the figure above.

Example calculation

LowestVehicleInertia is 100kg·m2 *(as seen by the engine, we can combine linear inertia with rotational inertia if we know wheel speed relation to vehicle speed and gear ratios)*

Qdot_max = 1000Nm/ 100kg m2 = 10rad/s2 (the engine data we got from the inverter/motor manufacturer)
Assume FTQI = 8rad/s and in this example the FDQI is set to 6rad/s (this is deduced from our hazard analysis and the safety goals)
Then we get that FRTI < (8-6)/10 = 0.2s

End Note

The above is a result of the product development at Inmotion Technologies of an ASIL C classified Inverter for commercial vehicles. If you have any questions please let me know. For more information about our product range of inverters please visit the Inmotion Technologies home page.

About the author

Jesper Adolfsson currently works as a Safety Manager at Inmotion Technologies AB and holds a PhD in Mechanical Engineering from KTH.

Published By

Jesper Adolfsson

Jesper Adolfsson
Safety Manager and Systems Devel...

Follow

I wrote an article on how to generalize the FTTI/FHTI (Fault Tolerant/Handling Time Interval) concept described in ISO26262. I believe this generalization make it more useful for some real-world applications. Feedback is welcome.

2 comments

Sign in to leave your comment

Anders Agnvall

Anders Agnvall
System Engineer på Evidente AB
2y

Interesting ideas, Jesper! This should be useful in any application where the hazard is related to the accumulated error. I think the way you derive FRTI can be generelized to derive something lika a "minimum FHTI", meaning the fastest time that the system can detect and react to a fault i.e. corresponding to the error torque being equal to the maximum available torque in your example. This could be useful for dimensioning FHTI at system level.

Like Reply

Jan Björkenfjäll

Jan Björkenfjäll
General Manager Projects at Prison Island AB
2y

Bra. Jag ska be någon mer detaljkunnig i vårt (Combitechs) safetynätverk titta på denna.

Like Reply | 1 Like

More from Jesper Adolfsson 1 article