Insights and best practice

EMC COMPLIANCE KNOW-HOW

TECHNICAL NOTE 0113

REDUNDANT AUTOMOTIVE SAFETY SYSTEMS

ELECTRICAL DISTURBANCE TESTING

The challenge

With the addition of redundancy in safety functions, Test Engineers are faced with a new variable in testing.

This technical paper discusses best practices, originally from the aerospace industry, and how they can be applied to modern redundant safety functions in the automotive industry in theory and in practice. The document covers multiple types of testing, with the main focus on dropouts and voltage variations, and solutions for parallel operation.

The document is designed to accompany a video recording of a **live webinar presented by Tim Horacek**

You can view the **recording here**

Author:
Tim Horacek
Automotive Product Manager
AMETEK CTS

AMETEK CTS GmbH Sternenhofstrasse 15 4153 Reinach, Switzerland info.cts@ametek.com

AMETEK®
COMPLIANCE TEST SOLUTIONS

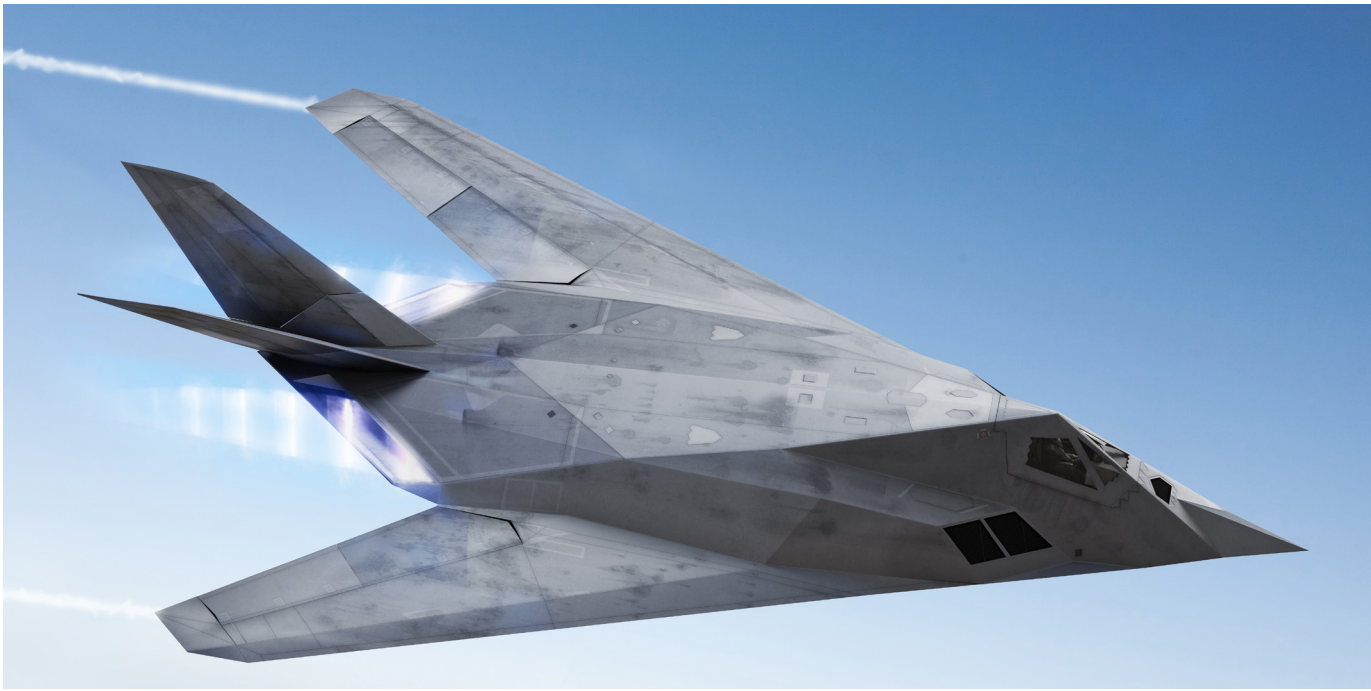
Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 00:52

WHAT CAN WE LEARN FROM THE AEROSPACE INDUSTRY?

- Redundancy is common in aerospace applications
- Self-flying airplanes are older than many think
- Road transportation has arguably a more complex environment, but less weight restrictions
- This experience helps with considering aspects for conducted disturbance testing



"In aerospace applications. It's very common to have multiple systems, multiple sensors, all working together. This is critical when you have planes that fly themselves. In fact Self flying airplanes are older than you might think. The first rudimentary autopilot was available just ten short years after the Wright brothers flew their Wright Flyer in 1903

The challenges for road transportation is even greater with many more variables and unpredictable situations. There are no pedestrians or bicycles in the sky and not a lot of traffic.

But the experience of the aerospace industry provides us with a lot of insights when considering conducted electrical disturbance testing."

AMETEK CTS GmbH Sternenhofstrasse 15 4153 Reinach, Switzerland info.cts@ametek.com

AMETEK
COMPLIANCE TEST SOLUTIONS

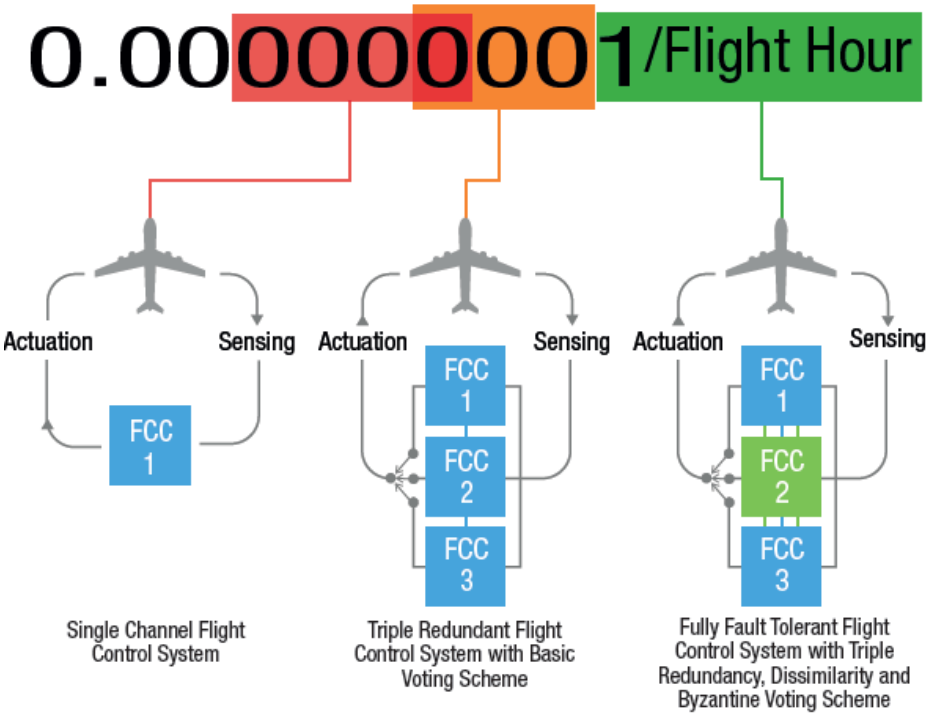
www.ametek-cts.com

Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 02:32

EXPERIENCE FROM THE AIRCRAFT INDUSTRY



"The simplest system is shown on the left, with a sensor input into a computer which then controls an actuator based on the computer program

But what the aircraft industry has figured out, is that reliability can be dramatically improved when you have multiple flight computers monitoring the sensor inputs. The computers will communicate amongst themselves and they'll agree on the optimum course of action, in practice this may mean 2 computers out voted a third.

The most complex method that is being used today, and the most reliable, is for the computing system to be comprised of dissimilar computer - different software / programming language or even different hardware.

This means for example, that should there be a software fault, they can be sure that the same fault is not causing an error on all of the flight computers."

You can learn more at https://www.curtisswrightds.com/news/blog/how-to-strengthen-redundant-systems-with-dissimilarity-and-complex-voting.html

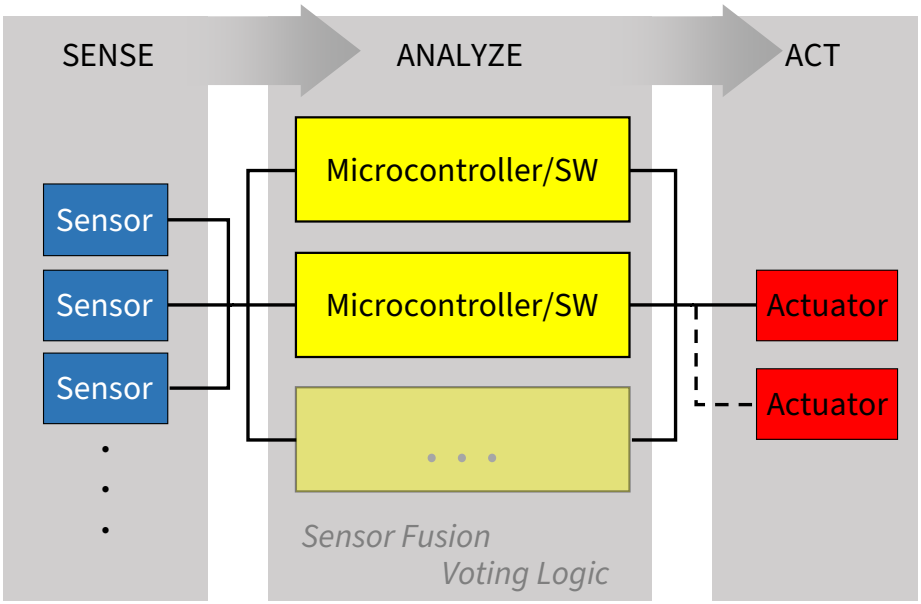
Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 04:34

CONCEPT

- In life-or-death systems, parallel decision making, is often used to evaluate all inputs and make decisions about what to do with the vehicle.
- Redundancy can apply to all three phases and their wiring harnesses. The test plan needs to take these into account.



"In the world of the car, the application of redundancy in safety is not so different. We might have multiple sensors, multiple microcontrollers and a wide range of associated actuators.

An example of this could be a steering system where the car has a back-up system that is not human, but computer controlled.

In safety critical systems, parallel decision making is often used to evaluate all inputs to make decisions about what to do with the vehicle. It's important to note that this redundancy is likely to exist not only on the sensor side, but can also be on the controller side and the related actuators.

It is therefore a requirement that an EMC test plan takes these different systems into account."

GO TO VIDEO 05:39

SAE J3016

SAE J3016™ LEVELS OF DRIVING AUTOMATION

	SAE LEVEL 0	SAE LEVEL 1	SAE LEVEL 2	SAE LEVEL 3	SAE LEVEL 4	SAE LEVEL 5
What does the human in the driver's seat have to do?	You are driving whenever these driver support features are engaged – even if your feet are off the pedals and you are not steering			You are not driving when these automated driving features are engaged – even if you are seated in "the driver's seat"		
	You must constantly supervise these support features; you must steer, brake or accelerate as needed to maintain safety			When the feature requests, you must drive	These automated driving features will not require you to take over driving	
	These are driver support features			These are automated driving features		
What do these features do?	These features are limited to providing warnings and momentary assistance	These features provide steering OR brake/ acceleration support to the driver	These features provide steering AND brake/ acceleration support to the driver	These features can drive the vehicle under limited conditions and will not operate unless all required conditions are met		This feature can drive the vehicle under all conditions
Example Features	• automatic emergency braking • blind spot warning • lane departure warning	• lane centering OR • adaptive cruise control	• lane centering AND • adaptive cruise control at the same time	• traffic jam chauffeur	• local driverless taxi • pedals/ steering wheel may or may not be installed	• same as level 4, but feature can drive everywhere in all conditions

For a more complete description, please download a free copy at https://www.sae.org/standards/content/j3016_201806/

"The standard covering these requirements is SAE J3016, which discusses levels of automation.

Today Teslas and other EVs are considered to be partial automation. With features such as lane and speed holding, with the driving environment still the responsibility of the driver.

In the future, systems will have the human as a backup and automated system will have primary responsibility.

In the case of steering a lot has be written around topics such as the force applied by the driver to the steering wheel to override the automated system.

What's not defined in the standard, is what needs to happen in an EMC testing environment for autonomous driving."

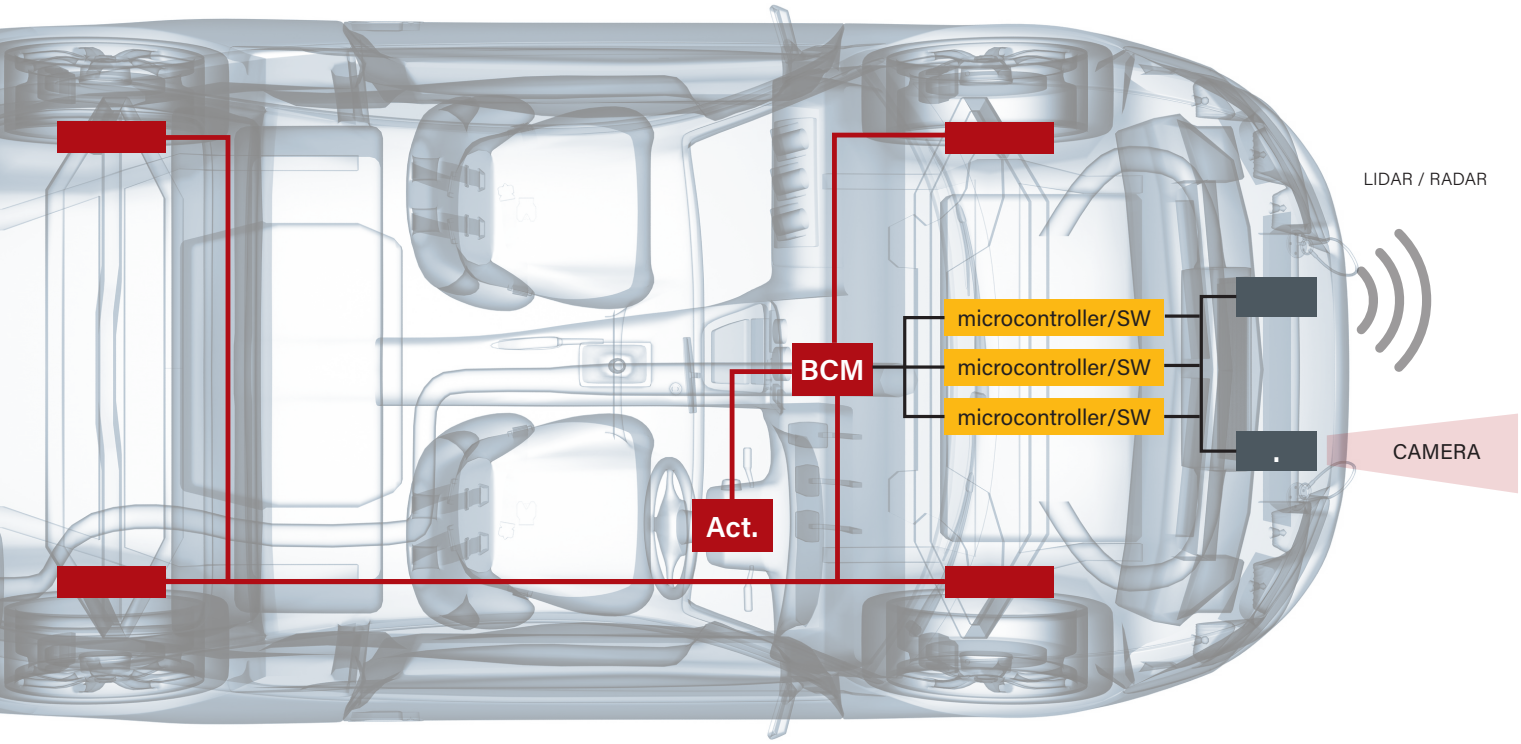
Further reading: UN ECE Portal on Automated Driving

Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 07:50

IN THE VEHICLE



"In the vehicle you very often have LIDAR, or maybe RADAR and sometimes cameras. They're working in conjunction with multiple microcontrollers monitoring and deciding what to do, and then providing output signals to the relevant actuator.

Just like in the aerospace example earlier, the system considers and acts depending on a feedback loop. But in this case we've got different types of sensors. With the camera monitoring wheel speed, and feedback coming from the acceleration and braking systems. Essentially multiple systems working together to keep the vehicle in a safe condition."

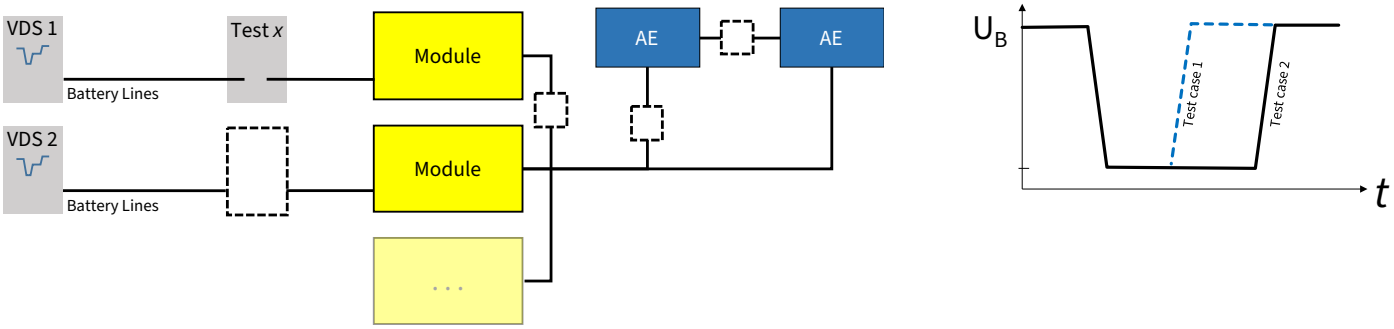
Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 08:55

STANDARDIZATION AND TEST PLAN

- The test plan needs to consider interactions between devices, and what happens if one faults out?
- Test Levels:
  An argument can be made for multiple test levels: some that shouldn't cause a fault, and one that will cause a fault - to see how redundant systems react.



So we have an example here. This is a DC source voltage, voltage drop simulator, where we might have multiple batteries and inputs into the various modules.

Now what you can do is take a test. Here's test X will leave this generic for the moment. And we can perform that test on module A, but not module B and the reason you might want to do that is to see what happens in the vehicle if you have a fail condition.

And you can put that similar kind of tests on a secondary module. You can put it on the communication slides between modules. You can put it in the communication lines between the actuators, that's part of your test set up.

Ultimately it all comes down to the test plan which needs to reflect the different levels of importance attached to individual systems. Is a system more safety related to a manufacturers safety consideration or failure classifications

In this example we're using time-based fault and in test case 1 we want the DUT to have no failures but in test case 2 we might want to intentionally cause a fault to see not how that module reacts. And how modules in parallel to that module, the redundancy modules to see if they kick in and if they start to do their function. We could leverage this test levels or multiple test case scenarios in order to make our redundancy systems more even more reliable.

Recently, manufacturers are even putting multiple redundant wiring harness is in the system, so that so that not only is the is the sensor the microcontroller and the actuator level redundant, but also wiring harness. These considerations should be included into your test plan for those kinds of tests.

Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 12:50

TEST SET-UP EXAMPLE

" Here is a practical example, we have on the left rack one and on the right track two and both of those are DC sources.

What we're trying to achieve in this case is we have one arbitrary waveform generated on our autowave and it's controlling through a T connector the left and the right hand rack.

Arbitrary waveform generators typically have multiple channels. At AMETEK-CTS we have we have versions 2, 4 and up to 8 channel devices, so you can independently control the voltage that goes to multiple redundant systems. But in this specific application we wanted to do 100% synchronization between the left and right during the test.

The devices on the far left and right of the image are dropout switches. What happens is the left hand dropout switch and the right hand drop out switch can be perfectly synchronized within microseconds.

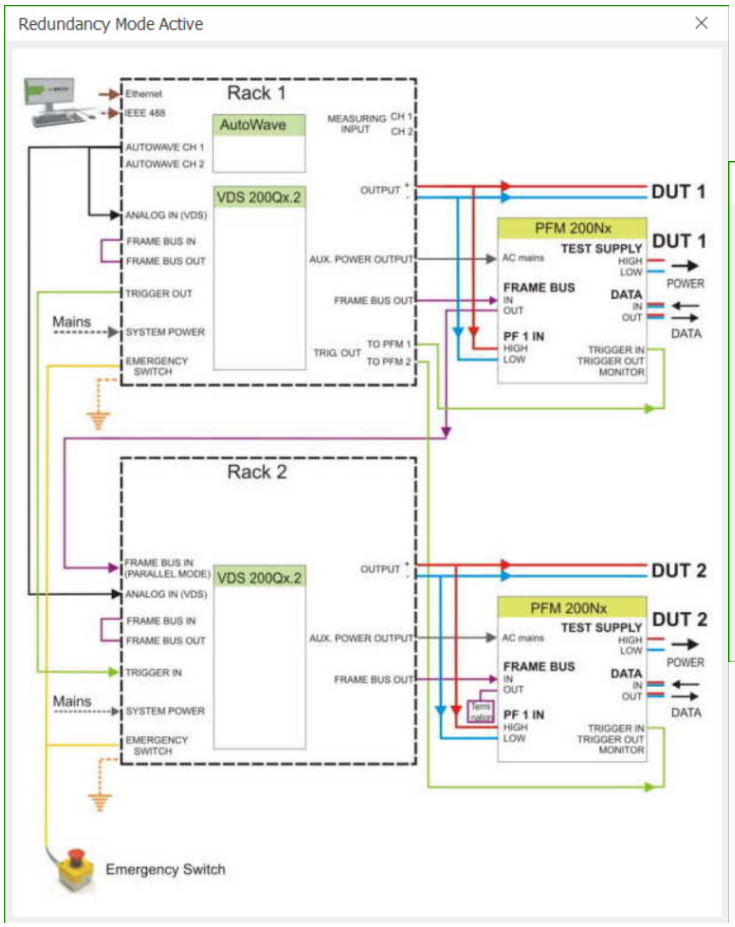
What you can do with those drop out switches is not only battery voltages, but also signal lines. And that's important because what we're doing on the signal lines is as critical as the battery lines. "

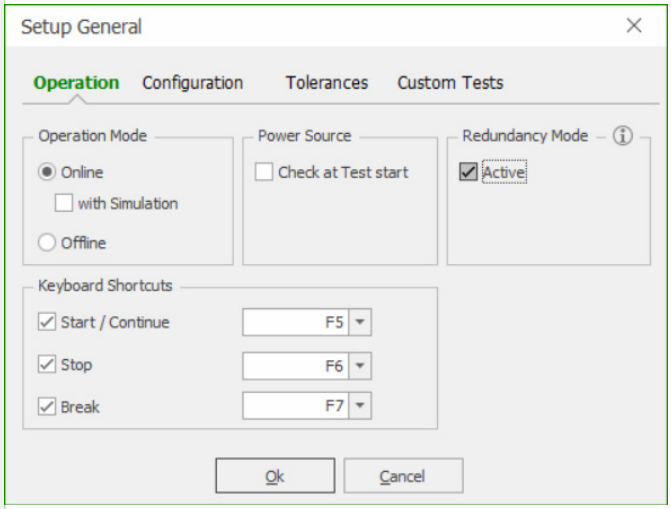
Insights and best practice

EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 15:02

SOFTWARE SETTING





In the software setup, from the example, we have the two different racks - Rack 1 and Rack 2.

And then we have the PFM - power fail module - which does both signal data and battery lines, and they can be synchronized over our digital proprietary buses called Framebus

Because of the developments that are taking place around redundant systems we've added a redundancy mode which can be activated in the set-up.

Insights and best practice

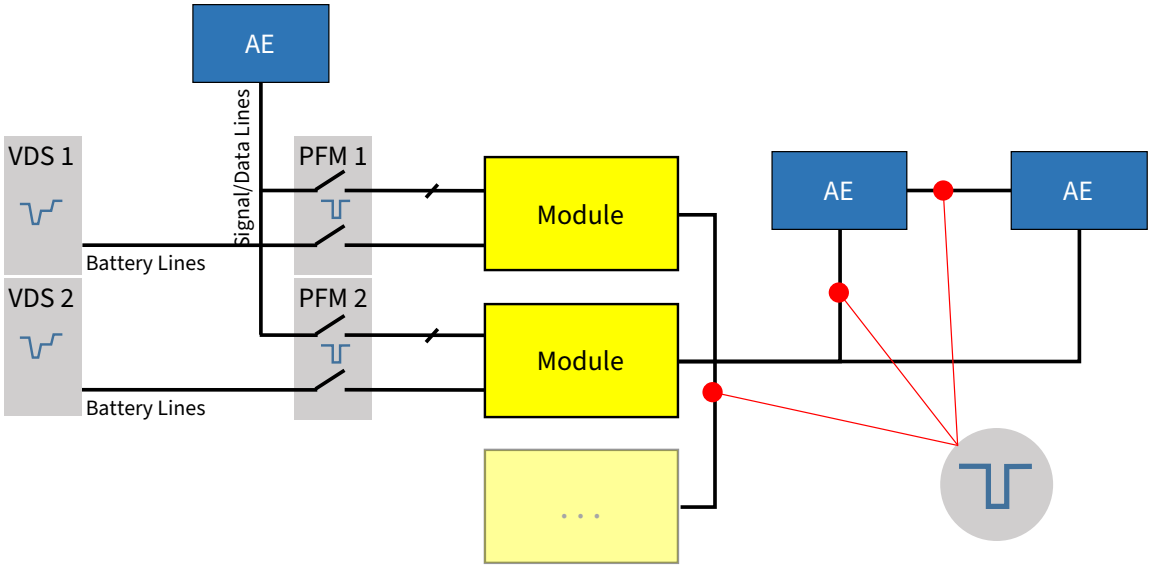
EMC COMPLIANCE KNOW-HOW

GO TO VIDEO 15:47

EXAMPLE FROM DROPOUTS – NEW PFM REDUNDANCY OPERATION

- Users can introduce dropouts in any necessary topography in the vehicle.

  Battery or signal/data lines. Either redundantly (all modules), or singularly (one module) to ensure that the other redundant systems switch properly



"Some additional examples for dropouts which highlight some of our new PFM redundancy operation. Here you can take the PFM and you can put it between the DC source and whatever module you're trying to test.

You can also do these kinds of tests between the controller and the actuator or between the two different actuators. You can run them on either signal or data lines either redundantly or singularly to ensure the other redundant systems switch properly or the backup systems operate when they have to."

Insights and best practice

EMC COMPLIANCE KNOW-HOW

About Tim Horacek

Tim is the Automotive Product Manager for 20 years, and expert in the ISO/TC 22/SC 32 working group. Tim has been in Test and Measurement for 30 years, starting in a military accredited calibration lab and expanding into software automation and product marketing.

About AMETEK CTS

AMETEK CTS is a global leader in EMC compliance testing and RF power amplifiers. AMETEK has been designing and manufacturing precision instruments for more than 30 years. Under the brand names of EM TEST, Teseq, IFI and Milmega the company produce a wide range of specialist solutions aligned to the individual needs of equipment manufacturers across a variety of industries. These include:

Automotive
Aerospace and Defense
Consumer electronics
Household appliances
Medical devices
Renewable energy

From its design and manufacturing facilities in Switzerland, Germany, the United States and the UK, AMETEK CTS provides customers with innovative solutions to the complex requirements of EMC compliance standards.

AMETEK CTS GmbH Sternenhofstrasse 15 4153 Reinach, Switzerland info.cts@ametek.com

AMETEK
COMPLIANCE TEST SOLUTIONS

www.ametek-cts.com