CHAIRMAN Resource

From: Tom Gurdziel <tgurdziel@twcny.rr.com>
Sent: Wednesday, May 22, 2019 8:40 PM
To: CHAIRMAN Resource
Cc: Transformation.Resource@nrc.gov; Bridget Frymire; Tim Echols; Screnci, Diane; Esberg, John R:(GenCo-Nuc); Miller, Eric
Subject: [External_Sender] More Thoughts Resulting from the 5/14/2019 Commission Meeting on Digital Instrumentation and Control

Good morning,

I have been thinking that discussion of Common Cause Failure, (CCF), for digital equipment has centered on the frequency of occurrence. Is that the case? If it is maybe we should just assume the occurrence of a (digital) common cause failure and worry, instead, about what would be the result. If human being action(s) could replace the failed digital (control) system, maybe we don't really have a problem. It would be my thought that such substitute (human) control would be most likely to be successful if the digital system is provided with a self-monitoring capability.

Here is what I am suggesting.

You need the digital control system, of course.

It must self-monitor itself every couple of hours and provide an alarm/notification when it is not in perfect health.

It cannot fail such that it prevents effective human being control (such as with the Boeing 737 Max 8 aircraft.)

Wouldn't that be sufficient? You then have 100% testing and redundant/diverse back up. What more is needed?

Thank you,

Tom Gurdziel