PMSTPCOL PEmails

From: Joseph, Stacy
Sent: Monday, August 22, 2011 11:12 AM
To: 'ccchappell@stpegs.com'
Cc: STPCOL
Subject: Member Brown response to ACRS Action Item 87
Attachments: C Brown Response to 11_06_21 SC Mtg Action Item 87 TG OST.doc; NINA Slides TG Primary & Emergency OST 11_02_02.pdf

Coley,

See attached response from Mr. Brown on ACRS action item #87. Please be prepared to address at 10/4 meeting.

Stacy

Stacy Joseph
Project Manager
U. S. Nuclear Regulatory Commission
Office of New Reactors
Division of New Reactor Licensing

(Office) 301-415-2849
Mail Stop T6-D04
Washington DC 20555-0001

Hearing Identifier: SouthTexas34Public_EX
Email Number: 3000

Mail Envelope Properties (BBC4D3C29CD0E64E9FD6CE1AF26D84D58C02BE8EFF)

Subject: Member Brown response to ACRS Action Item 87
Sent Date: 8/22/2011 11:12:28 AM
Received Date: 8/22/2011 11:12:28 AM
From: Joseph, Stacy

Created By: Stacy.Joseph@nrc.gov

Recipients:
"STPCOL" <STP.COL@nrc.gov>
Tracking Status: None
"'ccchappell@stpegs.com'" <ccchappell@stpegs.com>
Tracking Status: None

Post Office: HQCLSTR01.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	386	8/22/2011 11:12:28 AM
C Brown Response to 11_06_21 SC Mtg Action Item 87 TG OST.doc	67578	
NINA Slides TG Primary & Emergency OST 11_02_02.pdf	579771	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

The following figure will be added to COLA Part 2, Tier 2, Section 10.2.

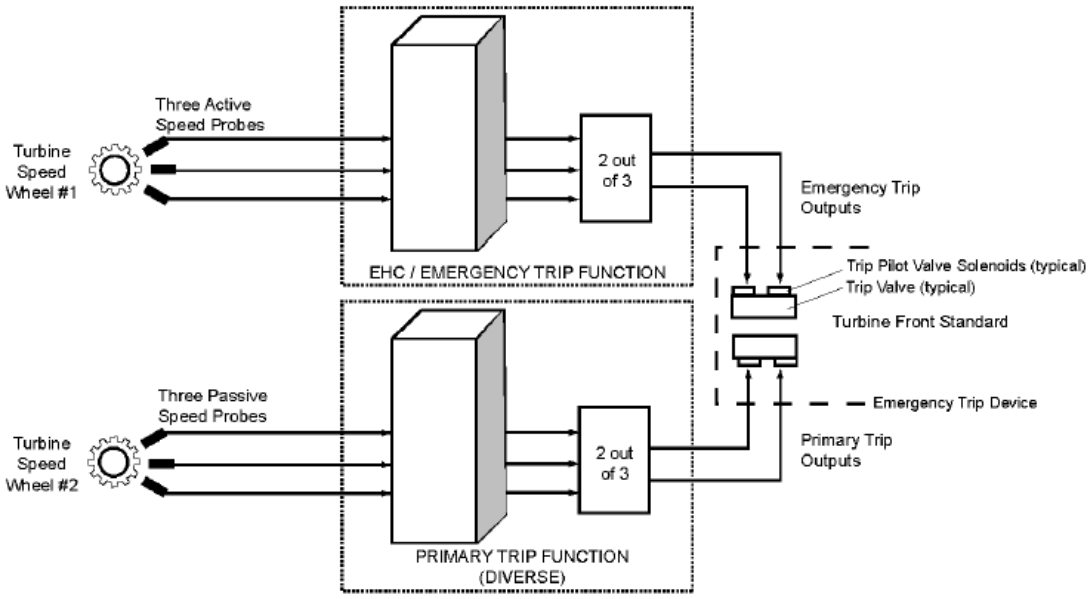


Figure 10.2-5 Turbine Overspeed Trip System Functional Diagram

C Brown Discussion: For my review of the TG OST functions, several RAIs were provided. The last set was forwarded by NINA letter U7-C--NINA-NRC-110006, which had 8 attachments. These were provided to resolve Action Item 45 which I agreed we could close, based on the RAIs. However, in Att. 5, page 5, NINA identified the following revisions to the COLA Rev 4:

"Changes from COLA Rev 4 are indicated by gray shading.

10.2.2.4 Turbine Overspeed Protection System

The information in this subsection of the reference ABWR DCD is replaced in its entirety with the following information.

STP DEP 10.2-3

The electro-hydraulic control (EHC) system provides the normal speed control system for the turbine and comprises a first line of defense against turbine overspeed. This system includes the main steam control valves (CV), intermediate steam intercept valves (IV), extraction system non-return valves, and fast-acting valve-closing functions within the EHC system. The normal speed control unit utilizes three speed signals. **Loss of any two of these speed signals initiates a turbine trip via the Emergency Trip System (ETS)."**

The speed sensors referenced in the last sentence are the sensors that feed the Normal Speed Control function and the Emergency Trip Function shown in Figure 10.2-5 above. They are active sensors requiring power sources.

The question I asked was "Does the loss of any two of the passive sensor signals that feed the Primary Trip Function shown in Figure 10.2-5 also initiate a turbine trip?"

NINA had no answer at the time.

On 6/23/11, The STP answer in Action Item slides 14 and 15 is No.

I do not agree with their conclusion since they are saying that loss of signals from the passive sensors for the Primary (diverse) Trip Function doesn't matter since (see STP Action Item response presentation pages 14 and 15):

1. They do not affect the redundant Emergency OST or the Normal Turbine Speed Control, and

2. Operators will know they failed and can take appropriate manual action.

All of the discussion on the OST system is because the design has two electrical OST functions and not one electric and one mechanical as expected. The design they have proposed has a satisfactory redundant and diverse architecture and that is why I agreed with closing Action Item 45. However, the details on component failure response were fuzzy and the staff pushed to get more detail.

Now the detail reveals that loss of signal from two of the three sensors does not initiate a turbine trip, but the loss of two of the active sensor signals of the Normal Speed Control and Emergency Trip function does produce a trip. This seems counterintuitive.

The problem is that the same active sensors feed both the Normal Speed Control and the Emergency Trip Function. This sets up a design where a sensor common mode failure can do two things. It can tell the Normal speed control to speed up and at the same time disable the Emergency Trip Function. While the likelihood is small that will happen, I have been involved in a circumstance where it did and the system was an analog system not a software based system as is being proposed.

My second attachment (two slides dated 2/2/11) shows the design in more detail and further illustrates the problem. Slide 8 is an expansion of Figure 10.2-5 above showing that the trip monitor processor is independent of the Normal Speed Control processor. Slide 7 shows that each active sensor feeds all three speed monitor processors for the Emergency Trip Function further enhancing the chance for one sensor to trick all monitors, particularly since each has a power

supply that can generate garbage that can be passed through to the processors. Not shown is how these same active sensors feed the Normal Speed Control function. I suspect that it has the same three processors with each sensor feeding all three.

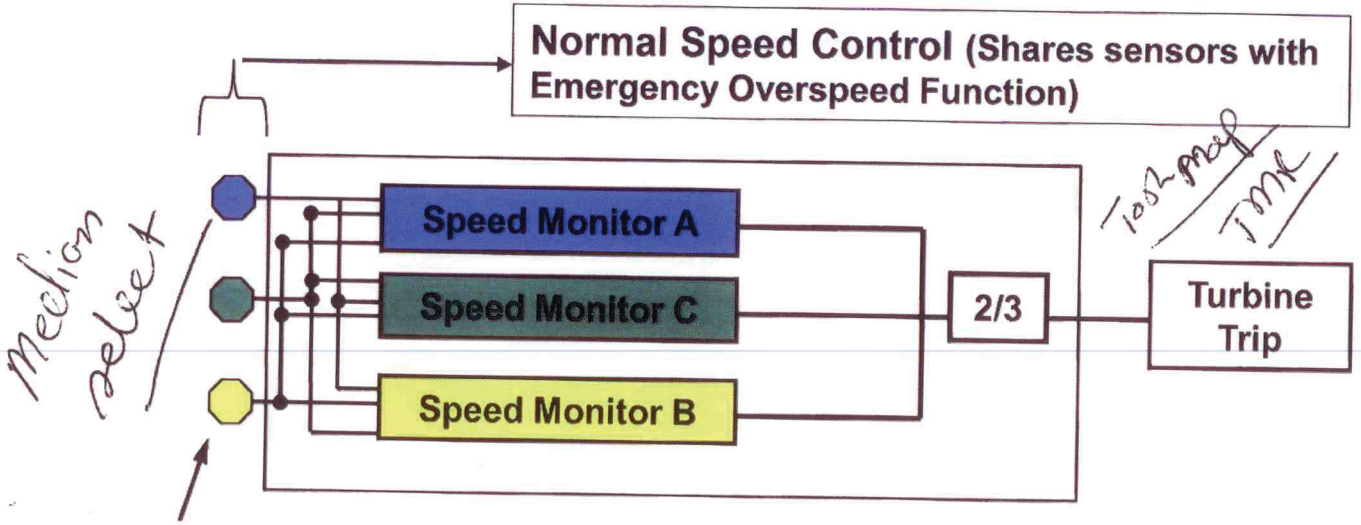
This makes for a very reliable stay on line architecture, which is good, but has less assurance of not having one sensor compromise not only the Emergency Trip Function, but also possibly falsely tell the TG to speed up.

Conclusion 1 - Unless there is something I have missed, the Primary Trip Function must not just alarm, but that the loss of signal or failure of two of the three passive sensors should initiate a trip as well.

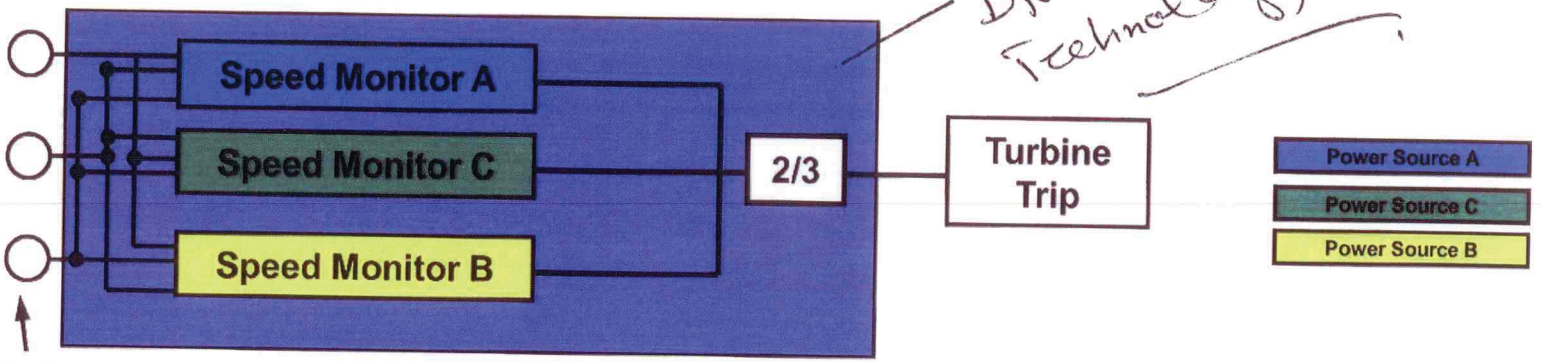
Note: The Primary Trip Function also has each sensor feeding all three of the monitor processors. However, they are required to be passive and the location inside the enclosure shields them (for the most part) from stray fields.

Conclusion 2 - This is a very good example of why detail counts when licensing DI&C designs. You should note that this detail is independent of the technology change which is frequently argued to not require detail.

Primary Overspeed Trip and Emergency Overspeed Trip Functions



3 Speed Pickups (Active) for Emergency Overspeed Trip Function
(Active detector needs power supply)



3 Speed Pickups (Passive) for Primary Overspeed Trip Function
(Each passive detector needs no power supply)

Summary of Turbine Overspeed Protection including Power Sources