Draft ISG-06, "Licensing Process," Revision 2 Tabletop Exercise
June 13-14, 2018

Sample Regulatory Commitments

Commitment 1
The platform tool will not normally be running while the platform is performing its safety function as described in Section [x.y] of the platform Safety Evaluation. If the platform workstation is connected during online safety operation for maintenance or troubleshooting purposes, its use will be controlled via administrative controls and qualified maintenance personnel.

Commitment 2
With the keyswitch not in RUN, the plant protection system (PPS) application will initiate an alarm on the Main Annunciator System and the channel for each function processed by the platform system protection set within the safety division will be declared inoperable with respect to its safety function.

Commitment 3
The electrical isolation qualification of the Class 1 E/non-1 E data communication will be qualified with an isolation fault test that will be conducted per IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1 E Equipment and Circuits" and Regulatory Guide 1.75, "Criteria for Independence of Electrical Safety Systems." This will be documented in a supplemental test report to be issued by [insert date].

Commitment 4
Control of operation of the platform keyswitch will be included in a procedure to ensure the protection set is declared inoperable when the keyswitch is not in the RUN position.

Commitment 5
Modification of platform application software will always be performed using approved plant procedures and will normally not be done with the plant online.

Commitment 6
Using approved plant procedures, addressable constants, setpoints, parameters, and other settings utilized in the platform PPS will be changed in one PPS protection set at a time.

Commitment 7
The algorithms in [Setpoint Methodology document] used to determine the Technical Specifications setpoints assume that actions specified in Section [x.y] of [Setpoint Methodology document] are included in the plant surveillance procedures. The actions specified in Section [x.y] of [setpoint methodology document] will be included in the plant surveillance procedures during implementation of the amendment.

Commitment 8
The licensee will continue to implement the commitments for the RTS and ESFAS reflected in Amendment [x] to avoid risk-significant plant-specific configurations and will continue to use the plant's plant-specific configuration risk management program procedure to provide plant configuration control and management with the PPS replacement.

Commitment 9
The licensee will verify that the maximum test voltages applied to the platform during qualification testing envelope the maximum credible voltages for the Non-Class 1 E interfaces with the PPS.

Commitment 10
The platform's response time will be verified as part of the FAT to verify that platform throughput time is bounded by the calculation and in no case exceeds the PPS replacement allotment (plus contingency) in accordance with the Interface Requirements Specification. The results will be documented in the [test report name and number], that will be available for inspection at the completion of FAT for the platform PPS replacement system.

Commitment 11
The platform FAT will test all specified safety-related functions and will also test the following interfaces:

1. Safety-related 4-20 mA DC analog temperature input signals from [separate subsystem]; these signals will be generated by a loop simulator or equivalent test equipment.
2. The FAT will verify bidirectional non-safety communications from the platform communication modules to the platform maintenance workstation (MWS) through the [platform specific network equipment].
3. The FAT will verify continued Multicast transmission from the communication modules in the event of MWS network communication failure.
4. The platform FAT configuration will include the MWSs, network switches, and any associated equipment.
5. The FAT will verify no inbound communication path from [platform specific port] to [platform specific port] exists.
6. The FAT will verify outbound communications from [platform specific port] of the [platform specific network equipment].

Commitment 12
1. The licensee's SAT will be performed on an integrated system, including the platform system, MWSs, network switches, and associated equipment.
2. The physical connection of the temperature channels from the [separate subsystem] to the platform will be verified during the SAT.
3. The SAT will verify interfaces that cannot be tested at the platform's FAT, including, in part, verification of information that is transmitted to the plant computer and the control board display.
4. Additional testing of communications between the platform and its MWS (including network failure) will be performed at the SAT.
5. The integrated system used for SAT will also be used to perform training and to develop and verify operational and maintenance procedures.

Commitment 13
The licensee will verify that the secure operational environment design requirements and configuration items intended to ensure reliable system operation are part of the validation effort for the overall system requirements and design configuration items, in accordance with RG 1.152 Regulatory Position 2.5.

Commitment 14
The licensee will verify that the platform developer correctly configured and enabled the design features of the secure operational environment, and that the developer tested the system hardware architecture, external communication devices, and configurations for unauthorized pathways and system integrity, in accordance with RG 1.152 Regulatory Position 2.5.

Commitment 15 [Response to Tricon V10 ASAI 7 example]
The licensee will verify, as part of the FAT, that the platform channel response times satisfy plant- and application-specific requirements for system response times presented in the accident analysis in Chapter 15 of the plant safety analysis report.

Note that some of these Commitments may become License Conditions