ORNL/TM-2023/3008

Technical Specification Surveillance Interval Extension Using Self-Diagnostics

Michael Muhlheim
Garill Coles
Pradeep Ramuhalli
Ron Jarrett
Edward Quinn
Vivek Agarwal

August 2023

OAK RIDGE National Laboratory

ORNL IS MANAGED BY UT-BATTELLE LLC FOR THE US DEPARTMENT OF ENERGY

ORNL/TM-2023/3008

Nuclear Energy and Fuel Cycle Division

TECHNICAL SPECIFICATION SURVEILLANCE INTERVAL EXTENSION USING SELF-DIAGNOSTICS

Michael Muhlheim
Garill Coles*
Pradeep Ramuhalli
Ron Jarrett**
Edward Quinn**
Vivek Agarwal***

* Pacific Northwest National Laboratory
**Paragon Energy Solutions
*** Idaho National Laboratory

August 2023

Prepared by
OAK RIDGE NATIONAL LABORATORY
Oak Ridge, TN 37831
managed by
UT-BATTELLE LLC
for the
US DEPARTMENT OF ENERGY
under contract DE-AC05-00OR22725

CONTENTS

ABSTRACT

As part of the Light Water Reactor Sustainability program, an ongoing research effort is being conducted on technical specifications surveillance interval extension of digital equipment in nuclear power plants. The research team is led by Idaho National Laboratory and includes Pacific Northwest National Laboratory, Technology Resources, and Oak Ridge National Laboratory.

This research focuses on developing methods for applying the U.S. Nuclear Regulatory Commission (NRC)–approved guidance to implement a licensee-controlled, risk-informed surveillance frequency change program in digital instrumentation and control (I&C) systems that include self-diagnostics and online monitoring (OLM) capabilities. Although approved methods exist for extending technical specifications (TS) surveillance test intervals (STIs) for general equipment, including analog I&C equipment, gaps remain in technology and guidance on crediting newer digital equipment's internal self-diagnostics and OLM characteristics. Previous research described a general methodology for crediting internal self-diagnostics for extending surveillance test intervals. The methodology used self-diagnostics to detect—and credited recovery from—failure. Self-diagnostics were also applied for performance monitoring during the extended surveillance interval.

This report discusses the status of recent activities to evaluate the previously developed methodology using a pilot study. Although both a utility partner for a pilot study and a specific digital asset were identified in FY2020, delays in obtaining proprietary information resulted in a limited ability to fully evaluate the methodology, and further interactions were complicated by the COVID pandemic. Therefore, at that time, the use of public-domain information—along with current processes for surveillance interval extension through a surveillance frequency control program—identified the need to fully assess diagnostic coverage as part of the pilot study. Furthermore, self-diagnostics were also identified as a potential option to replace the drift analyses conducted as part of current STI extension procedures.

In FY2022, the project was reconstituted with the industry partner, and information and data were made available by the industry partner to the research team for review. The shared information included failure event descriptions and data for a digital I&C system since its implementation, as well as recent STI extension interval reports developed by the utility partner on that digital I&C system. This report presents an evaluation of this information and data and describes an application of the proposed methodology cited above. The methodology seeks to take advantage of the self-diagnostics and OLM capabilities to reduce risk or reduce the level of qualitative monitoring assessment needed to perform a risk-informed STI extension using existing NRC approved guidance or both.

Addressing these issues of STI extension by crediting self-diagnostics is likely to result in benefits for current and future nuclear power plant (NPP) operations, including lowering the barriers to adoption of digital I&C systems and increasing cost savings by deferring or eliminating unneeded preventive maintenance (tasks or checks or activities). Specifically, self-diagnostic and OLM capabilities of newer digital equipment being installed in non-safety and safety applications are designed to detect failures, provide early warning of potential failures, and notify plant operators to take appropriate action to reduce out of service (OOS) time thus protecting safety margins. Moreover, the equipment is expected to provide information that time-related operational degradation is identified early to ensure timely and planned corrective actions instead of a reactive and unplanned approach ahead of an extended-surveillance interval.

1. INTRODUCTION

This activity's objective is to develop and evaluate a methodology for extending technical specification (TS) surveillance test intervals (STIs) for digital equipment used in commercial nuclear power plants (NPPs). The goal is to define methodologies that integrate advancements in online monitoring (OLM) and equipment self-diagnostics with risk assessment methodologies to reduce operating costs and enhance the reliability of commercial NPPs. Previous research developed an initial methodology for surveillance interval extension that integrated risk assessment methods with self-diagnostics, building on the surveillance interval extension methods described in the previously approved TSTF-425 framework [1, 2]. This report documents initial results of evaluating the aforementioned methodology using a planned pilot-scale study. The outcomes of the project will provide technologies enabling industry-led innovation and technology deployment in the current fleet of US NPPs to reduce maintenance costs to assist the nuclear industry remaining economically competitive and viable option in the energy market.

1.1 BACKGROUND

TSTF-425, Rev. 3 [3] is applicable to all standard technical specifications for NPPs and requires the application of the Nuclear Energy Institute (NEI) 04-10, Rev.1 [4].[1] Each licensee applying for the changes proposed in TSTF-425 will need to include documentation regarding the probabilistic risk assessment [PRA] technical adequacy[2] consistent with the guidance in Regulatory Guide 1.200 [5].

The TSTF-425 framework and the associated guidance documented in NEI 04-10 describe a generic process for moving TS required surveillance tests to a licensee-controlled surveillance frequency control program (SCFP). The TSTF 425 framework requires the use of risk assessment methodologies to provide assurance that STI extension will not increase the risk in an unreasonable manner. The framework and guidance are applicable to both analog and digital equipment, though there appear to be additional methods related to crediting internal self-diagnostics and OLM characteristics of newer digital equipment that may augment existing guidance and technology.

Prior research activities on the development of a methodology for extending TS surveillance intervals for digital equipment included [1]: (1) a review of how the existing approach to achieve TS surveillance interval extension using the NEI 04-10 guideline was performed; (2) identification of digital equipment with built-in OLM and self-diagnostic capabilities that are considered by plants for installation in non-safety and safety applications; and (3) development of an initial high-level workflow for crediting self-diagnostics features of digital I&C equipment within a surveillance frequency control program (SFCP). This workflow consisted of three basic approaches to crediting self-diagnostics (summarized here and detailed in Section 3).

- In Approach 1, no credit is taken for self-diagnostics as part of the risk analysis. Instead, self-diagnostics are credited as a tool for monitoring the plant's performance only once the extension period is determined. This approach might be applicable for tested functions that have a small impact on the overall plant risk without crediting the self-diagnostic capabilities of digital equipment yet can be used to leverage other benefits of employing self-diagnostics.

[1] The NRC staff reviewed and approved NEI 04-10, Rev. 1, by letter dated September 19, 2007. [NRC ADAMS Accession No. ML072570267]

[2] The term "PRA acceptability" and related phrasings in RG 1.200 Rev. 3 are synonymous with previously used terms such as "PRA quality" and "PRA technical adequacy." The staff is using the term "PRA acceptability" with respect to the scope, level of detail, conformance with PRA technical elements (i.e., technical adequacy), and plant representation of a PRA as related to the outcome of the NRC staff's review of a given risk-informed application. For additional information, see DPO-2016-001 (ADAMS Accession No. ML17013A015).

- In Approach 2, self-diagnostics are credited in the risk analysis for reducing the risk contribution of failures that can be detected, diagnosed, and recovered in a timely fashion. Using this approach, the risk increase associated with the STI extension is shown to be acceptable. In addition, self-diagnostics might also be used for performance monitoring once the extension period is determined.

- Approach 3 is used when Approaches 1 and 2 are unsuccessful. In this approach, the plant surveillance test procedure, which may cover multiple tests, components and functions, is deconstructed with the objective of performing the STI extension only for the subset of functions covered by the surveillance test of most interest.

Given the potential for reducing maintenance costs through TS-STI extension, industry groups are conducting related research. However, this research differs from industry-led activities for TS-STI extension in the following ways.

- Industry-led research is focused on crediting the self-diagnostics capability of digital equipment (to our knowledge) to eliminate or replace some current surveillance testing, with the methodologies potentially requiring regulatory review and approval. In contrast, this effort is focused on methodologies that can be accommodated under the TSTF-425 framework. It should be noted however, that not all current surveillance testing can be eliminated with self-diagnostics and completeness of the testing would need to be addressed.
- The current TS-STI extension process and practice is to assume limits on each surveillance frequency extension (doubling the frequency at maximum) and additional long term data collection, whereas the proposed methodology in this project examines whether such limits can be increased substantially by developing approaches for crediting diagnostic functionality in a risk-informed methodology.
- Methods developed by industry on TS-STI are likely to be proprietary to digital asset vendors. The proposed work would result in a more general set of guidelines that can be adapted by individual utilities to meet their specific needs. The proposed research outcomes would also benefit both types of currently operating plants in the United States, pressurized water reactors and boiling water reactors.
- Industry's proposed use/credit of IEC 61508 safety integrity level (SIL) certification and published reliability for components would be in lieu of in situ plant data. The proposed methodology in this project is evaluated using actual plant data. It recognizes that generic data and SIL certification may not provide information at the level needed to properly evaluate TS-STI, though generic data may be able to supplement analyses when plant data availability may be limited.

The project team used a combination of available public-domain information on digital equipment reliability and the consequent impact on system unavailability and reviewed information and data supplied by a utility partner. Open data sources include unavailability assessments using historical failure data (for example, NUREG/CR-5500 [6]); vendor published non-proprietary information on failure information and surveillance test intervals (for example, from the International Electrotechnical Commission [7, 8]), safety analyses reports and evaluations from the regulator on licensee submittals (for example, Tennessee Valley Authority Sequoyah Nuclear Plant's updated final safety analysis report [9]), and generic failure rate information (for example, IAEA-TECDOC-478 [10]). Plant risk models are usually proprietary and difficult to access in a non-proprietary way, but documents such as NUREG/CR-5500 [6] as well as those cited above provide some information on generic risk models or models from a

specific plant used as a case study. Standard TSs were also consulted for information on TS-required surveillances and recommended surveillance frequencies in the absence of a licensee controlled SFCP.

1.2 ANTICIPATED BENEFITS

The research scope of this project will help the pilot utility develop technical evidence to implement the proposed TS surveillance interval methodology for the identified digital asset, and it will enable NPPs to accelerate minimization of inefficiencies in the current preventive maintenance strategy and enhance cost savings.

2. DIGITAL SYSTEM EXAMPLE

As a specific but highly simplified example, consider the common scenario for a pressurized water reactor in which there are two reactor protection system (RPS) trains in the logic cabinet. The RPS trains receive trip signals from the channels that indicate that a TS has been exceeded, process the signals, and then open the reactor trip breakers (RTBs) given appropriate combinations of signals from the channels. The digital instrumentation system might be applied to perform the channel processing function for signals coming from the various sensors, and it may perform the function of the channel bistable units (which compare the sensed parameters against their set point and generate a signal if the set point is exceeded). This functionality may require multiple physical (e.g., I/O, processor) modules. A solid-state protection system (SSPS, generally a separate system) is then used to perform the reactor trip voting function and operator notifications. This approach is applicable to other types of reactor designs.

Normal RPS periodic surveillance testing consists of the following steps:

1) Operator channel checks for identification of gross sensor failures.
2) Channel operability tests (COTs), or functional tests that verify functional operability and may or may not verify defined performance requirements such as accuracy.
3) Channel or loop calibration testing, which verifies the complete channel functionality, including defined performance requirements.
4) Testing of actuation of voting logic (i.e., actuation logic test or ALT).
5) Final actuation device testing, such as relays, breakers, indications, and alarms (i.e., Trip Actuation Device Operational Test or TADOT).

Most digital systems include some level of self-diagnostic checks and self-calibration to that ensure one or more of these checks are conducted periodically during operation, and generally at a much greater frequency than required by TS. This section discusses a specific example of a digital system to describe the self-diagnostics capability in greater detail. The Westinghouse Eagle-21 system is used in this section as an example of a digital system, given its longevity (over 30 years), generally high reliability, its use in multiple power plants for a variety of protection functions, and the amount of information available in the public domain.

Given the relatively long (almost 30 years) experience in the US nuclear industry operating the Eagle-21 systems, it is likely that operational data (including operational failure data) exist for the Eagle-21 system. In contrast, operational data from more recent digital systems is likely to be limited, merely because of the amount of time that these systems have been in operation. Factors that may compensate for limited operating experience—a digital device's simplicity and high testability—may provide assurance of dependability that helps to compensate for a limited operating history. However, the availability of operating data should adequately support PRA modeling of the Eagle-21. PRA modeling ease is important for implementing the TSTF-425 process, and other digital systems may lack this advantage of operational experience. Another of Eagle-21's advantages (in terms of PRA modeling ease) that may not

apply to other digital systems is its simplicity because it requires a specific subset of the sensor-to-actuation functions for I&C channels associated with the RPS.

NUREG-0847, Supplement No. 13, dated April 1994 [11], states that the Eagle-21 "software design implementation has no interrupts or reentries and uses coding standards for high level and assembly language routines, high-level module logic, and single task programs (no multi-tasking)," and is "provided in programmable read-only memory (PROM)." Note that while the simplicity of design that results from the use of these techniques can help in modeling and incorporating self-diagnostics, the potential use of self-diagnostics is not limited to older technologies and modern digital equipment incorporate a number of diagnostic techniques as part of their design.

Eagle-21 is microprocessor-based process protection system designed to be a functional replacement (over thirty years ago) of an analog process protection system used to monitor process parameters and initiate actuation of the reactor trip system (RTS) and engineered safety feature actuation system (ESFAS) per the Westinghouse Topical Report on Eagle-21 published January 1987 [7]. As such, the Eagle-21 helps to automatically keep the reactor operating within a safe region by shutting down the reactor whenever the limits of the region are approached as the results of anticipated operational occurrences (AOOs) and design basis events (DBEs.) It also provides the ESFAS initiating signals to the various safety features to prevent or mitigate damage to the core and to maintain containment integrity. Given Eagle-21's role in RTS and the ESFAS, it is by definition a safety system designed to mitigate the effects of operational and environmental conditions associated with normal operation and postulated accidents.

According to the description provided in a response to audit questions by NRC dated April 28, 2022 [12] associated with a request to adopt risk-informed completion times, the licensee stated that RTS and ESFAS include the process protection set racks including Eagle-21 and SSPS (Figure 1Figure 1). These two systems (a) generate the necessary process protection signals, combine them into logic matrices, and initiate a reactor trip or actuate necessary ESFAS equipment, and (b) maintain physical and electrical separation by providing four sets of process protection system (Eagle-21) cabinets and two sets of SSPS cabinets (racks), one for each protection train (A and B) [13].

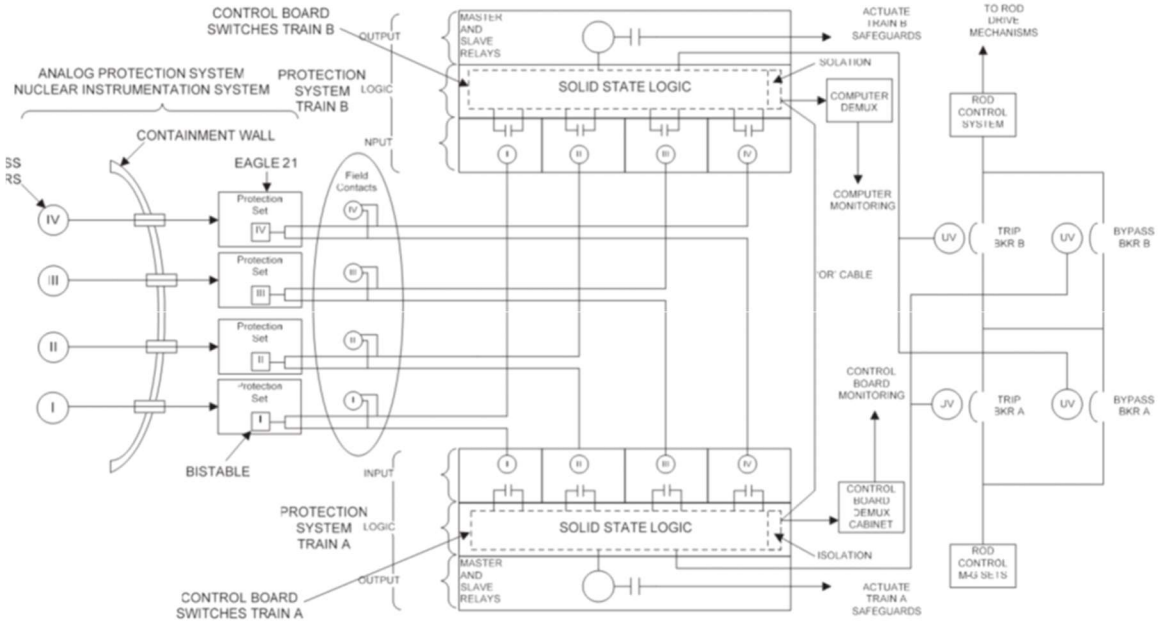

Figure 1. ESFAS simplified diagram for the RTS Showing the relative relationship of the Eagle-21 cards [12].

Protection channels that may be processed by Eagle-21 include [7]:

- RCS average temperature and delta temperature (narrow range RCS temperatures)
- pressurizer pressure and water level
- steam flow
- feedwater flow
- reactor coolant flow
- turbine impulse chamber pressure
- steam pressure
- containment pressure and temperature
- reactor coolant wide range temperatures
- reactor coolant wide range pressure
- RWST and Containment Sump levels
- steam generator narrow range and wide range water level

Transmitters (i.e., flow, pressure, level) and resistance temperature detectors (RTDs) are generally connected to provide inputs with frontend analog signal processing cards, which convert sensor inputs into voltages and digital data. Some of the input boards are also used to provide power to the sensors. The digital data are then fed to the loop control processor (LCP), which provides signal conditioning and calculation operations on the inputs and performs protection system setpoint calculations and comparative trip functions for the final channel trip signal for the SSPS voting logic [7]. Typical functions performed by the LCP are summation, lead/lag, multiplication, comparator, averaging, and square root conversion. In this sense, the function of Eagle-21 is similar to the signal conditioning and comparators/bistables functions of an analog system, where a certain input parameter configuration threshold leads to the generation (or not) of a given signal. In addition, all Eagle-21 process protection channels are configured to perform automatic surveillance testing such as a centralized test sequence processor (TSP). The LCP sends the data to the tester Subsystem through one-way communications for LCP output comparison and validation. The LCP also provides output data to the analog output modules that convert digital data to an analog signal (i.e.., 4 to 20 ma) for indication and control system inputs. A safety to non-safety isolated one-way communication link is used to transmit digital data information to the plant computer for monitoring capability.

Commonly performed surveillance tests in this system include COT checks, which are performed per TS (usually every 6 months, depending on the channel type and function) unless the surveillance tests have been extended under an SFCP.

From an STI perspective, the following cited features of Eagle-21, as noted in NUREG-0847, Supplement 13, are likely to be important [11]:

1. Built in continuous automatic platform testing that performs 24/7 testing coverage of Eagle-21 components and ensures system goes to a safe state upon a detected failure.
2. Automated test tools (Man Machine Interface – MMIs) that significantly reduce the time required to perform periodic TS surveillance tests.
3. Automatic surveillance testing to significantly reduce the time required to perform surveillance tests.
4. Self-calibration to eliminate rack drift and time-consuming calibration procedures.
5. Self-diagnostics to reduce the time required for troubleshooting.

6. Significant expansion capability to easily accommodate functional upgrades and plant improvements.
7. Modular design to allow for a phased installation into existing process racks and use of existing field terminations.

Note that similar capabilities exist in other modern digital systems [2].

Eagle-21 has several internal self-diagnostic functions [14] and associated test system communications. A man-machine interface (MMI) cart provides the human machine interface for periodic surveillance testing, parameter settings and setpoint updates, and printing out test results and internal parameter settings and values. A key feature relevant to eliminating or automating the COT function is the continuous auto calibration function that ensures the precision accuracy of Eagle-21. The LCP performs the RPS protective safety functions while the TSP performs internal self-diagnostics and provides the ability for continuous automated periodic surveillance testing. In addition, test interfaces associated with the analog output signals are used to check the health of the Digital-to-Analog conversions going to safety related indications in the main control room (MCR) and inputs to non-safety control systems. The RPS output trip status originating from the LCP is fed to the digital output modules along with a watchdog timer reset signal. These digital output modules voltage signals interface with SSPS voting logic input relays. If the watchdog timer is not reset by the LCP, the output will be set to the tripped state. Note that TSP will also provide a Set channel trip upon failure detection by the TSP's self-diagnostics. Eagle-21 also provides the ability to place the channel in bypass during surveillance tests, so the output does not go to the tripped state during online testing. Because the bypass function will disable the trip function, the allowed bypass time-period is administratively controlled by plant TS.

Like other digital systems, the Eagle-21 prevents signal drift due to its self-calibration feature in which it checks itself to a precision reference source on a periodic deterministic schedule. Section 2.3.7 of the Westinghouse Topical report on Eagle-21 [7] states that Eagle-21 PPS provides for continuous on-line self-calibration of analog input signals. The digital filter processor (DFP) provides high and low reference signals to a multiplexer circuit on each analog input channel. The DFP then compares the output of its analog to digital converters (A/D) to the high and low reference signals to determine whether any errors have been introduced by analog signal processing and A/D conversion. If necessary, the DFP automatically adjusts the D/A gain and offset to eliminate any errors.

As discussed earlier, it is expected that PRA modeling of digital systems will be necessary for the TSTF-425 process. However, the level of detail may vary depending on the complexity of the system and functions being modeled. NUREG/CR-5500, Volume 2, "Reliability Study: Westinghouse Reactor Protection System, 1984-1995" [6] proposes modeling Eagle-21 as single-module failures for each of the four channels plus the 2-of-3 and 3-of-4 common cause failure of those modules. These module failures comprise the channel processing function for signals coming from the hot temperature, cold temperature, and pressures sensors, which are then sent to a channel comparator function. Though the NUREG only addressed the Eagle-21 system functionality at the module level, Eagle-21 may also be applied to perform the function of the bistable units. The bistable function is to compare the sensed parameters against their set point and generate a signal if the set-point is exceeded. In general, the function fulfilled by the Eagle-21 may be performed physically by multiple modules and cards. Therefore, modeling of the Eagle-21 could probably be done at different levels of detail but, in the end may be limited to the level of detail that the failure data exists.

Using the example of the Westinghouse RPS design [6], one may determine the dominant failure modes that drive the unavailability of the RPS. Failure of undervoltage driver cards in both trains results in failure of RPS (unless manual scram is initiated). This common-cause failure (CCF) event is the dominant

contributor (almost 50%) to RPS unavailability [6]. Using the failure probabilities provided in NUREG/CR-5500 for the component independent failures from the Westinghouse RPS data results in a mean unavailability (failure probability upon demand) of 2.0E-5 (with no credit for manual scram by the operator) for the Eagle-21 RPS design. When manual scram by the operator is credited, the mean unavailability decreases by about 75% to 4.5E-6. This reduction is significant and occurs mainly because the manual scram signal bypasses the dominant undervoltage driver card failures. That is, the manual controls are connected downstream of discrete logic based I&C safety system outputs (i.e., close to the actuation device without any intervening logic). Issues related to reactor trip breakers, arising during the early 1980s, are no longer dominant with respect to RPS unavailability. (This is true for both cases of RPS unavailability's—with or without crediting operator action). Automatic actuation of the shunt trip mechanism within the reactor trip breakers and improved maintenance procedures have resulted in improved performance of these components.

If specific RTS modeling information including plant-specific data cannot be accessed and other applicable PRA or risk results are not available, the fault tree models, failure data, and estimated failure rates from documents such as NUREG/CR-5500, Vol. 2 (Table 2 and Appendix D) could be used to identify important RTS failures and classify them as safe or unsafe and detectable or undetectable failure failures for self-diagnostic coverage.

3. CREDITING SELF-DIAGNOSTICS FOR RISK REDUCTION: OVERVIEW OF METHODOLOGY

This section overviews the proposed methodology for crediting self-diagnostics for risk reduction and provides preliminary guidance about applying this methodology. Three high-level approaches are included in overall methodology, and are intended to be applied sequentially (i.e., assess if Approach 1 can be applied; if not, assess if Approach 2 may be applicable; and if not, evaluate Approach 3). In the event that none of the three approaches are applicable, this methodology for crediting self-diagnostics for risk reduction is unlikely to be applicable. In this case, the existing TSTF-425 guidance may be applied, or other avenues for TS-STI will need to be explored by utilities.

Approach 1 is the case where self-diagnostics is not needed to show sufficiently low risk after STI extension but might be credited as applicable for performance monitoring. This approach consists of the following workflow steps, which are illustrated in Figure 2Figure 1.

1. Use the guidance in NEI 04-10 [4] to determine the risk increase of the target STI extension in the same way that the risk increase of STI extensions for non-digital equipment is determined in the SFCP without crediting the self-diagnostics features of digital I&C equipment.

   The digital equipment of interest may or may not be modeled in detail. For example, some plant PRAs do not model the individual I&C channels and trains associated with all I&C systems included in the PRA, whether the I&C equipment is analog or digital. Similarly, some plant PRAs model the entire I&C function as a single basic event. In the case where the I&C associated with the tested function whose STI is being extended is not modeled in detail in the plant PRA, it must be clear that the modeling used in the risk analysis performed for the SFCP (See Step 12 of NEI 04-10, Revision 1 [4]) is conservative enough to bound the risk increase associated with the extension. For example, if the I&C modeling is not performed at the channel and train levels, then the failure frequency of the of the entire tested function might be increased; or if the failure of a channel or train is represented by a single basic event, then the failure of the channel or train could be set to 1.0 rather than determining a failure rate increase for the channel.

   Given the PRA modeling of the digital equipment associated with the tested function whose STI is being extended is modeled in detail, it must still be shown to be of sufficient quality to support

the risk-informed application (See NRC guidance in RG 1.200, Revision 3 [5]. Known modeling challenges exist for digital equipment, such as the lack of industry data for digital components, the differences between digital and analog system failure modes, and the complexities associated with modeling software failures.

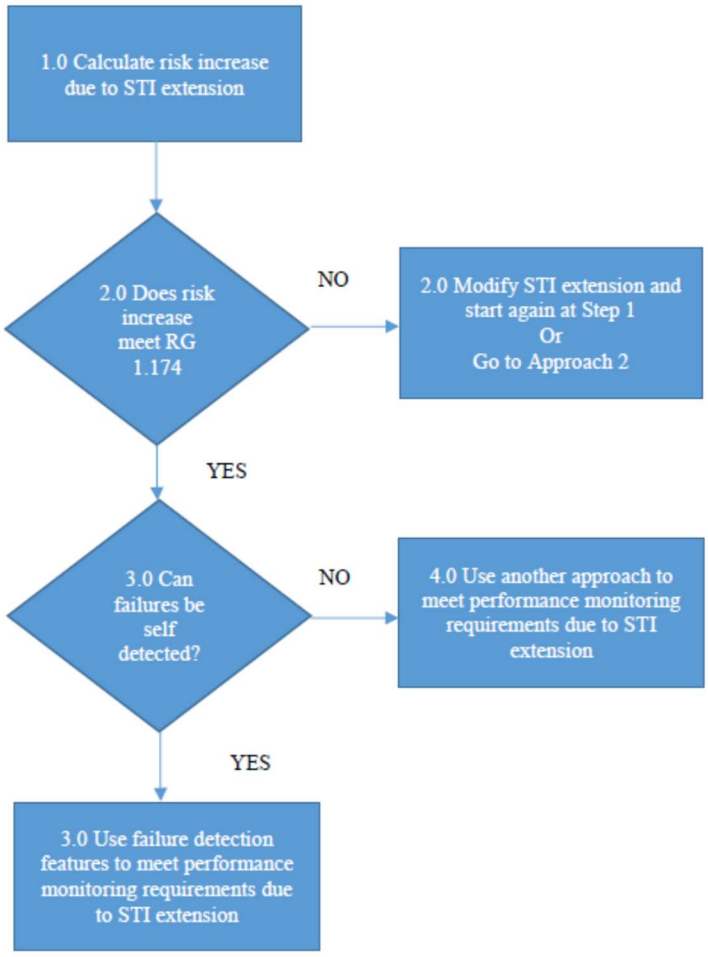

Figure 2. Approach one: self-diagnostics not credited for risk reduction.

2. If the risk increase using the guidance in NEI 04-01 (Step 12) is determined to be unacceptable, then either (a) adjust the proposed STI extension or extensions to decrease the risk and go back to the beginning of Step 1 or (b) proceed to Approach 2 if the risk increase cannot be shown to be acceptably small for any desired STI extension period. If the risk increase associated with the STI extension or extensions can be shown to be acceptably small (i.e., it meets risk-acceptance guidelines from RG 1.174, Revision 3, "An Approach for Plant-Specific, Risk-Informed Decision-making: Technical Specifications" [15]) without crediting self-diagnostics, then proceed to Step 3.
3. Determine whether self-diagnostics can be used to help fulfil the performance monitoring requirements of NEI 04-10, Step 18 (Monitoring and Feedback). This consists of confirming that no failure mechanisms that are related to the revised surveillance frequencies become important enough to alter the failure rates assumed in the justification of program changes, and ensure that

adequate component capability (i.e., risk margin) is maintained. As part of this step, it is important to document the failure mechanisms related to the revised surveillance frequencies that can be reliably detected by the self-diagnostic methods and to compare against present manual surveillance testing being performed to ensure equivalent testing coverage.

The guidance in NEI 04-10 states that the monitoring must have the following attributes.

- Enough surveillance tests are included to provide meaningful data.
- The test is devised such that incipient degradation can reasonably be expected to be detected.
- The licensee trends appropriate parameters as necessary to provide reasonable assurance that the component will remain operable over the test interval.

Self-diagnostics provide continuous real-time testing and may have the capability to detect incipient failures or degradation that has not yet resulted in a failure. By providing real-time data, there is also the opportunity for real-time or near-term assessment of the data (e.g., trend analysis of incipient failures).

An important element of this step is that the determination of which failures modes cannot be detected by the self-diagnostics are detected by surveillance tests (i.e., determination of the fault coverage). If there are important failure modes that can be detected only by surveillance tests, then information about the results of tests that reveal those failures is also needed to support the Performance Monitoring criteria required by NEI 04-10.

If the self-detected failure modes can be used to support performance monitoring for the STI extension, then consider the benefits of using the self-diagnostics for performance monitoring. If failures cannot be self-detected or if there is no benefit to using the self-diagnostics for performance monitoring, then proceed to Step 4.

4. If self-diagnostics cannot be used to fulfill the performance monitoring requirement, then a more traditional approach could be used, one that includes monitoring test surveillance results to ensure that the performance monitoring requirements of NEI 04-10 are fulfilled.

Approach 2 is the case where self-diagnostics are credited for risk reduction and might also be credited for performance monitoring. This approach consists of the following workflow steps illustrated in Figure 3Figure 3.

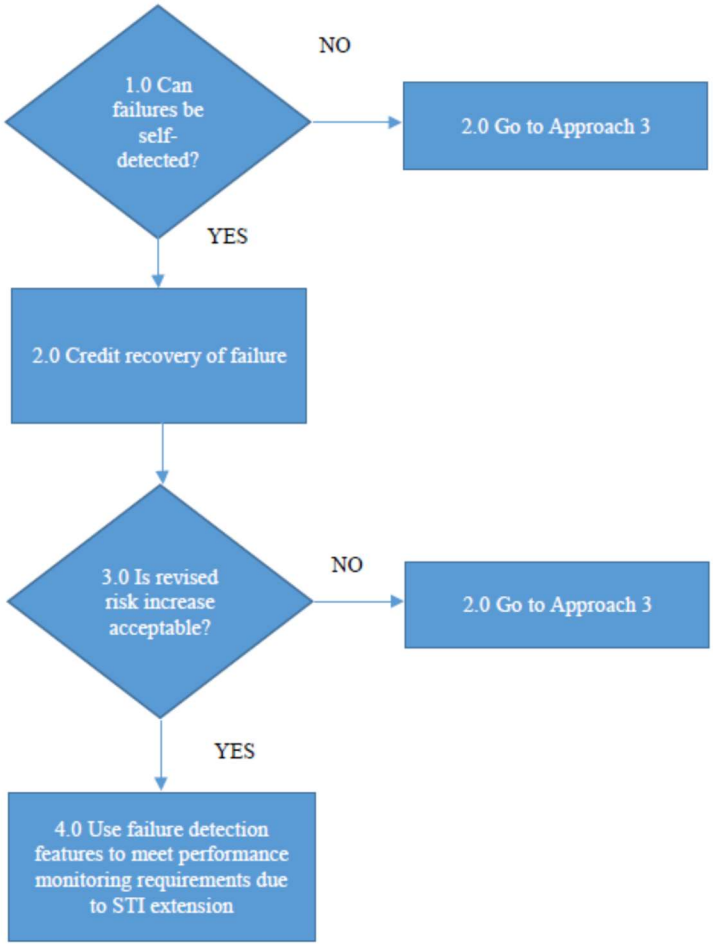

Figure 3. Approach two: self-diagnostics credited for risk reduction.

1. Determine the failure modes that can be detected by self-diagnostics of the digital equipment versus the failures that can only be detected by surveillance tests associated with the tested functions whose STIs are being extended. A review of plant surveillance testing procedures associated with the applicable functions should be performed to define existing critical tests required for operability. For new systems, the failures of the new system should be reviewed for new/additional failures that are not detectable and require periodic surveillance or additional application test functionality to provide detectability. If one or more failure modes of interest can be detected by the self-diagnostics of the digital equipment, then proceed to Step 2. Otherwise, if these failures cannot be detected, then proceed to Approach 3, where deconstruction of the surveillance test procedure into smaller subsets of functions of interest could lead to meeting the risk acceptance guidance in RG 1.174 without crediting self-diagnostics.
2. Add modeling to the plant PRA that credits the detection and recovery of the self-detected failures for use in the SFCP risk analysis. This modeling could consist of credit for manually recovering the failure by replacing the failed module or circuit card. The modeling should consider operator failure to perform the recovery adequately and the possibility that the self-diagnostics fail to detect and announce the failure. Human reliability analysis (HRA) of operator

actions to perform the recovery should provide results that lead to a significant increase in reliability for the failures that are detected and can be recovered particularly if plant procedures provide instructions to perform the recovery. The conditional probability that the self-diagnostics fail coincident with the failure that would normally be a detectable failure should be considered but, if the failures are independent from each other, the failure of the self-diagnostics are not likely to be a significant contributor to risk.

Failures that cannot be self-detected cannot, of course, be modeled as recoverable in the manner described above and therefore, must be separately treated as unrecovered failures. Fault overage by self-diagnostics can be expressed as percentage of coverage. Therefore, if the fault coverage of the self-diagnostics is medium (i.e., 90–99 % coverage), then 1–10% percent of the failure probability needs to be modeled as unrecoverable.

3. Reperform the SFCP risk analysis associated using the PRA plant model with credit for the detected and recovered failure using guidance from NEI 04-10 to redetermine the risk increase associated with the STI extension. If the risk increase associated with STI extension can be shown to be acceptably small, then proceed to Step 4; if not, proceed to Approach 3.
4. Determine the extent to which self-diagnostics can also be used to help fulfil the performance monitoring requirements of NEI 04-10, Step 18 (Monitoring and Feedback). As stated in Step 3 of Approach 1 above this determination consists of confirming that no failure mechanisms that are related to the revised surveillance frequencies become important enough to alter the failure rates assumed in the justification of program changes, and to ensure that adequate component capability (i.e., margin) is maintained. As part of this step, it is important to document the failure mechanisms related to the revised surveillance frequencies that can be reliably detected by the self-diagnostic methods.

   Self-diagnostics provide continuous real-time testing and may have the capability to detect incipient failures or degradation that has not yet resulted in a failure. Real-time data also presents the opportunity for real-time or near-term assessment of the data (e.g., trend analysis of incipient failures).

   As a part of Step 1 above, the determination of which failures modes cannot be detected by the self-diagnostics has already been performed. If there are important failure modes that can only be detected by surveillance tests, then that test information is needed to support the performance monitoring criteria required by NEI 04-10 for these failure modes.

Approach 3 is the case where the surveillance test procedure is divided into subparts and Approaches 1 or 2 are reapplied, but to a subset of the surveillance tests. This approach consists of the following steps and is illustrated in Figure 4Figure 4.

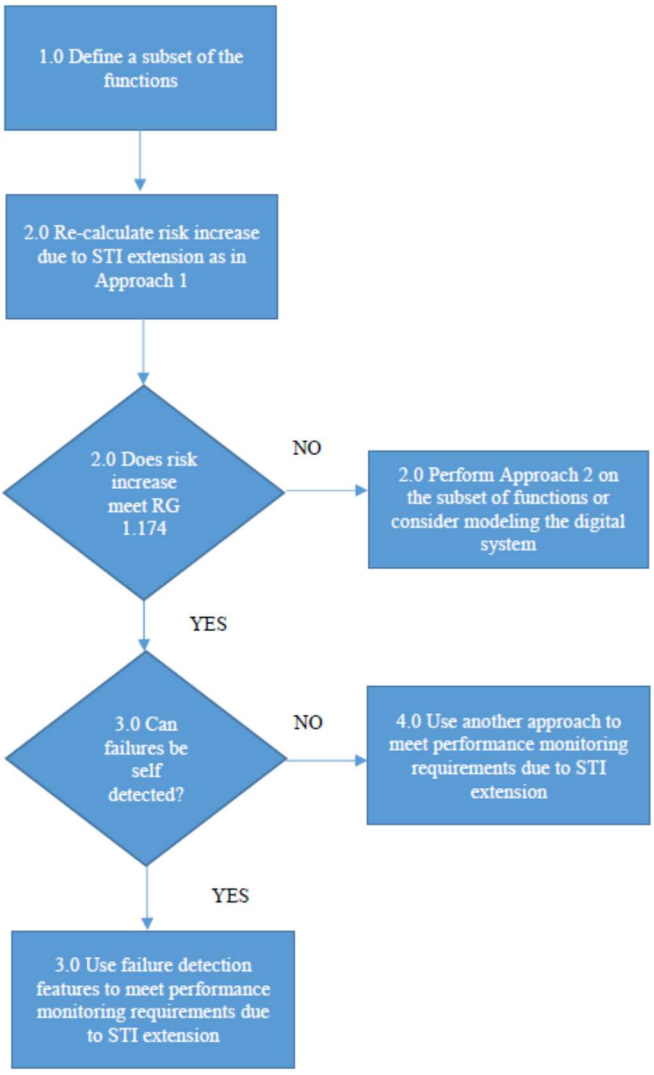

Figure 4. Approach Three: Surveillance test subdivided and Approach 1 and/or 2 reapplied.

1. Define a subset of the surveillance tests covered by the surveillance test procedure for which the plant has greatest interest in increasing the STI. The plant surveillance test procedures for performing the surveillance test can covers multiple tests, components, and functions. Therefore, the procedure is deconstructed with the objective of performing the STI extension only for the subset of functions covered by the surveillance test of most interest.[3]
2. Recalculate the risk increase associated with revised STI extensions using Approach 1 in which self-diagnostics is not credited for risk reduction. If the risk increase calculated in Approach 1 for the subset of the surveillance test defined in Step 1 is not shown to be acceptably small using the guidance in NEI 04-10 Step 12, then recalculate the risk increase associated with the revised STI extensions using Approach 2 in which self-diagnostics are not credited for risk reduction. If the

[3] As an example, and as discussed in the earlier sections, one of the primary tests of interest is the COT. Under Approach 3, the COTs portion of the test procedure could be considered separately from the other tests in the procedure and the STI extension risk analysis performed only for the COTs tests if Approach 3 is needed to show that risk acceptance guidelines are met.

risk increase calculated for the subset of surveillance test defined in Step 1 using Approach 1 is acceptably small, then go to Step 3.

3. Determine the extent to which self-diagnostics can also be used to help fulfill the performance monitoring requirements of NEI 04-10, Step 18 (Monitoring and Feedback). As described above, this determination consists of confirming that no failure mechanisms related to the revised surveillance frequencies become important enough to alter the failure rates assumed in the justification of program changes, as well as ensuring that adequate component capability (i.e., margin) is maintained. As part of this step, it is important to document the failure mechanisms related to the revised surveillance frequencies that can be reliably detected by the self-diagnostic methods. If there are important failure modes that can only be detected by surveillance tests, then the results of that test information are needed to support the performance monitoring criteria required by NEI 04-10 for this set of failures. This is generally addressed in an analysis document output in the form of a Failure Modes and Effects Diagnostics Analysis (FMEDA) to address all failure mechanisms and the detection and coverage needed to justify extension and elimination of the current surveillance specific test steps and frequency.
4. If self-diagnostics cannot be used to fulfill the performance monitoring requirement, then a more traditional approach may be needed that includes monitoring test surveillance results to ensure that the performance monitoring requirements of NEI 04-10 are fulfilled.

Modeling the digital I&C equipment could produce more refined approaches. Given the challenges of modeling digital I&C equipment, attention is needed to develop models of the digital I&C equipment that are acceptable to NRC. Open questions about the modeling that could impact an STI extension determination include the possibility that software CCF failures impact more than one I&C system or more than one function if the same digital platform is used for multiple functions. Also, given that different portions of I&C systems can operate in either a standby or a continuous operating mode, there remains a question about how to calculate increased failure probability based on the increased time between surveillance tests.

4. APPLICATION OF PROPOSED WORKFLOW: EXAMPLE

This section describes the underlying analyses necessary for fully crediting self-diagnostics and assessing the corresponding change in risk. The results from a specific use case examined using data provided by a utility partner from a specific digital system are also discussed. Given that the complete analysis requires access to some vendor-proprietary information that was not readily accessible, the assessments using the available data are necessarily limited. However, the analysis provides useful information relative to applying the proposed workflow and is summarized in this section.

4.1 CHANGE-IN-RISK AND DIAGNOSTIC COVERAGE FROM SELF-DIAGNOSTICS

Self-diagnostics provides a mechanism for rapid and reliable detection of some faults. The overall impact of these faults on plant risk may be taken to be very small (~zero) if the self-diagnostics function is reliable (low false calls, low missed detection).

For self-diagnostics to be viable for extending surveillance intervals, the self-diagnostics and OLM capabilities of the digital equipment must equal or surpass the TS requirements. Self-diagnostic tests can detect the same failures as would be detected by the channel check, COT, ALT, and Actuation Logic Output Test (ALOT) [2] surveillance tests but on an automatic and continuous basis. The self-diagnostics tests are automatically and continuously executed. This contrasts with the manual tests that are executed per the surveillance test program, which could be anywhere from every 92 days, 24 months, or complete elimination. Therefore, the self-diagnostics tests are executed more frequently than the manual tests.

A significant advantage to self-diagnostics is that in addition to being run continuously, the self-diagnostics tests do not reduce the redundancy of the safety system. The RPS remains at full system redundancy during the self-diagnostic tests, unlike the manual surveillance tests that require the system to be at less than full redundancy when a channel is taken out of service for testing. Because the surveillance tests are accomplished by an operator or maintenance crew, they also have a higher probability of a human error adversely impacting the operation of the safety system than the self-diagnostic tests that are inherently less prone to error. In addition, failures are identified and fixed quickly (typically within a day) and the system is returned to full operability so out of service time from detection to repair is significantly reduced.

The workflow for surveillance interval extension described in NEI-04-10 includes the use of risk assessments as a major element, with the suggested approach to crediting self-diagnostics discussed above. As discussed earlier, for a digital system, self-diagnostics may support Approaches 1 or 2, and the COT surveillance test is potentially separable if Approach 3 is required. The decision on the selected approach will be heavily dependent on the risk modeling methods used for the digital system and the change in risk due to the surveillance extension. Models of digital I&C that include self-diagnostics should reflect the fault-coverage of the diagnostic system by including faults that are not detectable using the self-diagnostic functionality.

Key to assessing the change in risk is determining the effectiveness of self-diagnostics. This may be assessed through diagnostic coverage, using mechanisms such as those provided in IEC 61508-6 [16].

A comprehensive discussion on diagnostic coverage is provided in Appendix A of this report. Annex C of IEC 61508-6 [16] provides an example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2 [17]. Technically, IEC-61508 addresses only hardware failures; the issue of performing similar analyses for software failure rates and systematics appears to still be an open question (Quinn et al [18] and IEEE Std 1633 [19] review potential software reliability assessment methods).

In general, diagnostic coverage refers to the fraction of failures that may be detected by the diagnostic test. Usually, these failures are categorized into dangerous and non-dangerous categories, based on the impact of the failures. The resulting assessment of diagnostic coverage can be partitioned into detectable and undetectable failures, in each of the two categories. Thus, failures can be

- Non-dangerous (safe), detectable (SD),
- Non-dangerous (safe), undetectable (SU),
- Dangerous, detectable (DD), and
- Non-dangerous, undetectable (DU).

Detected failures are in relation to hardware and software failures, or faults, which are not hidden because they announce themselves or are discovered through normal operation or through dedicated detection methods. Undetected failures are used for failures or faults that do not announce themselves when they occur and remain hidden until detected by some means (e.g., diagnostic tests, proof tests, operator intervention like physical inspection and manual tests). The repair of such failures can begin only after they have been revealed (revealed means that the failures or faults become evident due to being overt or as a result of being detected).

In IEC 61511, the term dangerous detected failures/faults (i.e., DD) are related to dangerous failures detected by diagnostic tests. Overt is used for failures or faults which announce themselves when they

occur (e.g., due to the change of state). The repair of such failures can begin as soon as they have occurred. When the detection is very fast (e.g., by diagnostic tests) then the detected failures or faults can be considered to be overt failures or faults. When the detection is not very fast (e.g., by proof tests) the detected failures or faults cannot be considered to be overt failures or faults when addressing safety integrity levels. A dangerous revealed failure can only be treated as a safe failure if effective compensating measures, automatic or manual, are taken in a short enough time to ensure the safety integrity requirements are met for the safety function.

In contrast, undetected, unrevealed, and covert failures are not detected or not revealed or not overt. In IEC 61511, the term "dangerous undetected failures/faults" is related to dangerous failures/faults not detected by diagnostic tests (i.e., DU). That is, these dangerous failures are undetected failures that are not detected by the automated diagnostics, operator intervention (for example, physical inspection and manual tests), or through normal operation.

A key part of the analysis in extending a test interval is then the expected increase in failure rates with a surveillance extension, with self-diagnostic testing credited, which are calculated as specific probability of failure of demand (PFD), per IEEE-352 and IEEE-577. The failure rates are important because if the failure is undetected, then its probability of failure, assuming a constant failure rate as a conservative bounding condition, increases as the surveillance interval increases. The greater the diagnostic coverage, the smaller the probability of undetected failures. Thus, the probability of failure on demand is approximated by

$$p = \lambda \, t_{test}/2 \, ,$$

where λ is the time-related standby failure rate, and t_{test} is the time interval between tests. The same linear increase can be expected for those failures that are undetected by diagnostics but are detected by surveillance (end-to-end) tests. Increasing the surveillance interval from 6 m (t/2 = 3) to 12 m (t/2 = 6) results in an increase in the failure probability for an additional 3 m (assuming that the failure occurs half-way through the interval). Thus, in this example the increase in probability of failure on demand for a dangerous, undetected failure is $\Delta p = 3 \, \lambda_{DU}$.

Given that STI extension impacts only the time-related standby failure rate, one way to reduce the risk increase associated with an STI extension is to refine the definition of failures that are counted as time-related standby failure for digital systems. (As stated in NUREG/CR-6141 [20], standby failures are normally associated with corrosion, erosion, and wear, which are less dominant failure mechanisms for digital equipment than they are for other equipment.)

Self-diagnostics are used to ensure that failures are detected; however, self-diagnostic coverage could never be 100%, similar to testing that could never be 100% coverage, because of the unknown unknowns and not knowing all of the failure modes. Because of these unknowns, their potential failure mechanisms or phenomena are not reflected in either the PRA or traditional engineering analyses. Nevertheless, the greater the knowledge and history of a component could provide a means to provide a graded review by accepting the diagnostic coverage and the confidence in that coverage.

Diagnostics are used to detect both safe and dangerous failures. The diagnostic coverage (DC) is used to indicate the fraction of failures detected by diagnostics. The dangerous undetected failure rate is strongly impacted by the diagnostic coverage provided for random hardware failures. Comprehensive diagnostics dramatically improve the diagnostic coverage, thereby reducing the possibility of a dangerous undetected failure (i.e., DU). Because it can be difficult to conclusively prove that the self-diagnostics can provide a certain level of diagnostic coverage, it is necessary to make a conservative assumption about the percentage of failures that the self-diagnostics can identify.

IEC 61508-2 [17] provides levels of diagnostic coverage and designates diagnostic coverage as low (60%), medium (90%), and high (99%). Utility assessments from operational history appear to indicate levels of failure detection that are consistent with the IEC standards and vendors' assessments of diagnostics.

The 90% confidence interval of a failure rate λ is the interval [$\lambda_{5\%}$, $\lambda_{95\%}$] in which its actual value has a probability of 90% to belong to; λ has a probability of 5% to be better than $\lambda_{5\%}$ and worse than $\lambda_{95\%}$. On a purely statistical basis, the average of the failure rate may be estimated by using the "maximum likelihood estimate" and the confidence bounds ($\lambda_{5\%}$, $\lambda_{95\%}$) may be calculated by using the χ^2 function. The accuracy depends on the cumulated observation time and the number of failures observed.

The converse of diagnostic coverage of 90%, 95%, and 99% equates to 10%, 5%, and 1% of the failures being undetected. Accounting for diagnostic coverage would mean that $\lambda_{DU} = 0.1\ \lambda$ (or $0.05\ \lambda$ or $0.01\ \lambda$ depending on the diagnostic coverage level). For the example discussed earlier (Eagle-21), a detailed coverage evaluation would be needed to demonstrate that the self-diagnostics provide the same level of surveillance test coverage as required by the existing system and that there are no gaps in coverage. This coverage evaluation may require supporting proprietary information from the failure modes and effects analysis (FMEA) of the selected digital system. Although propriety information may be necessary to determine that there are no nondetectable failures, it could be logically assumed that the FMEAs did not identify any failures or eliminated them as required during the design phase (per IEEE-379). In lieu of the card-level FMEAs, an alternate method would be to evaluate the current COT testing being performed with respect to the self-diagnostic testing for coverage.

For the existing surveillance coverage based upon standard generic TS (NUREG 1431 [21, 22], an evaluation is needed to define the purpose of each surveillance test. Note that for Westinghouse plants, the surveillance testing is divided into several overlapping tests—sensors, logic solvers, instrument racks, voting logic (SSPS), and the final actuation devices—due to physical limitations or associated risks while the reactor is operating.

The coverage evaluation should utilize the plant TS-specific surveillance testing definitions, which can vary between plants. These implementation requirements can be used to evaluate any new system and provide guidance about how existing surveillance tests can be performed for the new system.

For new digital system upgrades, using FMEAs or FMEDAs is recommended for evaluating self-diagnostics test features and coverage. These analysis methods can be performed to determine which failures are and are not covered by the self-diagnostic testing. Additional automated testing can be added to the system if gaps are identified from the analysis.

It should be noted that system upgrades will also require a failure analysis for the identification of nondetectable failure modes; this consideration is outside of the scope of this research but is discussed for completeness. New digital systems may have new internal failure mechanisms that the existing system lacks. Supporting failure analysis of the digital system for these failure mechanisms is required to ensure that the self-diagnostics provide coverage for any new failure mechanisms. A FMEA or FMEDA is a recommended method of performing this analysis.

Potential new requirements associated with the use of self-diagnostics are as follows.

1) The self-diagnostics credited for surveillance testing elimination must receive periodic surveillance or analysis supporting that self-diagnostic failures are self-revealing. An alternative

to this is if the PRA importance analysis (e.g., Fussell–Vesely) demonstrates that the self-diagnostic testing is not risk significant, then no periodic testing of the tester would be required.

2) To address software failures, digital safety system software should be developed under a structured software quality assurance (SQA) development process along with rigorous verification and validation; the software should not fail or wear out over time. All software can have flaws/bugs, but these flaws must not be fatal/dangerous, and they also must have triggers to initiate those flaws. The operational history and surveillance testing results are beneficial in identifying software flaws. Changes to the software must also be controlled under plant configuration control. Administrative procedures should be in place to ensure that software versions are correct.
3) Digital system setpoints and parameter settings must be under configuration change control and periodic verification to confirm that they have not been changed. This could be performed by administrative procedures during outages, or they could be automated using software comparison tools.
4) Upon detection of a fatal/dangerous fault by the self-diagnostics, the system should be placed in a safe state or a predefined preferred state with alarming. Where an all-encompassing safe state cannot be defined by required multiple operational modes, the system should be placed in a preferred state with alarming and adequate time to support correction of the failure. Non-dangerous faults can be designed to alarm only if timely repair is required by TS, supporting PRA analysis, etc.

Self-diagnostic testing should address off normal conditions, not just failures, such as slow response times (i.e., adequate cyclic response time).

4.2 METHODOLOGY FOR REPLACING DETERMINISTIC ANALYSIS WITH SELF-DIAGNOSTICS

Besides the use of diagnostic coverage, failure rate calculations, and risk estimates, NEI 04-10 also requires a *qualitative* review of information and procedures relevant to surveillance interval extension. Such assessments might include, for instance, operational experience with the system, surveillance test history, reliability review, unavailability review, industry and plant experience, vendor-specified maintenance frequency, code specified test intervals, impact on defense-in-depth protection, impact on systems not quantified in the PRA, uncertainty associated with the quantitative process, and other qualitative considerations. The fundamental reason for including this type of assessment is to ensure that the system has historically been reliable and may be expected to continue to operate reliably with no measurable increase in failure rates. This has been addressed in an analysis document output in the form of an FMEDA to address all failure mechanisms and the detection and coverage needed to justify extension and elimination of the current surveillance specific test steps and frequency.

A specific step that is used to demonstrate the reliability of the system is drift analysis (Appendix B). There are two separate results that are calculated and used to assess the acceptability of extending the calibration interval using as-found, as-left (AF-AL) data. The first evaluation calculates the drift of the specific instruments in scope over the data recovery period and compares the results to existing acceptance criteria. The second evaluation calculates the drift over multiple calibration intervals eliminating any effect of intermediate adjustments to the trip units. The methods used to determine the characteristics of the drift following NEI 04-10 Rev 1 and the associated reference are documented in Appendix B. These methods are consistent with acceptable industry practices [23, 24]. There are two separate results that are calculated and used to assess the acceptability of extending the calibration interval using AF-AL data. The first evaluation calculates the drift of the specific instruments in scope over the data recovery period and compares the results to existing acceptance criteria. The second

evaluation calculates the drift for time dependency over multiple calibration intervals eliminating any effect of intermediate adjustments to the trip units. Note that if adjustments are made over several intervals, the data for a trend of multiple changes is examined in only one direction. Otherwise, this could result in an unplanned replacement if an adjustment can be made instead (i.e., out of pot adjustment). Self-diagnostics may also be applicable to replace or enhance drift analysis as part of the NEI 04-10 Step 7, "Identify Qualitative Considerations to be Addressed."

Most of today's digital systems have continuous self-calibration of input A/D inputs to a precision reference source that self-corrects within limits for changes that would classify as instrument drift due to subcomponent changes. For protection systems, once the analog signal is converted to digital, drift is no longer an issue with respect to safety related bistable functions (trips and actuations) that remain digital through the output. In addition, some digital systems (e.g., Triconex) perform comparison checks of the digitized signal and will self-identify out of tolerance (OOT) conditions via alarms and bypass the OOT input or placing the system in a safe state. RPS can perform cross-division communications that provide comparisons that are not only for the logic solver but includes the cross divisional checks of the independent sensors; however, this adds complexity to the RPS. For Setpoints, the setpoint voltages inputting into the electronic comparators in analog systems are now digital data and can longer drift due to subcomponent changes. For safety related outputs such as indicators and controls, digital-to-analog (D/A) conversion drift that can be addressed by 95/95 probability and confidence level drift analysis and inclusion in the associated setpoint and uncertainty calculations.

For digital systems that self-calibrate without cross divisional checks, drift of the precision reference is a potential source of drift that would require further evaluation and justification. This could be in the form of a drift analysis or an evaluation of the design. Another possibility is that digital systems have the ability to provide internal data points that could be digitally transmitted to an external non-safety monitoring system (i.e., a digital control system or plant computer system) for comparison between redundant divisions notifications of out of tolerance conditions (NRC NUREG 0800 BTP 7-17 includes additional guidance), and OLM of the logic solver for drift. Due to the increased precision of today's logic solvers, a monitoring system can also be used to monitor both the sensors and logic solvers for drift using OLM techniques. More information on OLM implementation may be found in AMS Topical Reports 1) Submittal of Analysis and Measurement Services Corporation Topical Report Monitoring Technology to Extend Calibration Intervals of Nuclear Plant Pressure Transmitters, AMS-TR-0720R0, dated August,18,2020 (ADAMS Package Accession No. ML20231A208); 2. Re-Submittal of Analysis and Measurement Services Corporation Topical Report Monitoring Technology to Extend Calibration Intervals of Nuclear Plant Pressure Transmitters, AMS-TR-0720R1, dated November 12, 2020 (ADAMS Package Accession No. ML20317A111); and 3) NRC Safety Evaluation[4].

Given these available capabilities of self-diagnostics and the potential for additional monitoring systems that can monitor both sensors and logic solvers for drift, a case can be made that drift analysis supporting the NEI 04-10 performance process could be eliminated based upon the self-diagnostics that provide adequate coverage for detection of internal failures. As with the diagnostic coverage assessment and change-in-risk calculations, a detailed assessment of the digital system performance data and self-diagnostic performance will be needed before drift analysis can be eliminated as part of the SFCP process.

[4] https://www.nrc.gov/docs/ML2117/ML21179A062.pdf

4.3 EXAMPLE

4.3.1 Available Data

Given the proprietary nature of the data, a detailed description of the information is not included in this document. Information that was made available to the project team for review included risk-informed surveillance documentation for surveillance tests and digital equipment performance data. The surveillance documentation included the surveillance test risk-informed documented evaluation (STRIDE) reports and the other consisted of the corresponding test interval change risk assessment.

The STRIDE packages are designed to support extension of conventional surveillance requirement test intervals, in accordance with "Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies, Industry Guideline," NEI 04-10, Revision 1 [4]. The work elements associated with STRIDE development includes PRA case studies, deterministic assessment (DA) evaluations, and, where required, instrument drift evaluation (IDE). Development of the STRIDE packages include the support of independent decision-making panel (IDP) meetings at the implementing power stations and trained IDP member participation.

STRIDE reports reviewed by the project team were for COT surveillances, which are one of the types of tests considered appropriate for STI when crediting self-diagnostics as failures are addressed by the diagnostic module of the selected digital system. In the surveillance test section of these reports, all applicable surveillance test procedures are identified, the TS surveillance requirement bases are presented and discussed for each test, the components exercised by surveillance requirements are identified, and the pros and cons of the STI extension are discussed. In the Maintenance Rule section, the report identifies the maintenance rule functions that would be impacted by the STI extension. The NRC Maintenance Rule (10 CFR 50.65) requires all safety equipment (and some nonsafety related equipment) to be included in the monitoring program scope, so plant owners and the NRC can make better informed decisions about the effectiveness of maintenance activities and, more importantly, about the reliability of the safety equipment being maintained. Given that the STI is being extended, heightened attention will be given to equipment that do not meet applicable performance criteria. In the engineering evaluation section of the STRIDE package, (1) NRC commitments are reviewed (e.g., commitments in the TS bases and Final Safety Analysis Report), (2) the history of the surveillance test is reviewed, (3) the operational and maintenance history of components and systems associated with the STI extension are reviewed, (4) past industry and plant experience with functions affected by the proposed STI extension are reviewed, (5) vendor-specified maintenance frequency documentation is reviewed for test frequency impact, (6) any STIs specified in appliable industry codes and standards are reviewed, (7) other qualitative engineering factors are considered such as whether any of the components operate in a harsh environment, whether there are common cause failure implications, and whether alternative testing exists that would be affected by the change, (8) qualitative engineering analysis that make conclusions about any challenges to the STI extension is provided, (9) proposed phased implementation recommendations are provided, and (10) the proposed performance monitoring plan is provided. The section on risk analysis using PRA, provides (1) identification of the PRA types (e.g., internal events, internal flooding, internal fire, seismic events, other external hazards, and low power shutdown) used to determine the risk change associated with the STI extension, (2) the risk results of the PRAs, (3) pending PRA model changes, (4) discussion of any open independent peer review findings, (5) the total effect of the STI extension from all PRAs, (6) the cumulative effect of all STI extensions (which has a different quantitative threshold than individual STI extensions), (7) impact on the impact of defense-in-depth philosophies, and (8) the risk conclusion using PRA.

The detailed risk analysis using PRA is usually documented in a separate report, focused on the STI change risk assessment generated to document the risk analysis using PRA performed to evaluate the

acceptability of extending the associated STIs. It encompasses (1) evaluation of modeling assumptions and sources of uncertainty and unit differences and their impact on the risk change calculations, (2) description of types of PRAs contributing to the overall risk impact of STI changes, (3) detailed modeling discussions such as explanation about how the modeling changes are made in the PRAs needed to reflect the test frequency changes, and (4) the risk contribution results from the applicable PRAs. The discussion of the PRA types contributing to the overall risk impact of STI include discussion of the impact of any outstanding finding from independent peer reviews required by NRC in Regulatory Guide (RG) 1.200, Revision 3, "Acceptability of Probabilistic Risk Assessment Results for Risk Informed Activities" [5] against the currently NRC endorsed PRA standard [25]. This risk analysis report ends with a conclusion about the risk impact of the STI extension.

As discussed earlier, a key element of the risk analysis is the diagnostic coverage and the failure rate assessment for the components relevant to the surveillance test under consideration. Data reviewed by the project team included a summary of events as well as a description of these events. Of particular importance to this analysis was the included description, that included analysis by the plant of the sequence of events that occurred, and crucially, an indication of whether occurrences were detected by surveillance tests, self-detection, or operational awareness. Such data can provide an estimate of failure rates of relevant components of the digital system. It however does not allow an assessment of diagnostic coverage.

4.3.2 Analysis

4.3.2.1 Change in Risk

This section provides an evaluation of the material reviewed by the project team to exercise the proposed process of trying to credit the self-diagnostic features of digital I&C to TS STI extension. Accordingly, the focus of the analysis in this section this section is on the specific surveillance tests documented in the reviewed STRIDE documentation. Where available, publicly available information on risk sensitivity was also used to supplement the utility provided information.

The primary conclusion of the two STRIDE packages reviewed is that for the functions in the surveillance test that addressed the STI extension has negligible impact on core damage frequency (CDF) or large early release fraction (LERF). The reported CDF for all TS surveillance test extensions evaluated were negligible (less than ~1E-08 per year) and addressed not only internal events but included flooding and internal fire. In all cases, the proposed STI extension was from 184 days to 18 months. All other values (e.g., from other hazards and for LERF) were reported as negligible. These values are so low that they are not counted against the cumulative CDF for the risk-informed SFCP. The engineering evaluation described in the two STRIDE reports did not identify any technical issues that would call these quantitative risk results into dispute. As discussed earlier, as part of the engineering evaluation staff reviews licensing commitments, the surveillance test, operational and maintenance history, industry and plant experience of associated components/systems, applicable plant functions, applicable vendor-specified and code requirements, and other engineering factors such as whether any of the components operate in a harsh environment.

There is additional evidence of the risk insensitivity to failures in the plant's TSTF 505 safety evaluation (SE) to extend allowed outage times (AOTs) in which the function and modeling of the digital system was examined in detail. The modeling included consideration of CCF events, though CCF failure across multiple channels and functions due to software function was not seen to be credible. The SE for that license amendment request (LAR) states that the NRC staff concluded that modeling of the digital system in the TSTF-505 application was appropriate, and changes in failure probabilities of surrogate events were shown to have an inconsequential impact on the Risk Informed Completion Times (RICT)

calculations for relevant representative TS Limiting Conditions of Operation (LCO) conditions. Results of an importance analysis using Risk Achievement Worth (RAW), computed by the licensee, also show the general risk insensitivity to failure of the digital system (low RAW values, in the vicinity of 1.0). The calculation of RAW is determined by the ratio for CDF/LERF when the basic event(s) of interest are assumed to be failed (i.e., are set to 1.0) divided by the nominal CDF/LERF. In other words, zero credit is given for the component(s) of interest.

A more detailed review of the available information indicated that the PRA modeling of the digital system was assumed to have the same structure as fault tree modeling for an equivalent analog system but populated with digital system failure rates. It appears, however, based on statements in the SE that fault tree modeling issues such as the possibility of CCF were evaluated by NRC, and, despite the simplified modeling, NRC found it sufficient for the allowed outage risk-informed application, based on sensitivity studies, importance analysis, and evaluation for CCF. This includes a conclusion that the LCP cannot cause CCF because it performs separate calculations for different functions and the CCF analysis was performed across the digital system cards.

The conclusion of the discussion above concerning the risk significance of the digital system selected for this case study is that failures of the digital system are not risk significant, and STI extension of COTs tests have negligible impact on risk based on (1) the conclusion of the STRIDE packages for specific COTs tests and (2) the general importance calculation showing that complete failure of the system has only a marginal impact on CDF and LERF. This appears to be a reasonable conclusion given (1) the diversity of signals, (2) the fact that the anticipated accident without scram (ATWS) Mitigation Actuation System (AMSAC) is designed to mitigate ATWS events is a backup to RTS, and (3) the fact that failure of trips can be mitigated by operator action in the main control room.

Given that the analyses show that failures of the selected digital system have a negligible impact on the risk increase associated with STI extension and that, in general, failures have a low impact on CDF and LERF, the applicable approach from Section 3 for crediting self-diagnostics is Approach 1. In this case, following the process listed in Approach 1, self-diagnostics may be able to provide the necessary monitoring function. However, crediting self-diagnostics for the monitoring function will require that the diagnostic function be capable of detecting relevant failures. This is discussed below.

4.3.2.2 Failure Data Analysis

A review of reported reliability data provided by the utility indicated that over 90% of failures were either self-detected or detected by operational awareness. A review of the data indicated that the self-diagnostic function appeared to be capable of detecting failures in relevant components (boards) a significant fraction of the time. While this indicates a high detection rate for the self-diagnostic component, it is difficult to estimate the diagnostic coverage, given the proprietary nature of information on the system design. However, the diagnostic performance appears to indicate an ability to use the self-diagnostic capabilities of the digital system to detect failures of relevant components in the digital system. Indeed, a review of the STRIDE documentation also showed that a detailed utility review did not find any cases of failure of the components of interest that were not detected by the self-diagnostic function of the digital system. This appears to be consistent with the IEC standards and vendors' assessments of diagnostics.

A specific aspect of monitoring is the ability to detect signal drift, and a review of the data focused on drift-related events. While 10 events were identified where it appeared that a drift had occurred, most (7) of these occurrences appeared to be associated with a device used for functional testing of the system rather than transmitter drift. The project team understand this to mean that the drift was not associated with reactor I&C but rather instrumentation used in surveillance testing.

Eliminating these seven drift occurrences from the analysis showed three remaining cases that were all identified by the self-diagnostic capability of the digital system. While this is not necessarily evidence of the capability to detect all drift events associated with the selected surveillances, a review of the STRIDE documentation also demonstrated that no measurable drift was identified over the 5-year period covered by the STRIDEs.

NUREG/CR-6823 [26] recommends using the Jeffreys noninformative prior to develop a mean likelihood when there is insufficient information to develop a distribution based on prior information or, in this case, insufficient failure data information of digital I&C systems employed on active NPP safety systems and zero failure event that went undetected and were not resolved. The Jeffreys noninformative prior is intended to convey little prior belief or information, thus allowing the data to speak for itself. The mean of the Jeffreys distribution (L_{fh}) is calculated as follows:

$$L_{fh} = (x + ½) / t$$

where

x = number of events
t = time over which the events occurred

Based on the above discussion, $x = 0$ (there are zero signal drift events that went undetected and unrecovered). Using the appropriate operational time for the plant, the L_{fh} was estimated to be less than 1E-06 undetected and unrecovered drift events per reactor-hour. Accordingly, based on the data it appears extremely unlikely that signal drift event will go undetected and unrecovered.

Collectively, these data indicate the following. (1) There were very few (three) potential drift events over the lifetime of the digital system at the facility. (2) These drift events were self-diagnosed by the system and provided a prompt for maintenance intervention. (3) Failures relevant to the selected surveillances were self-detected by the digital system. As a result, the continuous on-line calibration of the analog signals appeared to work almost flawlessly over the lifetime of the digital system.

4.3.2.3 Application of the Proposed Process

As described above in Section 3, the process proposed by the team consists of three different approaches and of which can provide value to the STI extension process depending on the circumstances. Approach 1 is the case where self-diagnostics is not needed to show sufficiently low risk after STI extension but might be credited for performance monitoring as applicable. Approach 2 is the case where self-diagnostics is needed to show sufficiently low risk after STI extension reduction and might also be credited for performance monitoring. Approach 3 is a combination of Approach 1 or 2 and the need to subdivide the tests if possible and practical. Clearly, the applicable approach in the selected use case is Approach 1 because the STRIDE reports and PRA sensitivity studies and importance analyses as discussed above show that the digital system failures have a negligible impact on the risk increase associated with STI extension and that, in general, the digital system failures have a low impact on CDF and LERF.

In addition to *quantitative* analysis, NEI-04-10 also requires a *qualitative* review of information relevant to surveillance interval extension which are largely addressed by the engineering evaluation performed for a STRIDE package as discussed above. The purpose of this requirement is to ensure that the system has historically been reliable and may be expected to continue to operate reliably with no increase in failure rates. A specific step applicable to I&C systems to support demonstration of the reliability of the system is drift analysis (see description in Appendix B). One drift assessment evaluation calculates the

drift of the specific instruments in scope over the data recovery period and compares the results to existing acceptance criteria. Another drift assessment evaluation calculates the drift over multiple calibration intervals to eliminate any effects of intermediate adjustments to the trip units. These approaches to signal drift evaluations are consistent with acceptable industry practices as described above. It is proposed that, in this case, the self-diagnostics is sufficient to replace the signal drift evaluation directed in NEI 4-10 Step 7, "Identify Qualitative Considerations to be Addressed".

Step 15 of the NEI 04-10 procedure stipulates that qualitative and quantitative assessment (defined in prior steps of the procedure) be summarized and established monitoring recommendations be provided to the IDP. The IDP is comprised on the Maintenance Rule Expert Panel, a Surveillance Test Coordinator, and a Subject Matter Expert (SME). Monitoring drift is provided by the digital system in this case, as the digital system prevents signal drift. This feature precludes the need for the drift evaluations that is typically performed for a STRIDE package for applicable systems. Explanation to the IDP about the continued positive track record of the digital system in preventing and detecting drift would help inform their decision making.

Application of the proposed process would lead to elimination of drift evaluations from a STRIDE package for which the surveillance tests of digital I&C system that has features which continually checks and calibrates for drift and detects drift related failures.

While the ability to directly credit self-diagnostics in the risk analysis was not able to be evaluated using the specific examples of surveillances for the selected digital system, the review of provided information indicated a potential path to evaluating and demonstrating Approach 2. Specifically, Approach 2 is triggered when the estimated change in risk does not meet the guidance described in RG 1.174. In this case, the available data seem to indicate that the detection of relevant failures was possible using a combination of self-diagnostics and situational awareness. However, crediting recovery from these failures is likely to require knowledge of the diagnostic coverage. It is clear that drift, at least, is extremely unlikely to be missed (based on reported data) and therefore, a timely recovery from this event may be credited during the risk calculations. Similar analyses for other failure modes will be necessary as part of Approach 2 and can be evaluated in specific systems that may have a greater contribution to the overall plant risk than the selected digital system.

4.4 DISCUSSION AND RECOMMENDATIONS

A specific digital platform was identified in consultation with an industry partner as a potential candidate for the pilot-scale evaluation of the methods identified herein. Based on the available information and data reviewed to date, the following observations can be made.

- Self-diagnostics can be used effectively as part of the monitoring function in the proposed STI framework and can be included in the basis for eliminating drift evaluations in digital equipment STI extension. As described previously, the basis for eliminating drift evaluations in digital I&C STI extension is as follows. (1) The selected digital system has features that continually evaluates and calibrates signal drift and detects drift-related failures. (2) Evaluation of the history of operational drift–related failures for the plant shows that continuous on-line calibration of the analog signals appears to have worked almost perfectly over the lifetime of the digital system, and—in the rare case that drift events did occur—the system generated a prompt for operators to investigate drift which resulted in identification, evaluation, and resolution by plant staff. (3) digital system failures have low impact on risk even if they do occur even if drift occurred on a single channel or even on multiple channels of the same function, the impact would be negligible on CDF and LERF.

- Crediting self-diagnostics for recovery from system failures appears to be a possibility based on the reported failure detection rates. However, a complete evaluation will require selecting a different digital system that has a greater contribution to the overall plant risk, as well as information on the diagnostic coverage of the self-diagnostic functions.

These findings to date inform the recommendations identified below.

- Drift detection and correction function of digital systems should be further evaluated to confirm that self-diagnostics may be used in lieu of drift evaluations in existing STI extensions.
- Improved PRA models that account for digital I&C systems, including the self-diagnostic function, should be explored [15]. In particular, identification of better models would assist with incorporating failure rates that account for the diagnostic function and/or drift elimination functions that are provided by modern digital equipment. It should be noted that the complexity of modern digital I&C systems necessitates extensive evaluation of the opportunity for failure, including CCF.

These findings also highlight the following data needs.

- PRA information on how the digital system is modeled. This should include information that is commonly found in a plant's PRA System Notebook such as a description of the system, the system and component failure rates used, the modeling assumptions, testing, and, if possible, the fault tree modeling. Though digital systems increase reliability over their analog counterparts, the complexity of system and PRA modeling is increased and introduces data needs on failure mode and effects analyses, availability of detailed hardware and software failure data, the interaction of internal system diagnostics on system availability, impacts of environmental conditions and potential CCF [27].
- Surveillance frequency extension information. Specifically, information/data on drift if self-diagnostics is not credited and failure of the equipment as well as the specific surveillance tests that are candidates for this extension will be needed.
    - Plant specific information on the digital system and component failures that were detected using self-diagnostics and failures that were detected using surveillance, with an additional category to capture all other failure detection methods such as operator channel checks.
    - Any existing evaluation of that data and any comparisons to failure data from other plants or comparison to failure data for analog systems.
    - Diagnostic coverage, i.e., relevant failure modes addressed by the surveillance test and the modes covered by the self-diagnostic function. This helps determine if additional tests might be necessary after the diagnostic coverage is credited for surveillance extension.
- Any information that is utility-owned or available through Owners Groups and related to the specifications and reliability of the selected system. Some information on reliability may be available publicly and may be used to supplement utility-owned information. Specific data might include:
    - System failures modes and reliability developed during design and/or installation.
    - System design regarding failure modes that can be self-identified versus those that must be test-identified.

Though it would be useful to also have data on the digital platform FMEA and self-diagnostics capability information, such information is generally proprietary to the vendor and difficult to obtain. Assessments based on public information (such as the discussion for the example digital system in Section 2) are not intended to, and do not, answer the question of the underlying reliability of the digital system.

It is worth noting that surveillance intervals being considered in this project are generally under a licensee SFCP program. Generally, an approved LAR is used to move the surveillance intervals to licensee SFCP control (10CFR50.90). In these circumstances, the surveillance test is still a TS-required test, but the surveillance interval is under licensee control. The process used by licensees under SFCP for interval extension has been previously approved by NRC through an SE of the TSTF-425 program; thus, the changes to STI under the licensee SFCP do not require a LAR but can be modified under 10CFR50.59. The initial LAR to move the surveillance intervals to licensee SFCP typically requires an analysis of the incremental risk and failure modes; such an analysis is often carried out by the system vendor and documented in technical reports that are evaluated by the regulator. Thus, although the information on FMEA and diagnostic coverage may be proprietary to the vendor, it is reasonable to assume that diagnostic coverage is likely to be very high and failure modes not covered by either self-diagnostics or periodic surveillance tests have been designed out of the system. It should be noted that the LAR process may also provide opportunities to also eliminate some TS surveillance requirements in lieu of SCFP.

5. SUMMARY AND FUTURE PLANS

A pilot study was conducted in collaboration with a utility partner to test the proposed approach for extending TS STIs for digital equipment used in commercial NPPs. Moreover, this work aimed to use the results of the pilot study to refine the workflow and quantify the benefits that might be realized by the proposed approaches. The use case of specific surveillance tests of interest for test interval extension focused on TS-required channel operability tests. To better validate the work, the team selected a reference digital system for this study, identified in consultation with a utility partner.

The study's workflow began with the selection of relevant surveillance tests such as COTs, ALTs and Channel Checks. The next step considered self-diagnostic coverage options related to surveillance test coverage. With limited ability to access vendor proprietary data, the analysis in this effort assumed a high coverage; failure modes not covered by either self-diagnostics or periodic surveillance tests were not considered in the system.

Extending the surveillance test interval without a drift evaluation will require verifying that failure mechanisms that could adversely affect the safety function of the specific system components identified as part of the surveillance interval extension can be detected using diagnostics. Recognizing that digital components do not have drift, the components that must be evaluated are in the input conversion from A/D conversions and any output conversions. These analyses are currently performed at a 95/95 probability and confidence level following NEI 04-10 Rev 1 and ISA S67.04-2018. Self-diagnostics provide a potential mechanism for eliminating these drift analyses if the diagnostic coverage is applicable to the relevant components.

Reviews of utility provided information indicated that self-diagnostics may be used as part of the monitoring function in the proposed STI framework and as a part of the basis for eliminating drift evaluations in digital equipment STI extension. Crediting self-diagnostics for identification of system failures appears to be a possibility based on the reported failure detection rates and the description of failure events that involved alarms or other indicators that cued a response from staff to investigate, identify, and fix a problem without shutting the plant down. However, this capability must be confirmed by evaluations of other digital systems.

The pilot study has indicated that although the proposed methodology may be applied for crediting self-diagnostics, additional evaluations using alternate digital systems are necessary to fully demonstrate the value proposition of the methodology. Specific recommendations include the following: (1) the drift detection and correction function of digital systems should be further evaluated to confirm that self-

diagnostics may be used in lieu of drift evaluations in existing STI extensions; and (2) value of improved PRA models must be explored. In addition, specific data compilation recommendations were identified through this effort.

Additional insights may be obtained through a continued assessment using data from other digital systems. Examples of potential insights—particularly for a system with greater risk significance than the system evaluated in the pilot study—include determining (1) the dominant risk contributions that impact the risk increase calculation, (2) whether more information or specificity about the self-diagnostics and fault coverage could reduce risk, (3) the impact of reduced likelihood of undetectable failures on risk reduction, and (4) the impact of CCFs across digital instrumentation and control functions on the risk increase. Ultimately, the use of self-diagnostics in this manner may provide additional benefits, such as reducing the likelihood of undetectable failures by ensuring completeness on diagnostic coverage, as well as identifying and reducing the likelihood of previously low-probability failure modes as a result of surveillance extension.

6. REFERENCES

1. Coles, G.A., et al. *Technical Specifications Surveillance Interval Extension of Digital Equipment in Nuclear Power Plants: Methods and Implementation Strategy. Idaho National Laboratory*. INL/EXT-19-55342 Rev. 0. 2019.
2. Quinn, E., et al. *Technical Specification Surveillance Interval Extension of Digital Equipment in Nuclear Power Plants: Review, Research, and Recommendations. Idaho National Laboratory*. INL-EXT-19-54251 Rev. 0. 2019.
3. Industry/Technical Specification Task Force (TSTF) Traveler, TSTF–425, Rev. 3, ‘‘Relocate Surveillance Frequencies to Licensee Control—RITSTF Initiative 5b,” March 18, 2009. [NRC ADAMS Accession Number ML090850642]
4. NEI 04-10 Rev. 1, Risk-Informed Technical Specifications Initiative 5b, Risk-Informed Method for Control of Surveillance Frequencies. NEI, 2007. [NRC ADAMS Accession No. ML071360456]
5. Regulatory Guide 1.200, Rev. 3, “An Approach for Determining the Technical Adequacy of Probabilistic Risk Assessment [PRA] Results for Risk-Informed Activities,” US NRC, December 2020. [ADAMS Accession No. ML20238B871]
6. S. A. Eide, et. al., *Reliability Study: Westinghouse Reactor Protection System, 1984–1995*, NUREG/CR-5500, Vol. 2, December 1998.
7. Westinghouse Topical Report, *Eagle-21 Microprocessor-Based Process Protection System*, January. 1987. [NRC ADAMS Accession No. ML082280218]
8. D. V. Lockridge, G. R. Andre, R. L. Haessler, J. D. Andrachek, and R. M. Span, "Risk-Informed Assessment of the RTS and ESFAS Surveillance Test Intervals and Reactor Trip Breaker Test and Completion Times," WCAP-15377-NP-A, Westinghouse, Pittsburgh, PA (2003).
9. Tennessee Valley Authority. Sequoyah Nuclear Plant Updated Final Safety Analysis Report, Amendment 16.
10. International Atomic Energy Agency (IAEA), "Component reliability data for use in probabilistic safety assessment," IAEA-TECDOC-478 (1988).
11. NUREG-0847, Supplement 13, *Safety Evaluation Report Related to the Operation of Watts Bar Nuclear Plant, Units 1 and 2*, April 1994. (NRC ADAMS Accession No. ML072060484)
12. Tennessee Valley Authority (TVA), Letter from Barstow, James, to NRC*, Supplement to License Amendment Request to Revise Technical Specifications to Adopt Risk-Informed Completion Times TSTF-505, Revision 2, “Provide Risk-Informed Extended Completion Times – RITSTF Initiative 4b” (SQN-TS-20-03) EPID L-2021-LLA-0145”,* dated April 28, 2022, TVA, Chattanooga, TN.

13. Watts Bar Nuclear Plant (WBN) Unit 1 - Proposed Changes to Final Safety Analysis Report (FSAR) For Installation of Westinghouse Eagle-21 Process Protection System (TAC 81063), November 5, 1993. [NRC ADAMS Accession No. ML073200287]
14. Garill Coles, Pradeep Ramuhalli, Edward (Ted) Quinn, Ron Jarrett, and Vivek Agarwal, "Approach to Crediting Self-Diagnostics Features of Digital Instrumentation & Control to Achieve Technical Specifications Surveillance Test Interval Extension," NPIC&HMIT 2021, June 14–17, 2021.
15. Regulatory Guide 1.174, Revision 3, *An Approach for Plant-Specific, Risk-Informed Decision-making: Technical Specifications*, US NRC, 2018.
16. IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3," Edition 2.0*. 2010-04.
17. IEC 61508-2, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 2: Requirements for electrical/electronic/programmable electronic safety-related systems*. 2010-04.
18. T. [Edward) Quinn, J. Mauck, R. Bockhorst, and K. Thomas, "Digital Sensor Technology," INL/EXT-13-29750, July 2013.
19. IEEE Std 1633-2016, IEEE Recommended Practice on Software Reliability, IEEE, 22 September 2016.
20. NUREG/CR-6141, Handbook of Methods for Risk-Based Analyses of Technical Specifications," prepared for the Nuclear Regulatory Commission, Washington D.C., December 1994.
21. NUREG-1431, Revision 5, Volume 1, "Standard Technical Specifications Westinghouse Plants, Specifications," US NRC, September 2021. [NRC ADAMS Accession No. ML21259A155]
22. NUREG-1431, Revision 5, Volume 2, "Standard Technical Specifications Westinghouse Plants, Bases," US NRC, September 2021. [NRC ADAMS Accession No. ML21259A159]
23. NUREG-1475, Revision 1, *Applying Statistics*, United States Nuclear Regulatory Commission, Dan Lurie, Lee Abramson, James Vail, March 2011.
24. ANSI N15.15-1974, *Assessment of the Assumption of Normality* (Employing Individual Observed Values, American National Standard.
25. American Society of Mechanical Engineers (ASME)/American Nuclear Society (ANS), RA-S-2008, Addendum A, *Standard for Level 1/Large Early Release Frequency Probabilistic Risk Assessment for Nuclear Power Plant Applications,* ASME New York NY, ANS, La Grange Park Illinois, February 2009.
26. NUREG/CR-6823, *Handbook of Parameter Estimation for Probabilistic Risk Assessment*, Sandia National Laboratories, Albuquerque, NM 87185-0748, September 2003. [NRC ADAMS Accession No. ML032900131]
27. Richard Rolland III and Raymond Schneider, "Lessons Learned in PRA Modeling of Digital Instrumentation and Control Systems," Probabilistic Safety Assessment and Management (PSAM)16, June 26-July 1, 2022, Honolulu, Hawaii, U.S.A.

APPENDIX A. Diagnostic Coverage

APPENDIX A. DIAGNOSTIC COVERAGE

Diagnostic coverage is defined as the "fraction of dangerous failures rates detected by diagnostics" and "does not include any faults detected by proof tests." *Dangerous failure* is defined as a "failure which impedes or disables a given safety action." [A.1]

Automatic diagnostic tests, or self-diagnostics, can be used to decrease the probability of dangerous hardware failures by detecting faults in a safety instrumented system. Self-diagnostics, also referred to as *diagnostics*, are used to ensure that failures are detected, and as a result, that they will use the appropriate default states. Self-diagnostics are dependent on knowledge of the failure modes of the system and components. Self-diagnostics can reduce the likelihood of a single failure that impacts a safety function through early detection and timely corrective actions, but it is practically impossible to detect all failure modes. Therefore, it is crucial to have a sufficiently complete set of failure modes and an understanding of the system and components is so important. The level of diagnostic coverage (DC) is related to the technical specifications (TS) testing interval. A more complete coverage can provide indications of faults and recovery actions in real time compared to waiting for a surveillance test sometime in the future.

Diagnostics can be performed on a system application or component level and can enforce a known state as the fault recovery action. Many systems have embedded self-diagnostics that are executed continuously. These self-diagnostics can be used to determine the health status of the system. It is recognized that self-diagnostic coverage can never be 100%—similar to how surveillance or proof-testing can never provide 100% coverage—because of the unknown unknowns and an incomplete understanding of all the failure modes. Nevertheless, greater knowledge and history of a system could facilitate a graded review by accepting the diagnostic coverage and the confidence in that coverage. With self-diagnostics, systems should be able to reliably detect failures, provide early warning of potential failures, and notify plant operators to take appropriate action so that safety margins are maintained. Moreover, self-diagnostics can provide added assurance that time-related degradation due to operation has not accumulated to a point that necessitates tests or corrective actions ahead of a scheduled surveillance interval.

Self-diagnostics can be useful in detecting failures.

IEEE Std 7-4.3.2-2016 [A.2], Clause 5.5.3, states that

> *Self-diagnostics are a means to provide timely detection of failures. Self-diagnostics are not required for systems in which failures can be detected by alternate means in a timely manner. If self-diagnostic functions are integrated into the safety system, these functions shall be subject to the same V&V processes as the safety functions.*

However, self-diagnostics should not affect the ability of the system to perform its function. IEEE Std 7-4.3.2-2016 [A.2], Clause 5.5.3, further states,

Self-diagnostic functions shall not adversely affect the ability of the PDD [programmable digital device] system to perform its safety function, or cause spurious actuations of the safety function.

The NRC also recognizes that although there are positive aspects of self-test features (i.e., self-diagnostics), these should not be compromised by the additional complexity that the self-test features may add to the safety system. Put simply, SRP BTP 7-17 [A.3] states that "[T]he improved ability to detect failures provided by the self-test features should outweigh the increased probability of failure associated with the self-test feature."

Failures can be announced (detectable) or unannounced (undetectable). One of the worst scenarios for a safety system is that it is in a failed state and there is no indication of a problem until the system is called upon to perform its safety function (i.e., it is in a standby state). Diagnostics can identify detectable failures, even for components in a standby state, and can thus be used to extend surveillance test intervals. It is the undetectable failures that may not be detectable until proof tests are performed, or an incident demands its operation. One goal of this research is to identify means to diagnostically test some of those (previously) undetectable failures.

The specific percentages of diagnostic coverage are specified to make it likely that any dangerous failure is detected by the self-diagnostics, thereby reducing the probability of an undiscovered failure. DC can be categorized by the following based on its design [A.4]:

- low: 60–90% coverage
- medium: 90–99% coverage
- high: >99% coverage

Annex C of IEC 61508-6 provides an example of calculating diagnostic coverage and should be read in conjunction with Annex C of IEC 61508-2.

> *A problem that remains is the confidentiality of information; manufacturers do not want to disclose details on the design of their sensors … This explains why reports on failure rates and diagnostic coverage exist on sensors, but they do not provide detailed design information. These evaluations give the numerical data–most importantly, failure rates and fault coverage–required by IEC 61508 for the calculations as presented its part 6.*
>
> *Sometimes independent assessors will perform fault insertion testing. In principle, this is comparable to performing a FMEDA. One advantage is that it concerns real insertion of faults, a disadvantage is that the number of faults that can be tested is lower and that some tests might be catastrophic. Also, the distribution of inserted faults might not reflect the distribution in actual use, and thus give a biased assessment of the fault behaviour that is to be expected. At the moment, the approach to smart sensor assessment, including fault insertion testing, is the subject of a new IEC standard …, now in its draft phase.*
>
> *The absence of design details makes it hard for users to assess the validity of the results and their applicability to each user's setting. Independent assessors (like EXIDA.com, TÜV, TNO and Factory Mutual) are therefore essential.*

In most instances, *detectable failures* are not hidden because they announce themselves or are discovered through normal operation or dedicated detection methods [A.4]. *Undetectable failures* are failures or faults that do not announce themselves when they occur and which remain hidden until detected by some means (e.g., diagnostic tests, proof tests, or operator intervention like physical inspection and manual tests). Undetectable failures cannot be repaired until they have been revealed or are repaired during routine maintenance. The term *revealed* is used for failures or faults that become evident due to being overt or as a result of being detected.

Undetected failures are not detected by automated diagnostics, operator intervention such as physical inspection and manual tests, or through normal operation.

After identifying a failure as detectable or undetectable, recognizing that the failure is a safe or dangerous failure is necessary so that the dangerous failure rate can be estimated. The consequence of the failures is used to classify the failure as safe or dangerous based on the impact or effect that the failure has on the device's operation [A.5]. A safe failure is a failure which favors a given safety action, whereas a dangerous failure is a failure which impedes or disables a given safety action; a failure is dangerous only

with regard to a given safety instrumented function (SIF). Of particular interest in being able to extend the surveillance interval is the dangerous undetected failure.

Failures are grouped in IEC 61508 into two main categories—safe failures and dangerous failures. Safe failures are divided into detectable (λ_{SD}) and undetectable failures (λ_{SU}) that do not affect the system's ability to perform its functions. Dangerous failures prevent the system from working properly on demand. Dangerous failures are also divided into detectable and undetectable failures with failure rates λ_{DD} and λ_{DU}, respectively. Some dangerous detectable failures can be detected by online self-diagnostics, whereas dangerous undetectable failures remain unobserved until the surveillance test. Therefore, the purpose of surveillance testing is to detect unrevealed faults at the time of testing, whereas diagnostic coverage allows the detection and remediation of fail-to-danger fault conditions between surveillance tests [A.6].

IEC-61508 defines these terms as follows:

> *Dangerous Detected Failure - A detected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous detected failures do not include hardware failures and software faults identified during proof testing, represented by the plant's surveillance testing.*
>
> *Dangerous Undetected Failure - An undetected failure which has the potential to put the safety instrumented system in a hazardous or fail-to-function state. Dangerous undetected failures do not include hardware failures and software faults identified during proof testing.*

In IEC 61511, the term *dangerous detected failures/faults* describes dangerous failures detected by diagnostic tests. The word *overt* is used to describe failures or faults that announce themselves when they occur (e.g., due to the change of state). Repair of such failures can begin as soon as they have occurred. When the detection is very fast, as when discovered using diagnostic tests, detected failures or faults are considered *overt* failures or faults. When the detection is not as fast, as when discovered using proof tests, the detected failures or faults cannot be considered overt when addressing safety integrity levels (SILs). A dangerous, revealed failure can be treated as a safe failure only if effective automatic or manual compensating measures are taken early enough to ensure that safety integrity requirements are met for the safety function.

In contrast, undetected, unrevealed, and covert failures are not detected, not revealed, and not overt. In IEC 61511, the term *dangerous undetected failures/faults* describes dangerous failures/faults that are not detected by diagnostic tests.

In a generic statement on the single failure criterion, IEEE 379-2000 states that "The safety systems shall perform all safety functions required for a design basis event in the presence of (1) any single detectable failure within the safety systems concurrent with all identifiable but nondetectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety function." Nondetectable failures are failures identified by analysis that cannot be detected through periodic testing or revealed by alarm or anomalous indication. Regulatory Guide 1.53 states that IEEE Std 379-1972 should be supplemented as follows: "The detectability of a single failure is predicated on the assumption that the test results in the presence of a failure are different from the results that would be obtained if no failure is present. Thus, inconclusive testing procedures such as continuity checks of relay circuit coils in lieu of relay operations should not be considered as adequate bases to classify as detectable all potential failures which could negate the functional capability of the tested device."

An extended surveillance interval will be dependent on time-related effects on components (drift and aging), component reliability, probability of failure on demand, announced/unannounced failures, and the ability to detect the health of the component if it is failing. DC represents the fraction of dangerous failure rates that can be detected by self-diagnostics [A.1]. Overall, DC has four failure states in which the component fails in a safe/unsafe state and the failure is detected/undetected by self-diagnostics. Once the failure rates are determined for each state, they can be used to determine the total dangerous failure rate. The relationship between detected/undetected and safe/dangerous is as follows:

λ_{SD} – failed in a safe manner, and the failure is detected by diagnostics or a plant trip

λ_{SU} – failed in a safe manner, but the failure was undetected by diagnostics but identified through proof tests

λ_{DD} – failed in a dangerous manner, and the failure is detected by diagnostics

λ_{DU} – failed in a dangerous manner, and the failure is undetected by diagnostics but identified through proof tests or occurrence of an incident

A key consideration in the crediting of monitoring is the treatment of what are termed *dangerous detected* and *dangerous undetected failure fractions*, which are established to provide input to the reliability model for the device and the associated system [18].

The total dangerous failure rate is then:

$$\lambda_{DT} = \lambda_{DD} + \lambda_{DU}$$

For safety applications, the DC is typically applied to dangerous failures. The DC for the dangerous failures of a device is

$$DC = \frac{\lambda_{DD}}{\lambda_{DT}}$$

For a safety instrumented subsystem with internal redundancy, DC is time dependent:

$$DC(t) = \frac{\lambda_{DD}(t)}{\lambda_{DT}(t)}$$

Extending the surveillance interval will require an understanding on component failures, their failure modes, and diagnostic coverage, its detectability/undetectability, and safe/dangerous failure state. ISA 84.00.01-1 Clause 11.9, ISA-TR84.00.02, provides guidance on (a) assessing random and systematic failures, failure modes and failure rates; (b) understanding the impact of diagnostics and mechanical integrity activities on reliability; (c) identifying sources of common cause, common mode, and systematic failures; and (d) using quantitative methodologies to verify the spurious trip rate.

Diagnostics may not be capable of detecting systematic errors such as software bugs [A.7]. However, appropriate precautionary measures to detect possible systematic faults can be implemented.

Testing is one method to provide assurance of the availability and effectiveness of functions important to safety and to confirm that they have not been degraded. In a system, channel, or component where failures would not be detected by testing or revealed by alarms or anomalous indications, the system should be analyzed for such undetected failures: the preferred course is to redesign the system or the test

schemes to make the failures easily detectable. Interconnected systems should also be tested to confirm that all of their interfaces operate correctly.

Testing falls into two areas:

1. Initial – Design V&V

2. Periodic (surveillance)

Initial testing can be used to prove functionality and operability upon completion of design or at the end of the commercial grade dedication (CGD) process. Periodic testing of an installed device can never be comprehensive. In particular, it is difficult to ensure that the test (or the self-diagnostics) will find and announce internal failures.

The surveillance test is manually initiated but may include automated or semi-automated test equipment to implement the test and/or record the test results. *Proof testing* is a synonym for surveillance testing used by IEC 61508. Surveillance testing should be designed to confirm that safety-critical functions are being performed properly (e.g., overlapping end-to-end), the test frequencies preferably being risk-based. *Self-diagnostics* are testing protocols that can be executed continuously. They try to perform most of the same functions but are implemented differently.

Often, self-diagnostics cannot be directly tested [A.8]. In fact, in most cases, there is no means to test the self-diagnostics to determine if they are working. Another aspect of this research is to identify possible tests for the diagnostics to ensure they are working and working properly. This could be through the use of watchdog timers to ensure that they are working, a digital twin to ensure that the software has not been modified, etc. Thus, no matter the diagnostic, the only way to be certain that a device is working is to test it. However, the test itself must adequately simulate real demand conditions.

Although the NRC uses the term surveillance test[5] rather than proof test in relation to I&C systems and components, ANSI/ANS NQA-1 requires tests, including, as appropriate, prototype qualification tests, production tests, proof tests prior to installation, construction tests, preoperational tests, operational tests, and computer program tests such as software design verification, factory acceptance tests, site acceptance tests, and in-use tests to be controlled. Required tests shall be controlled under appropriate environmental conditions using the tools and equipment necessary to conduct the test in a manner to fulfill test requirements and acceptance criteria. The tests performed shall obtain the necessary data with sufficient accuracy for evaluation and acceptance.

Proof testing is defined in IEC 61508-4 as a "Periodic test performed to detect dangerous hidden failures in a safety-related system so that, if necessary, a repair can restore the system to an 'as new' condition or as close as practical to this condition." A proof test is designed to reveal all the undetected/unrevealed failures that are not revealed until a demand is placed upon the component/system. A proof test is not a functional test or a diagnostic test. A functional test is conducted to ensure that a specified function is working correctly. However, a functional test in redundant channels does not necessarily reveal all faults. For example, a functional test in a subsystem with a one-out-of-two (1oo2) voting configuration may detect a dangerous fault of the sensor architecture, but it may not highlight the number of faults. A proof

[5] SRP BTP 7-17 defines surveillance tests as those tests that are "conducted specifically to confirm compliance with technical specification surveillance requirements." The BTP further defines periodic tests as those "tests performed at scheduled intervals to detect failures and verify operability" and notes that periodic tests include surveillance tests. The BTP defines a self-test as "a test or series of tests performed by a device upon itself" and recognizes that "self-tests include on-line continuous self-diagnostics, equipment-initiated self-diagnostics, and operator-initiated self-diagnostics."

test, however, would reveal all faults, even if there are multiple faults, as (typically) all elements are individually tested. In summary, the proof tests should demonstrate that all parts of the system are fully effective in delivering the relevant safety function, including any automatic or diagnostic test equipment that is used as part of testing either during service or during the proof test [A.9].

The benefit for industry is that the application of diagnostic techniques for cases in which none previously existed has the potential to decrease the surveillance test frequency and the scale of routine testing. However, surveillance testing does not necessarily render components any more reliable. Surveillance test intervals are set up to be consistent with the operating goals for the system.

Periodic surveillance tests, automated self-diagnostics, and surveillance tests can be performed to show the operability of the device and to meet availability targets. A system channel can be in a failed state while appearing to be running properly, and it is recognized that some failures will be undetected by self-diagnostics and surveillance tests. Surveillance testing should be designed to confirm that safety-critical functions are being performed properly (e.g., overlapping end-to-end). The test frequencies for surveillance tests should be risk informed.

France's Office of Nuclear Regulation (ONR) recognizes that surveillance testing can be more easily shown to be comprehensive for a simple system, so a failure that does occur can be expected not to persist beyond the next test interval [A.9]. For complex systems, especially software-based systems in which systematic faults are much more likely, the time-to-failure distribution is completely unknown, and periodic surveillance tests can only reveal random faults arising from non-software sources. In these cases, the level of uncertainty is higher, the safety margin must be larger, and the level of dependence placed on the system should therefore be correspondingly less.

Model-based testing methods may provide effective demonstration of whether devices are subject to certain types of common-cause failures (CCFs) and may establish a cost-effective automated testing framework for industry stakeholders to qualify equipment.

Automated testing programs are available for many OSs and languages. When a test will be run more than a few times, automated testing will usually save time and effort. Automated testing also removes the possibility of human error when a test procedure is followed. This removes the random error component, but it does leave open the possibility of systematic error, in which the automated test makes the same error every time it is run [A.10].

IEEE Std 1012-2004 [A.11], endorsed by RG 1.168, Rev. 2 [A.12], and IEEE Std 829-2008 [A.13], endorsed by RG 1.170, Rev. 1 [A.14], as well as the newer, unendorsed revisions do not provide the particulars of testing described herein, though perhaps they are implied. References to static analysis seem to refer to something more like code review and less like modern static analysis tools. Formal testing methods are mentioned briefly but not covered at length in later versions of IEEE Std 1012, which are not endorsed by the NRC at this writing (later versions of IEEE Std 1012-2004 include IEEE Std 1012-2012 and IEEE Std 2016).

NUREG/CR-6421 [A.15] evaluates six testing strategies:

1. static source code analysis
2. structural testing
3. functional testing
4. statistical testing
5. stress testing
6. regression testing

The industry and regulatory philosophy are shifting away from reliance on statistical testing and toward monitoring and trending to facilitate aging/reliability determinations. Nevertheless, statistical testing could be used to extend surveillance intervals. Statistical testing uses randomly generated test data from defined distributions based on an operational profile (e.g., expected use, hazardous use, or malicious use of the software product). Large amounts of test data are generated and can be targeted to cover particular areas or concerns, providing an increased possibility of identifying individual and multiple rare operating conditions that were not anticipated. Statistical testing may provide additional independent complementary activities.

NUREG/CR-6421 [A.15] states that "It is possible to use statistical testing for the goal of finding failures (random testing). Statistical testing does not rely on any knowledge of the internal composition of the software object and is the only way to provide assurance that a specified reliability level has been achieved. Statistical testing is a practical method in many cases when moderate-to-high reliability (in the range of 10-4 to 10-5 failures per demand) is required."

The main purpose of self-diagnostics is to increase reliability, so introducing diagnostics is beneficial, even if the volume of surveillance tests cannot be reduced. With periodic testing, some faults may remain undetected until the next periodic test, or in the worst case, until functional failure. The probability of these events can be greatly reduced using self-diagnostics. Because there are potential unrevealed (undetectable) failures, some of which may be unsafe failures, functional testing must still be performed to ensure that there are no unsafe failures remaining. The use of self-diagnostics may help to reduce the extent of the functional testing, but it will not eliminate the need for this testing.

In general, the surveillance test procedures do not address testing product diagnostics [A.16]. Conversely, the diagnostic coverage fraction of dangerous failure rates is not detected by diagnostics [A.7]. Diagnostic coverage does not include any faults detected by surveillance tests. Many devices have achieved a high IEC SIL via large diagnostic coverage factors, yet the means and procedures for testing the diagnostics are not provided or discussed in safety manuals.

Some failures are undetected by both diagnostic tests and surveillance tests. Because surveillance tests are not a very fast means of detecting undetected failures, the detected failures or faults cannot be considered overt failures or faults [A.17].

A.1 APPENDIX A REFERENCES

A.1 IEC 61508-1, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 1: Framework, definitions, system, hardware and application programming requirements*, 11 July 2018.

A.2 IEEE Std 7-4.3.2-2016, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Station," 29 January 2016.

A.3 SRP BTP 7-17, Rev. 6, "Guidance on Self-Test and Surveillance Test Provisions," August 2016. (ADAMS Accession No. ML16019A316)

A.4 IEC 61508-6, *Functional safety of electrical/electronic/programmable electronic safety-related systems – Part 6: Guidelines on the application of IEC 61508-2 and IEC 61508-3," Edition 2.0*. 2010-04.

A.5 ISA-TR84.00.02-2015, "Safety Integrity Level (SIL) Verification of Safety Instrumented Functions," Approved 8 September 2015.

A.6 S. Nunns, "Principles for proof testing of safety instrumented systems in the chemical industry," Prepared by ABB Ltd for the Health and Safety Executive, 2002.

A.7 ANSI/ISA-61511-2-2018 / IEC 61511-2:2016, Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 2: Guidelines for the application of IEC 61511-1:2016 (IEC 61511-2:2016, IDT)
A.8 "Proof Testing of Safety Instrumented Systems in the Onshore Chemical / Specialist Industry," UK Health and Safety Executive (HSE), Dec 14, 2018.
A.9 NS-TAST-GD-003, Revision 9, "Safety Systems," Office for Nuclear Regulation, September 2022. https://www.onr.org.uk/operational/tech_asst_guides/ns-tast-gd-003.docx
A.10 NASA-GB-8719.13, "NASA Software Safety Guidebook," National Aeronautics and Space Administration, March 31, 2004.
A.11 IEEE Std 1012-2004, "IEEE Standard for Software Verification and Validation," Piscataway, NJ, 2004.
A.12 Regulatory Guide 1.168, Revision 2, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," July 2013.
A.13 IEEE Std 829-2008, "IEEE Standard for Software and System Test Documentation," Piscataway, NJ, 2008.
A.14 Regulatory Guide 1.170, Revision 1, "Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," US NRC, July 2013.
A.15 NUREG/CR-6421, *A Proposed Acceptance Process for Commercial Off-the-Shelf (COTS) Software in Reactor Applications*, March 1996. [NRC ADAMS Accession No. ML063530384]
A.16 A. E. Summers, "IEC 61508 Product Approvals–Veering off Course," ControlGlobal.com, July 2008. https://www.controlglobal.com/articles/2008/187/
A.17 ANSI/ISA-61511-1-2018 / IEC 61511-1:2016, "Functional Safety – Safety Instrumented Systems for the Process Industry Sector – Part 1: Framework, definitions, system, hardware and application programming requirements," (IEC 61511-1:2016+AMD1:2017 CSV, IDT).

APPENDIX B. DRIFT ANALYSIS

APPENDIX B. DRIFT ANALYSES

B.1 METHODS

The methods used to determine the characteristics of the drift following NEI 04-10 Rev 1 and the associated reference are documented in this section. These methods are consistent with acceptable industry practices. Two separate results are calculated and used to assess the acceptability of extending the calibration interval using as-found, as-left (AF-AL) data. The first evaluation calculates the drift of the specific instruments in scope over the data recovery period and compares the results to existing acceptance criteria. The second evaluation calculates the drift over multiple calibration intervals, eliminating any effect of intermediate adjustments to the trip units.

B.2 USE OF MICROSOFT EXCEL OR SIMILAR SOFTWARE

Microsoft Excel 2007 are utilized to develop spreadsheets to perform the drift evaluation calculations. Manual calculations are utilized to provide an independent verification of the Excel calculations on a sampling basis.

B.3 DATA COLLECTION AND PREPARATION

AF-AL calibration data for the instruments in scope are collected from completed tests over a substantial time period and then entered into spreadsheets. The method in this section of NEI 04-10 is generally consistent with Section 6.2.6.3 of ISA-RP67.04.02-2010 (Reference B.9), which provides guidance for the implementation of ANSI/ISA-67.04.01-2006 (Reference B.4). Specifically, Section 6.2.6.3 provides a discussion of analyzing as-found and as-left calibration values.

Data points are calculated by subtracting the preceding as-left value from the subsequent as-found value for each of the test points. Only one data point is available for each bistable calibration interval. This determines the maximum change for the tested device for each calibration point as if no adjustments to the device had been made. The days between the tests are calculated in the same manner.

The collection of all of these data points (y_i) is the single interval data set. For multiple intervals, the single interval values are added together over the desired number of single intervals. If a trip unit is replaced, then the cumulative data string is stopped and restarted with the replacement unit.

The target test interval extension is used to help determine the number of segments or sets of data required including the 25% grace period. The differences in as-found and as-left values are calculated over a single interval and then over multiple test intervals depending upon the target extension interval. For each of the data sets created by these equations, the minimum, median, and maximum values of drift are determined.

B.4 IDENTIFICATION OF DATA OUTLIERS

Potential outliers will be identified, evaluated, and expelled if applicable. The critical value for G is calculated using the formula from NIST/SEMATECH e-Handbook of Statistical Methods, Section 1.3.5.17, Grubbs' test (Reference B.3).

B.5 TESTS FOR NORMAL DISTRIBUTION

B.5.1 D′ Test for Normality

The D′ test is recommended by ANSI N15.15-1974, Assessment of the Assumption of Normality (Employing Individual Observed Values), for moderate to large sample sizes (greater than 50) (Reference B.2). The D′ test calculates a test statistic value for the sample population and compares the calculated value to the values for the D′ percentage points of the distribution which are tabulated in ANSI N15.15-1974. The D′ test is two-sided, which effectively means that the calculated D′ must be bounded by the two-sided percentage points at the stated level of significance. For the given sample size, the calculated value of D′ must lie within the two values provided in the ANSI N15.15-1974 table so as to accept the hypothesis of normality.

The calculated D′ is then compared to values in ANSI15.15-1974, Table 5, associated with the sample size and 95% probability. If the calculated D′ value falls between the two table values, then the data are normally distributed. If this value falls outside the table values, the data are not normally distributed.

B.5.2 W Test for Normality

The W test is recommended by ANSI N15.15-1974, Assessment of the Assumption of Normality (Employing Individual Observed Values), for small sample sizes (fewer than 50). The W test calculates a test statistic value for the sample population and compares the calculated value with the percentage points of the distribution of the test statistic, which are tabulated in ANSI N15.15-1974.

B.6 BOUNDING VALUES, NORMAL DISTRIBUTION

The bounding values of the calibration data considering the 95% probability at a 95% confidence level can be calculated as described in Section 8 of Reference B.1 when the data are demonstrated to be normally distributed.

B.7 BOUNDING VALUES, NON-NORMAL DISTRIBUTIONS

If the sample fails the D′ test, then one option is to use the binomial pass/fail analysis. This method determines a value by arbitrarily selecting pass/fail criteria in an iterative process. The probability of the drift value falling within these criteria is described in Chapter 22 of Reference B.1 and can then be estimated by use of the binomial.

Since P is an estimate of the nominal probability that a value will fall inside the pass/fail criteria, the confidence interval on this estimate must be determined. A 95% confidence level is accepted for setpoint calculations by the NRC (References B.1, B.4, and B.5). Analysis following this methodology is also intended to comply with References B.6 and B.7. This process is repeated until a pass/fail criterion is found that will result in a minimum probability at the 95% confidence level of at least 95% that the drift values will fall within the pass/fail criteria.

To summarize the method, trial pass/fail limits are set, the nominal probability of meeting these trial limits is calculated, and the 95% confidence interval of the probability is calculated. If the minimum probability at the 95% confidence level of meeting the trial criteria is greater than 95%, then it is concluded that the trial criteria will bound the expected results on a 95/95 basis. The trial criterion is then considered to be the bounding variation in the calibration results.

B.8 ACCEPTANCE CRITERIA

After development of the 95/95 drift value based on AF-AL data is developed, it can be compared with the acceptance criteria in the associated surveillance procedure to see whether a change in either the AF or AL requirement is needed. The most important basis that should be explored is to evaluate

the plant setpoint and loop uncertainty calculation for the specific devices in the loop. The setpoint or loop uncertainty calculation of record should be kept in the design engineering group for the plant or fleet and may be an Nuclear Steam Supply System supplier generated and maintained document, or a utility specific document following the plant specific setpoint and loop uncertainty methodology. This methodology should reference ISA S67.04 in some version as well as a version of U.S. NRC Regulatory Guide 1.105 (Reference B.9).

We can envision three possible outcomes to the review of the 95/95 drift values derived from the AF-AL data for the specific loop:

1.) The drift values for the extended interval are within the surveillance procedure tolerances for AF-AL values, and no changes are necessary to either the surveillance procedure acceptance criteria or the associated setpoint and loop uncertainty calculation.
2.) The drift values for the extended interval are outside the acceptance criteria for the surveillance procedure but inside the uncertainty values included in the setpoint or loop uncertainty calculation. For this, a surveillance procedure change would be recommended to enlarge the AF-AL and a single page or minor change revision to the setpoint calc to refer to the revised analysis or latest drift values. This is a minor change.
3.) The drift values for the extended interval are outside both the acceptance criteria for the surveillance procedure and the allowances in the setpoint and loop uncertainty calculation. In this case both a surveillance procedure AND the setpoint calculation require revision. The level of effort for the revision process depends on the age of the calculation, number of minor revisions, etc. that must be incorporated and who the originating author is. Someone must be assigned to perform a new revision to the calculation to incorporate the new drift values. This may or may not result in a setpoint value change. Most of our experience has been to avoid setpoint changes to the best extent possible.

B.9 Appendix B References

B.1 NUREG-1475, Revision 1, *Applying Statistics*, United States Nuclear Regulatory Commission, Dan Lurie, Lee Abramson, James Vail, March 2011.

B.2 ANSI N15.15-1974, *Assessment of the Assumption of Normality (Employing Individual Observed Values*, American National Standard.

B.3 NIST/SEMATECH e-Handbook of Statistical Methods, http://www.itl.nist.gov/div898/handbook/, August 5, 2011.

B.4 American National Standards Institute (ANSI)/International Society of Automation (ISA), Standard 67.04.01-2018, *Setpoints for Nuclear Safety-Related Instrumentation*, ISA, Research Triangle Park, NC, 2018.

B.5 U.S. Nuclear Regulatory Commission, Regulatory Guide 1.105, Revision 3, "Setpoints for Safety-Related Instrumentation."

B.6 U.S. Nuclear Regulatory Commission, Generic Letter 91-04, "Changes in Technical Specification Surveillance Intervals to Accommodate a 24-Month Fuel Cycle (Generic Letter 91-04)," dated April 2, 1991.

B.7 U.S. Nuclear Regulatory Commission, Regulatory Issue Summary (RIS) 2006-17, NRC Staff Technical Position on the Requirements of 10 CFR 50.36, "Technical Specifications," Regarding Limiting Safety System Settings During Periodic Testing and Calibration of Instrument Channels, August 24, 2006.

B.8 ISA-RP67.04.02-2010, Methodologies for the Determination of Setpoints for Nuclear Safety-Related Instrumentation, International Society of Automation, 2010.

B.9 Regulatory Guide 1.105, Rev. 4, “Setpoints for Safety-Related Instrumentation,” US NRC, February 2021.