Introduction to the SDOE Tabletop Example

This example is intended to be complete and at the expected level of detail for the LAR. The phrase “the licensee” has been used throughout this example, which would be replaced by the licensee’s name for an actual LAR submittal, as well as “vendor” being replaced by the vendor’s name. Rewriting the example to eliminating the words “vendor” and “licensee” eliminates the need to identify who performed the evaluations, review, and acceptance. If neither is specified, then the assumption is that the licensee and vendor worked cooperatively.

The example loosely uses the Diablo Canyon architecture, for the portion of the system implemented with the Tricon, extended to include the Reactor Trip System (RTS), Engineered Safety Features (ESF), and Plant Protection System (PPS). Evaluations will be maintained, updated, and retained throughout the system lifecycle to provide supporting materials for NRC review, audit, and inspection as well as a basis for the licensee’s cyber security program. The example includes resolution of Triconex V10 Plant Specific Action Items (PSAIs) applicable to SDOE.

This example does not include a diverse actuation system (DAS) that might be employed, or the field programmable gate array- (FPGA-) based equipment applied to Diablo Canyon. Separate evaluations would be provided for DAS or FPGA-based equipment, to avoid the confusion that would result if two diverse vendors, processes, evaluations, and discussions were intertwined. Since the DAS is non-safety related, there would be no topical report or SE, and thus dependence on the licensee’s evaluation. The analog and discrete interfaces between the ESF, DAS, sensors, and actuated equipment will be included in other portions of this LAR.

D.8 Secure Development and Operational Environment (SDOE)

The licensee based their review and conclusions accepting the vendor’s Secure Development Environment (SDE), which generates equipment that will provide an acceptable Secure Operating Environment (SOE) when installed in the plant. The review is based on the regulatory requirements in RG 1.152, Revision 3, Regulatory Position C.2, and the NRC’s conclusions in the SE. This review and evaluation resolves Tricon PSAI Items 4, 14, 15, 18, and 19. The Vendor Oversight Plan ensures that the vendor follows all applicable plans, procedures, and instructions, including compliance to the updated SDOE Plan. The Vendor Oversight Plan will involve licensee technical staff for technical evaluations.

D.8.a Vulnerability Assessment

The licensee and vendor documented the existing SDE vulnerabilities that would allow unintended, inadvertent, or unauthorized access to the development environment that would lead to a compromise of the system. The vulnerability assessment has been completed for the SDE, including the permanently allocated computers, printers, storage media, off-site backups, and software tools required to implement the isolated SDE. All known vulnerabilities have been addressed in the SDE plans and processes. The assessment started with the NRC evaluation of the then-existing vendor’s SDE program as the program existed during the NRC audit. Changes to the vendor’s SDE since the NRC audit were evaluated and determined to be appropriate and effective.

The vulnerability assessment evaluated, and extended the existing industrial operational vulnerability assessment of the Tricon for SOE. This included those SOE vulnerabilities and compensating measures documented in the topical report and SE. The vulnerability assessment is specific to the replacement system architecture, including communication links to the engineering workstation (EWS).

The evaluation of system operational vulnerabilities for the as-designed system concentrated on the vulnerabilities of the system to unauthorized, inadvertent, or unintended access and the inability of the system to perform the required function or functions due to the undesired or unintended behavior of connected systems. The system level vulnerability assessment includes assessment of features required to prevent inadvertent access and change, and eliminate the potential for other connected systems to affect this system adversely. The vulnerability assessment was used to inform the system architecture and system requirements and will be reviewed and updated at each design and implementation stage.

The licensee has completed the SOE vulnerability analysis for the system requirements and architecture described in D.2.2.2.

For each identified vulnerability in the SOE, the assessment determined whether the vulnerability was 1) eliminated by the design, 2) mitigated to the extent practicable in the design, 3) eliminated or mitigated by installation practice and administrative procedures after installation at the licensee, or 4) represents an unresolved vulnerability that will require long-term monitoring.

Vulnerability assessments will be updated periodically as the design progresses, and closed assessments and requirements documents reopened and revised as necessary to reflect any required changes to the system, architecture, system, hardware, software, and HSI, including appropriate verification and validation through analysis, review, and test. Any gaps identified during verification and validation will be resolved through the same process.

To ensure that vulnerabilities are tracked through to system completion, system-level requirements were added that eliminate, mitigate, or initiate tracking for each vulnerability, while keeping the documented vulnerability assessments and the traceability to the requirements created from vulnerabilities within the vendor's and licensee's cyber security protections.

D.8.b SDE Controls

The vendor's enhancements to the evaluated system architecture, procedures, and instructions have been determined to be appropriate. The enhancements ensure that system files do not migrate outside the SDE boundary, and now include automated version control to ensure control of file content.

The vendor's design and V&V process demonstrates, through formal reviews as well as forward and backwards traceability, that each piece of application code is required by the design. The licensee reviews vendor V&V reports. As Tricons are moved into the vendor's SDE environment, the vendor performs actions to ensure that the Tricon contains only the platform software intended. The software tools are assessed for the possibility of infection with inappropriate software. Files moved into the SDE are assessed for malware. While in the vendor's controlled SDE area, the vendor ensures that all changes are documented, including hardware and software configuration, software tools, and application software. The V&V process also ensures that the transformations from system requirements through to implemented, reviewed, analyzed, integrated, and tested code is correct, accurate, complete, and implements the required functions. The vendor's V&V process includes use of automated test tools, to minimize human error when performing testing, including regression testing and simulation testing of the implemented system. The vendor's SDE process and activities performed by the design and V&V staff combine to ensure that inappropriate code is not included in the system.

The vendor's SDE hardware and software changes include the expected updates to the current versions of the software and hardware tools used by the vendor to protect their islanded development environment. These updates are applied in a controlled and secure manner. The SDE controls include scanning tools used to review files of portable media and mobile devices (PMMD) being imported into the development environment. The current SDE provides better protection from identified vulnerabilities with updated software and hardware versions from those evaluated in the SE. The licensee concludes that that the updated SDE provides additional protection appropriate for the vulnerabilities identified at the time of the evaluation.

The vendor's updated SDE program was used in the revised modules for this system, which were developed under the vendor's updated SDE program and environment. The licensee has reviewed and accepted the vendor's documentation demonstrating that the modifications were made under the new program. The effects of these new modules on the SOE are evaluated below.

The vendor staff writes all application software for this project either specifically for this project or from previously written software from prior safety related projects. There is no software of unknown provenance in the vendor's platform software, application software, software tools, or libraries, including the new modules.

The vendor is implementing project management, configuration control, change management, and the other expected software processes that preclude introduction of inappropriate requirements or coding into their platform, software tools, or application software in accordance with their established and accepted processes.

The licensee evaluated the vendor's processes for ensuring tamper resistance of the system while the vendor is packaging the system for shipment and during shipment. The vendor will make use of serialized security tape on boxes and separately transmitted serial number records to ensure tampering has not occurred during shipment or storage.

These processes will be applied to this system, which will be verified by licensee inspections and vendor oversight. The licensee concludes that this evaluation of the SDE resolves PSAI 14 evaluating the currently existing SDE and changes from the SDE evaluated in the SE. The completed and ongoing evaluation of the vendor's current SDE program resolves NRC SE PSAI #15 by evaluating the currently existing SDE program, including updates.

D.8.c Description of SOE Controls

The SOE security features require software, and SOE-specific requirements are incorporated into the software requirements documents. The V&V process defined in the software process will ensure that system and software requirements are implemented, reviewed, analyzed, and tested. For those SOE security features that require hardware, administrative procedures, or human interactions, the vendor's and licensee's processes will ensure that the features are implemented, and tested as part of the overall system testing, including interactions with the hardware, humans, and software. During the system lifecycle, all changes to the design will be evaluated for adverse effects on the SOE.

The system architecture has no data communications inward to the Tricons from external systems, and thus there is no potential for remote access to the system. The system elements implementing bistables, logic, bypasses, and actuations are safety related. There are communications links within the safety related systems, between RTS and PPS and between ESF and PPS. Installation features between divisional fire areas will protect these links appropriately. Communication within the system meets the regulatory expectations established in DI&C-ISG-04, as demonstrated in another portion of this LAR.

The system elements that broadcast data to the non-safety related communication equipment and then to the non-safety related Plant Computer System are safety related, with isolation and independence provided by the redundant, dedicated function, unidirectional fiber optic serial data paths and broadcast-only safety related communication features in the Tricon. No installed hardware supports sending data from the non-safety related PCS to the safety related Tricons, and thus no potential for non-safety related systems to affect the safety functions.

As described in the architecture, the vendor provides four EWS laptops, which are not normally connected to any Tricon, as described in revisions to existing and new plant administrative procedures (resolving Tricon PSAI 4). The licensee will assign each laptop to a specific division and control that assignment by administrative procedure. In order to access any of the Tricons, the engineer or technician must know the EWS software tools password. The engineer or technician must also have access to the Operations-controlled key to the cabinet in which the individual Tricon is installed (resolving Tricon PSAI 19) and Tricon key. In order to change anything in the Tricon, the engineer or technician must also have the key that transfers the Tricon platform software from Run to Program state, requiring physical access to the Tricon. Administrative procedures will be used to install software or configuration modifications in all three Main Processors. Since an EWS is not normally connected, and only one division can be taken out of service and a EWS attached, as controlled by administrative procedure, there is no potential for any or all EWS to adversely affect all divisions simultaneously.

The replacement system are considered Cyber Security Level 4, and protected appropriately by the system architecture and implementation. This is enforced in safety related hardware and software, in that the only fiber optic connections made are to transmitters on the safety related Tricons and receivers on the communications equipment. There is no hardware connection to the Tricon’s receiving fiber optic port. These requirements are included in the system design requirements, and enforced by both licensee oversight of the vendor and by the vendors’ internal verification and validation programs.

The vendor does not combine non-safety related communications, including communications with the EWS, on modules that perform safety functions. Since all bi-directional links are either internal to the Tricon or between a Tricon and the EWS, no further testing is required. This resolves PSAI Item 18.

Each EWS will be stored in a locked cabinet, under Operations control, within the Vital Area. The licensee’s Information Technology staff will update the EWS under a plant work order and normal plant configuration control. The vendor will scan each EWS before use and again after use, using current software tools and configuration, to detect malware.