THE *NUCLEAR NEWS* INTERVIEW

Scott Patterson: Digital I&C upgrades and regulatory guidance

A project manager offers comments on digital upgrades at Diablo Canyon, plus some information on an NRC task force that is dealing with guidance documents for going digital.

Scott Patterson is the program manager for instrumentation and control obsolescence management at the Diablo Canyon nuclear power plant. That means he deals with upgrading any piece of I&C equipment that has become outmoded or has an issue with reliability or maintenance.

Patterson works with a core group of three project engineers that specifically focuses on digitizing plant systems. When the situation calls for it, the group brings in technical advisors to help with "system architecture," which is another way of saying a design of a system that works. The group also deals with one set of vendors for integrating the new digital systems into the plant, and another set to make sure that the software used to run the systems does what it is supposed to do. For safety-related systems, another vendor does an independent review of the software before it is installed.

Patterson: "The NRC is in the process of developing improved guidance that the industry can use to upgrade from analog to digital I&C equipment."

Pacific Gas & Electric Company operates the two-unit Diablo Canyon plant, in Avila Beach, Calif. Unit 1 started commercial operation in April 1984, and Unit 2 in August 1985. The plant's management has not yet decided whether it will seek license extension from the Nuclear Regulatory Commission—the units' current operating licenses do not expire until the mid-2020s—but system upgrades continue to be an important part of the plant's high reliability and solid operating cycles.

Patterson, who has been at Diablo Canyon for 26 years, started as a technician at the plant while earning a degree in electronic engineering. He then became an I&C maintenance engineer and later a digital systems engineer, and was supervisor of the digital systems engineering team. Most recently he has been a project engineer focusing strictly on I&C systems.

Patterson participated in a panel session on I&C licensing issues at the ANS/ENS International Meeting in Washington, D.C., in November. He talked with Rick Michal, *NN* senior editor, about system upgrades at Diablo Canyon and about his work on an NRC task force that is looking into digital I&C issues for nuclear power plants.

Diablo Canyon's two control rooms were retrofitted with digital soft control human-machine interfaces such as these for feedwater and main turbine control systems. (Photos: Scott Patterson)

What kind of I&C upgrades have been made at Diablo Canyon?

Most of the equipment in the control room is still the original analog equipment from when the plant went on line in the 1980s, but we've upgraded several control systems to digital, such as the main turbine control system and the feedwater control system. Those are the big projects that we've completed, but we've also done smaller ones that involve analog-to-digital or digital-to-digital upgrades. We're also replacing the control room's paper recorders with paperless recorders, due to obsolescence, because there are no spare parts for the paper recorders.

"One of the biggest challenges is getting the right people on the project team and keeping them engaged in completing the project."

What's up next?

A large I&C project currently in progress is the digitizing of our process control systems. Each of our two reactors has its own system. While the hardware is the same, the systems themselves operate independently. The systems currently are made up of old analog equipment, but their failure liability is starting to increase, and that's why we're upgrading them. We are also replacing our plant process computers, and those are scheduled to be installed in both units in 2008.

Are your control rooms set up in separate buildings, or in one shared space?

The two control rooms share one big space, which looks like two horseshoes that come together at the open ends. The control rooms are back to back, with Unit 1 on one side and Unit 2 on the other.

What is the most challenging aspect of your job when doing an upgrade?

One of the biggest challenges is getting the right people on the project team and keeping them engaged in completing the project. There are other issues that come up in the plant that take the focus off the project at hand, and there is always competition for resources from other projects. That is why it is so important to have a core group that is dedicated to a project. But even with a successful team in place, there are many other people involved in the day-to-day maintenance of the plant who are needed to have a successful project.

Are you doing upgrades in the plant outside the control room?

Yes. There are many systems located outside the control room that we are addressing, but most of them have parts in the control room. We'll be digitizing the ventilation control systems for our fuel handling and auxiliary building because those systems still have old discrete digital equipment that was designed in the late 1960s or early 1970s. The replacement job is planned for 2009 for Unit 2 and 2010 for Unit 1. Then, following the upgrades to our process control systems in 2009 through 2011, we'll be replacing part of the reactor protection system. That system is already digital—we replaced the original analog system in the early 1990s—but it has issues that need to be addressed, and our strategic plan has identified a common platform for these systems that will minimize maintenance and increase reliability. For upgrading that system, we're working with the Nuclear Regulatory Commission on what is called a "diversity and defense-in-depth" evaluation for the project. The NRC has provided guidance (NUREG/CR-6303) for doing that evaluation, and we want to make sure that we understand the guidance and that the design architecture we do for the job is acceptable to the NRC.

The work on the process control systems is broken down into two phases: The first phase will be done in 2009, and the second phase in 2010 and 2011. Then the reactor protection system is scheduled to be done in 2012. It takes about two years to get a license amendment approved by the NRC—I should point out that before we make any changes to the reactor protection system, we need to get a license amendment from the NRC.

What are the NRC's guidelines that you mentioned?

The NRC is in the process of developing improved guidance that the industry can use to upgrade from analog to digital I&C equipment. In fact, in August we submitted a white paper to the NRC that describes the new equipment we would like to install for our process protection systems. The NRC is reviewing it as a "test case" for its new I&C guidance. The agency is going to apply the new guidance to our test case to see if what we submitted is an acceptable architecture based on the existing and new guidance. It will also help the agency determine if more detail is needed in the guidance or if it needs some other revision. The process will also help us by getting the NRC's feedback on our systems architecture.

Did you help develop the white paper?

I did. The white paper is a preliminary diversity and defense-in-depth evaluation. It describes the existing plant architecture and the proposed architecture of the control and protection systems. The main focus of the paper is addressing common-cause failures and how they are handled with either a diverse actuation system or defensive measures that are built into the system or

The future of rod control is NOW

We're pioneers in digital rod control technology with 30 years of experience.

Data Systems & Solutions' rod control systems are operating with unequaled reliability in 75 plants throughout the world. Our newest state-of-the-art system is ready to install in your plant today.

Let us show you how we can upgrade your rod control system and ensure high reliability and low operating costs well into the future.

Contact: Data Systems & Solutions, LLC
Tel: USA: +1 (256) 705-2166 / +1 (978) 250-1684 EUROPE: +33 (0) 4 76 -61-15 00
info@ds-s.com www.ds-s.com

ProtectPerformPredict

Data Systems & Solutions

component architecture. I am working with the NRC right now on a task force working group for I&C diversity issues. The NRC is trying to come up with better guidance for determining when a plant would need a diverse actuation system or diverse indication and controls.

What does "diverse actuation system" mean?

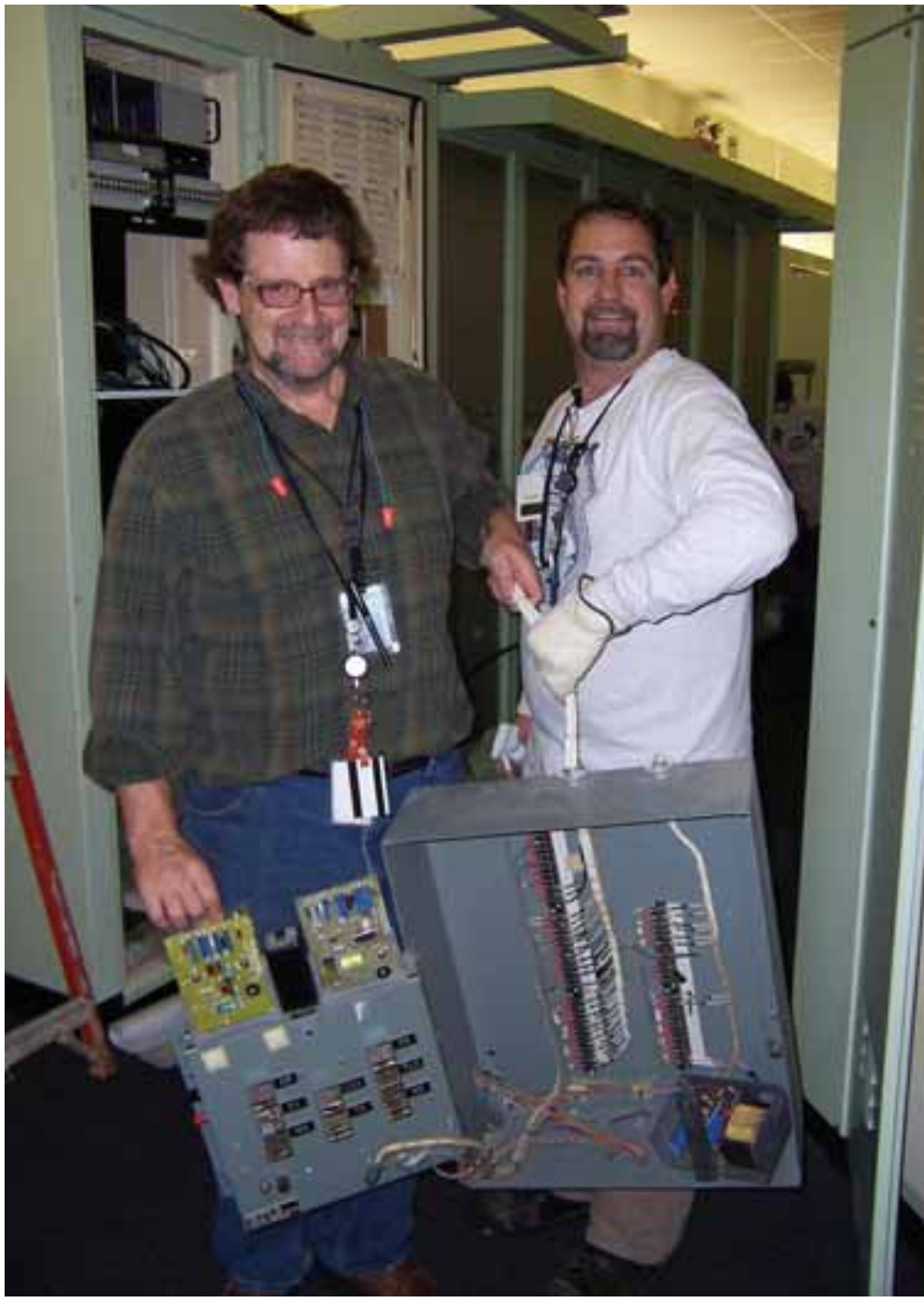
It means that if we had to replace the reactor protection system, for example, the NRC would require that we do a diversity defense-in-depth evaluation for the project to make sure that what we install won't have a negative impact on the safe operation of the plant and that we have backup systems in place to negate the likelihood of system failure. The agency's basic concern with installing new digital equipment is that there might be some sort of common-cause failure that is new to the software being installed. Or there might be common problems with how the software interfaces with the hardware. So, if the analog reactor protection system is upgraded with digital equipment, the plant has to evaluate whether or not there is a diverse backup system in case there is a failure that affects all equipment that is on the same platform. Adding a diverse backup system, which could be analog or another digital system made by a different manufacturer, can provide this extra layer of protection, which is defense-in-depth. The task force is trying to help the NRC come up with better guidance that will help plants and the NRC determine acceptable solutions when a license amendment request is submitted.

Is the task force looking at digital systems to be installed at existing plants, or are you also considering new plants that are yet to be built?

Both. This guidance will affect all existing plants and all the new reactors that are coming up. The same I&C concerns that existing plants have now will exist for the new reactors. The new plants obviously will be installing digital equipment everywhere in the plant, so this is a big issue for them.

How did this diversity issue develop?

There are very few manufacturers that are developing analog equipment anymore. The advantages of digital equipment over analog are many, and digital is the desired architecture for most industries. The existing nuclear plants originally had mostly analog equipment because they were built before digital was available. Analog equipment is relatively simple and can be completely tested, eliminating the possibility of common-cause failures. Digital equipment, with software, is very complex, and there is usually no way to test every condition. Plants started installing digital equipment in the late 1980s and early 1990s, resulting in the NRC's publishing Branch Technical Position HICB-19, which requires that a diversity and defense-in-depth evaluation be done to determine whether a diverse system is required. When software is added to the equation, common-cause failures cannot be ruled out, so they need to be addressed.



I&C technicians Jeff Carter and Mark Machala remove old analog equipment from the moisture separator reheat system before replacing them with new digital components.

What are some common-cause failures?

There are several types. The NRC is most concerned about failures that prevent the safety function from occurring. In other words, if a reactor trip is called for and it doesn't happen, then that is a concern. There are the undetected failures that can happen that are not discovered until the system is tested or challenged. Unless the system is called upon, such a failure won't be recognized until it's too late. Spurious actuations are not as much of a concern because they identify themselves immediately and can be corrected before the protective function is required.

Do you do periodic testing of your analog systems?

Yes, we test them at various intervals, depending on the system. But if something occurs between those tests that causes a multiple redundant channel fail, then that's

40 years from now, you'll still feel the love.

Lasting love. It's reliable. It's predictable. It's safe. And it can survive life's most grueling challenges.

The same holds true for Thermo Scientific Neutron Flux Monitoring Systems. Our state-of-the-art systems measure the full neutron flux range with a single detector—more than 11 decades from cold reactor shutdown to 200% full power.

Upgrade your source and intermediate range channels to Thermo Scientific systems with fission-chamber technology. Our solutions are not only less costly and more reliable, they have a 40-year qualified life. Which is a long time in any relationship.

To learn more, visit www.thermo.com/nuclear or call 1 (800) 488–4399.

Thermo Scientific Neutron Flux Monitoring Systems—
Qualified for Post-Accident Monitoring and Class 1E Safety-Related applications.

Part of Thermo Fisher Scientific

Thermo SCIENTIFIC

what we're talking about protecting against. The diverse actuation system would be needed, and that would be the backup in case multiple failures happen. The probability of a multiple or common-cause failure is extremely low, but since it cannot be proved that something does not exist, we have to provide some backup means to protect the plant and the public if it does occur.

Could you talk more about the NRC's diversity task force?

Up to this point, the NRC guidance that is available is not clear, so it is very difficult to figure out what will be acceptable to the NRC. In order to submit an acceptable architecture, better guidance is needed to keep the proposal as simple as possible and to minimize the NRC's review cycle. This is a complex issue, and the task force has identified problem statements that are being addressed to clarify areas of most concern. For example, one of the problem statements addresses how much diversity is enough.

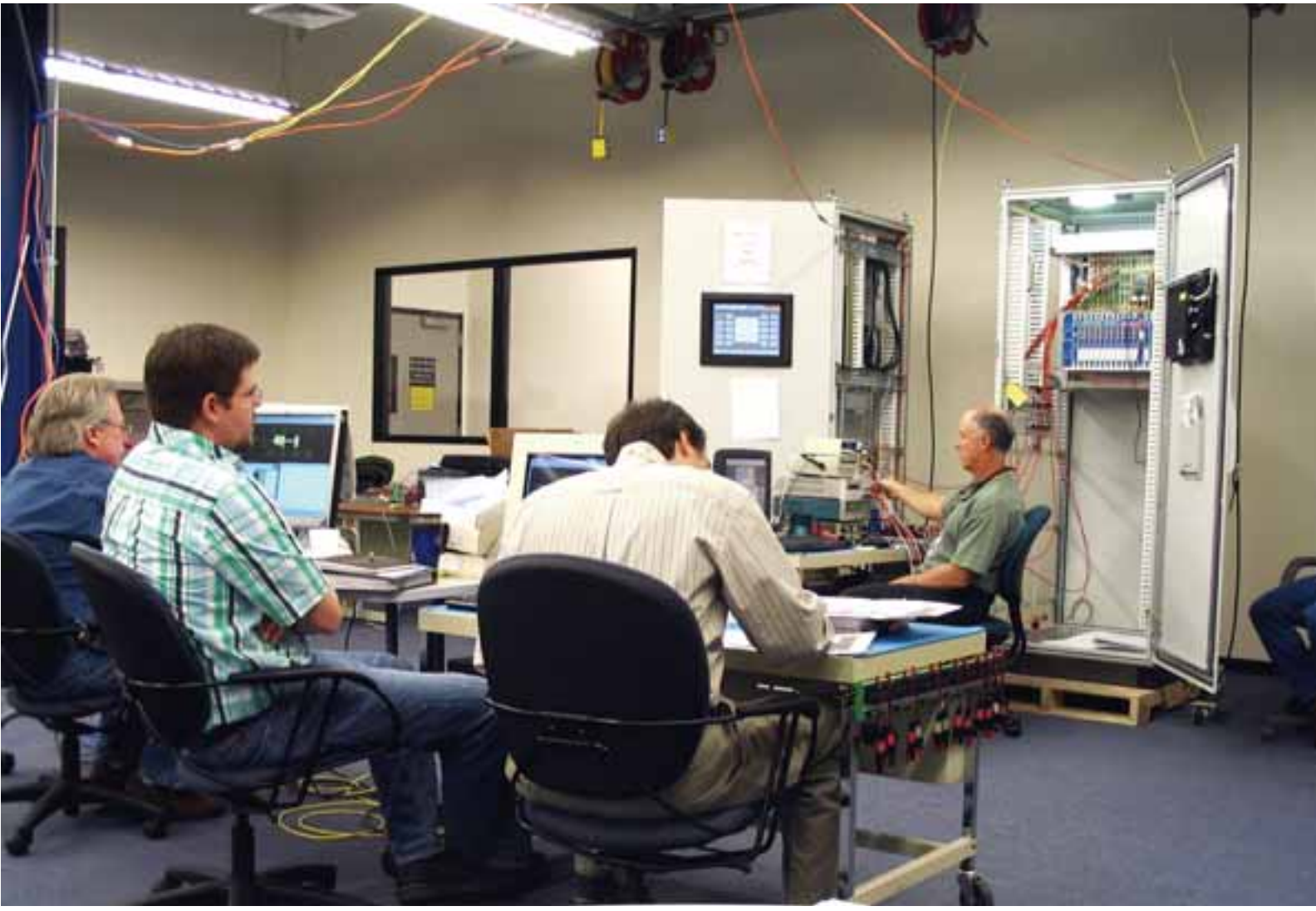
"In order to submit an acceptable architecture, better guidance is needed to keep the proposal as simple as possible and to minimize the NRC's review cycle."

Who is on the task force, and when was it formed?

The task force was formed in 2006 and includes representatives from the NRC, the Nuclear Energy Institute (NEI), vendors, and industry. There are six working groups: Cyber Security, Diversity and Defense-in-Depth, Risk-Informed Regulation of Digital I&C, Highly Integrated Control Rooms—Digital Communication Systems, Highly Integrated Control Rooms—Human Factors, and Licensing Process. The working groups were established to address each area of concern regarding digital systems. There is some overlap between groups, and that is coordinated by the NRC and NEI.

What are the responsibilities of the task force?

When the working groups were established, problem statements were identified that would be addressed for each area of concern, and short- and long-term goals were established for each group. The short-term goals were to produce interim staff guidance for applicable problem statements that could be completed by the end of September 2007. The task force recently finalized three or four interim staff guidance documents, which the NRC published in October. The long-term goals will continue to be worked on and will address the harder



I&C technicians and engineers perform factory acceptance testing of Diablo Canyon's main feedpump vibration monitoring system.

issues that will take time or require rulemaking.

What's the next step for the guidance documents?

The documents the NRC submitted to the task force are the final Revision 1 versions. The task force and the NEI representatives are reviewing them now. We're going to report back with our comments, and if the guidance needs to be revised, the NRC will do that. The guidance is not set in stone at this point.

In the meantime, are designers of new plants working by these guidance documents?

They will be. They've been active on the task force, so their concerns are being addressed. The reason the new-plant designers are very interested is that it directly affects the architecture and complexity required for the I&C systems of new plants. Since all of the equipment in them will most likely be digital, the designers will need to perform a diversity and defense-in-depth evaluation and implement diverse systems as necessary. This could significantly increase the complexity of the plant designs, and, obviously, the cost.

Has the task force done research on I&C issues at new plants, such as in Japan?

At an International Atomic Energy Agency conference in Washington, D.C., in June 2007, the NRC made a presentation that compared what France, Japan, Sweden, Germany, Taiwan, and Canada have done about I&C diversity issues at nuclear plants. The NRC also looked at other industries, such as the airline industry, to see what has happened there. So the NRC was aware of what was going on around the world on I&C issues when it wrote the guidance documents.

Are you aware of any "lessons learned" that have come from the international experiences?

I'm not, but I do know that EPRI [the Electric Power Research Institute] is putting together a report based on the evaluation of 324 system failures that have occurred over the years. EPRI evaluated each one of those failures to determine the root cause, and it plans to submit a report to the NRC about them. The report will contain evaluations of digital systems that have been installed, the failures that have occurred, and the determination of how many are software common-cause failures. There is a very low probability of common-cause failures, but without data to look at and evaluate, a valid conclusion can't be reached. Once the NRC has the report and analyzes it, it will have a better handle on how far its guidance needs to go in requiring diversity for digital systems. NN