NOR-CAL CONTROLS
ENERGY SOLUTIONS

THE FUTURE OF SCADA

PUBLISHED APRIL 2021

YOUR PROJECT.
OUR PASSION.

OUR EXPERTS

BOB LOPEZ
CEO OF **NOR-CAL CONTROLS**

Bob founded Nor-Cal in 2006 with the passion to provide customer-focused automation and controls engineering solutions that truly serve their clients. Bob is a senior level engineering professional with over 35 years of concentrated experience in the power generation industry, both traditional and renewables.

ERIC VALLETON
CTO OF **SOLV, INC.**, A SWINERTON COMPANY

Eric joined the Swinerton Renewable Energy (SRE) team in 2014 and oversees technology development for SOLV Inc., the operations and maintenance (O&M) group that manages over 9 gigawatts of solar PV facilities in North America. Eric is an experienced solar industry professional, who has focused his career on the design, development and implementation of monitoring and control solutions that have been applied to residential, C&I and utility-scale solar PV facilities.

INTRODUCTION

With the vast number of technological changes and rapid business growth the solar PV industry has undergone in the last 10 years, it is a somewhat arduous task to keep our eyes on the horizon and start considering the future of SCADA systems. According to SEIA, “The U.S. solar industry will install more than 324GW of capacity over the next 10 years,”[1] which would quadruple the current solar capacity installed today.

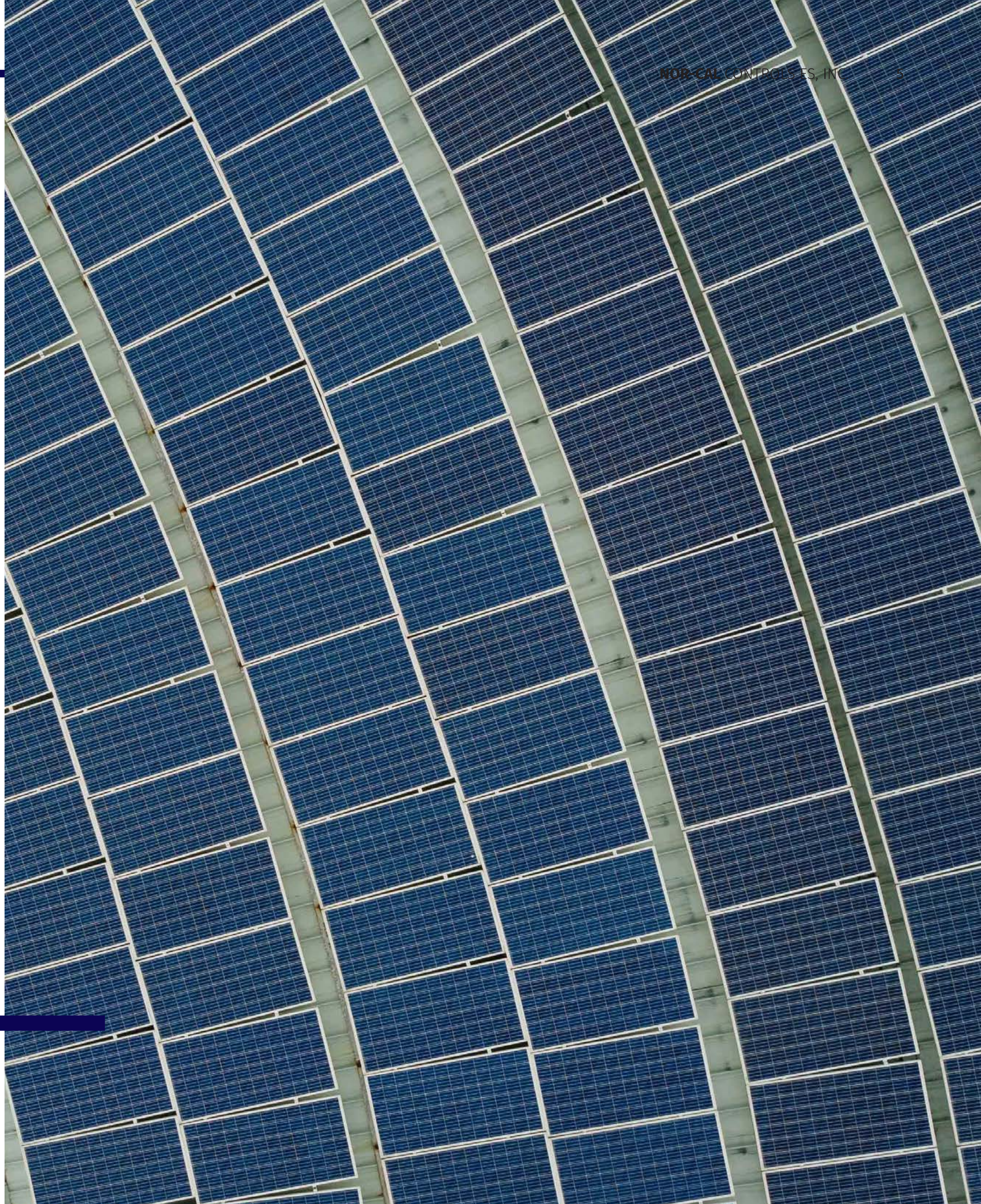
As the fastest growing new power generation industry, what can we expect for the future? We know that most panel arrays will last 20-25 years, but what will happen to the SCADA systems controlling them? How will these advancements impact O&M teams, EPCs and Asset Owners? We sat down with Eric Valleton, CTO of SOLV Inc., an O&M solution from Swinerton Renewable Energy, and Bob Lopez, CEO of Nor-Cal Controls, to see what their predictions are looking forward towards the next 5 years in solar PV SCADA systems.

“As generation capacities for utility-scale solar PV sites continue to increase, how will these expansions impact the SCADA systems that control them?

CAN YOU GIVE A BASIC OVERVIEW OF WHAT MAJOR CHANGES YOU HAVE SEEN HAPPEN FOR SCADA APPLICATIONS IN THE LAST 5 YEARS?

ERIC VALLETON: One of the biggest changes we have seen in SCADA platforms is a shift towards open architecture solutions. In the early days of utility-scale solar, the industry relied on platforms ranging from proprietary SCADA solutions adapted from industrial and infrastructure type applications, to black-box solutions developed by monitoring software start-ups. As our industry has matured and grown, this approach has presented many challenges with system integration, scalability, and long-term maintenance. We are now seeing a desire for modernized, browser-based solutions that utilize off-the-shelf hardware and software with a focus on comprehensive support.

BOB LOPEZ: As far as the SCADA systems we integrate, the software platforms themselves have not had a lot of changes. What I have seen happening is a migration towards interoperability protocols along with cloud-based solutions, interactions, and activities. These changes have happened through secure protocols like OPC UA (Open Platform Communications United Architecture) and MQTT (Message Queuing Telemetry Transport) for IoT (Internet of Things) applications. These protocols will take automation and control to the next phase of things.



WHERE DO YOU SEE SCADA GOING IN TERMS OF TECHNOLOGY IN THE NEXT 5 YEARS?

> There will be a big shift in how we design these platforms, with more emphasis on **cybersecurity** and improved operations and maintenance practices."
>
> - ERIC VALLETON

EV: That is an interesting question. I think as platforms move towards a more open architecture and we continue to see an increasing number of intelligent, IP-based nodes on the network, there will be a growing need to address cybersecurity and good security posture around SCADA systems and the facilities in which they are deployed. There will be a big shift in how we design these platforms, with more emphasis on cybersecurity and improved operations and maintenance practices. The other advancement will be more emphasis on designing for system maintenance. Many proprietary or legacy systems currently in use are outdated with little to no support left behind them. This presents risk to the long-term asset for which they are installed. Addressing system maintenance will be key to ensuring the safe and reliable operation of these assets.

BL: What I see happening will be a shift towards greater interoperability through common protocols. By that I mean if we are all speaking the same language, it does not matter what job you are doing on the specific site, whether it is a part of the DAS or part of the solar PV or site expansion. If all of the SCADA platforms and field devices are speaking a common language, we can all talk together, and we can all be orchestrated to act together supporting the grid with tight reliable

HOW DO YOU SEE ENERGY STORAGE, EMS LEVEL REQUIREMENTS FOR MONITORING AND CONTROL, FITTING INTO THE SCADA PROVIDER'S SCOPE OF WORK?

EV: It will be a natural progression for SCADA integrators. When we look at an EMS platform in relation to energy storage and at SCADA in relation to PV, they start to look very similar from an architectural and operational perspective. EMS enables a high level of supervisory control and performance optimization that the SCADA system could also be utilized to provide. I think SCADA integrators are going to be naturally pushed into expanding their product offering and taking on the site level controls and system integration for their clients. As a combined industry, we will need to align the terms and definitions used to describe the monitoring and controls to provide well defined scopes of work.

I think this progression is very analogous to what we saw in the early days of PV, where a lot of software companies providing monitoring solutions were forced into acting as DAS hardware providers. As the industry grew and more utility scale PV came online, these monitoring software vendors began to add control capabilities into their product offerings, additions that were often not a natural fit for their business models and presented several challenges. In response, SCADA integrators took the opportunity to leverage their experiences to offer a more robust solution that works with monitoring providers to fulfill their clients' needs. In energy storage, we are seeing a similar shift occur. As PV Asset Owners incorporate storage into their portfolios and attempt to standardize their preferred vendors, SCADA integrators will be compelled to expand their product offerings and continue to build partnerships with 3rd party EMS software providers to satisfy the needs of their clients

BL: This migration seems to be a logical fit. I see a BESS cabinet like a turbine compartment. In a turbine compartment you have fire suppression along with chemical dumping, damper controls, HVAC systems, etc., and you have those same things in a battery compartment. What I see happening will be a small, distributed controller placed inside each BESS compartments utilizing traditional I/O interface, (eg: analog connection to a temperature reading or a digital connection to a pressure switch). The BESS compartment protection and monitoring is critical to site safety and operation - I can see these BESS compartments driving the typical SCADA communion and go back to a more direct hard-wired interface since, as stated, the protection and control of the environment inside those compartments are critical and it could be catastrophic if something went wrong.

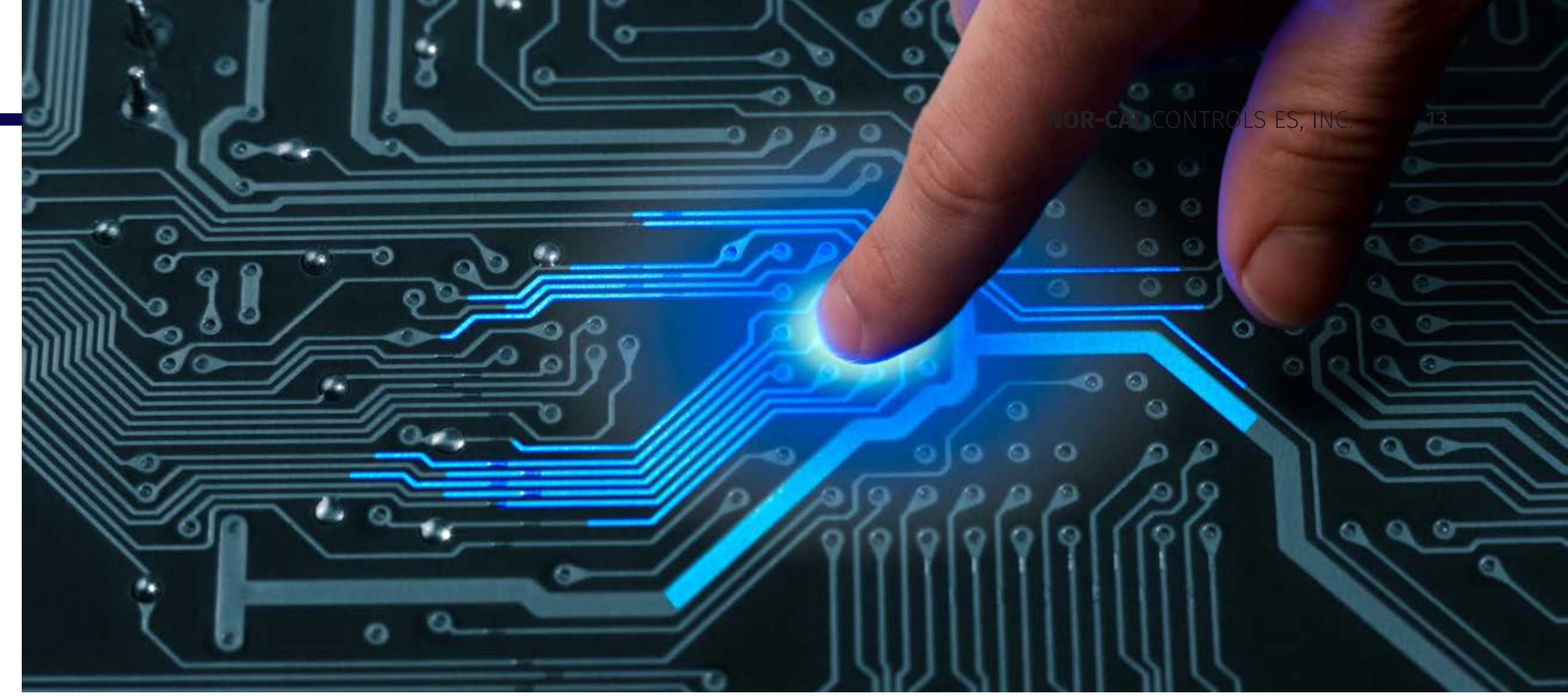
> There is a need to **better define** applicable standards and regulatory requirements around how SCADA systems are designed and utilized, especially with the heightened awareness around **ICS vulnerabilities**."
>
> \- ERIC VALLETON

WHERE DO YOU SEE SCADA GOING IN TERMS OF REGULATIONS IN THE NEXT 5 YEARS?

EV: From an RFP standpoint, the industry has taken an all-of-the-above approach when applying standards and regulations to the SCADA system, including NERC CIP, IEEE, IEC and ISOs. There is a need to better define applicable standards and regulatory requirements around how SCADA systems are designed and utilized, especially with the heightened awareness around ICS vulnerabilities.

I do not think we can ever get to just one all-encompassing set of regulations, though it should be looked at more holistically to leverage some of the existing work within NERC CIP, NIST Cyber Security Framework, IEEE 1547 and its applicable extensions. There is a lot of good work taking place right now within various industry working groups to distill the various standards and regulations down into a digestible view of where they apply in relation to system architecture. It will certainly utilize a layered approach that considers control methodology, security layers, communication protocols used, testing procedures, and more.

BL: I do not think SCADA is necessarily going to go anywhere as far as regulations. If you look at NERC CIP now, as long as the outbound protocols are encapsulated in SSO (single sign-on) or TOS (type of service) requirements and they are secure, and as long as the system interface in a data transmission is secure, SCADA systems will continue to have the requirements they already have. This might include assigning users with user rights and audit trails, both of which might get a bit more complicated. Change management software may also become integrated into the system as a security measure. But overall, those components are already there, so I do not see them changing a whole lot. That being said response times will be scrutinized and regulated, and the general network communication at a solar site will need to become tighter and faster. I believe this demand will drive protocols and network equipment, but not sure how these requirements would generally impact a SCADA package.



HOW DO YOU SEE ANY CYBER SECURITY REQUIREMENTS (I.E., NERC CIP) CHANGING AS PROJECTS GET LARGER IN CAPACITY AND GENERATING PORTFOLIOS CONTINUE TO GROW?

EV: They are going to continue to evolve, especially as the definition of system capacity continues to be refined. Currently, NERC CIP standards are applicable based on system size and voltage within a given interconnect on a facility by facility bases or as a MW aggregate for a control center. However, when we look at concentration of smaller facilities in geographic areas and the advancement of "virtualized" power plants, suddenly you have hundreds of megawatts or more of generating capacity. This presents a new set of cybersecurity challenges and exposes potential vulnerabilities in the bulk electric system. If we step back and look at renewables' growth and advancements in grid modernization, I think NERC and other regulatory entities are starting to see that there is a need to apply standards more consistently across the industry.

BL: Again, I do not know how much more it would change. We have a few large nuclear sites in the United States like Diablo Canyon, or coal plants like the Jim Bridger site in Wyoming (even though these sites are being decommissioned) with thousands of megawatts of capacity, and we are only now just starting to reach those megawatt levels with solar energy storage. It would appear that NERC is looking ahead as far as solar penetration and megawatt size goes. I think what we will have a more concentrated focus on controlling will be access and data transmission. Every solar site wants to pump the data they are tracking out to the cloud. They want analytics on it, and they want total remote visibility of it. The focus moving forward will be on how to get that data out securely and only have outbound traffic with the only inbound traffic being for control point adjustment. As solar sites and storage do get bigger, that does become a bigger vulnerability and threat.

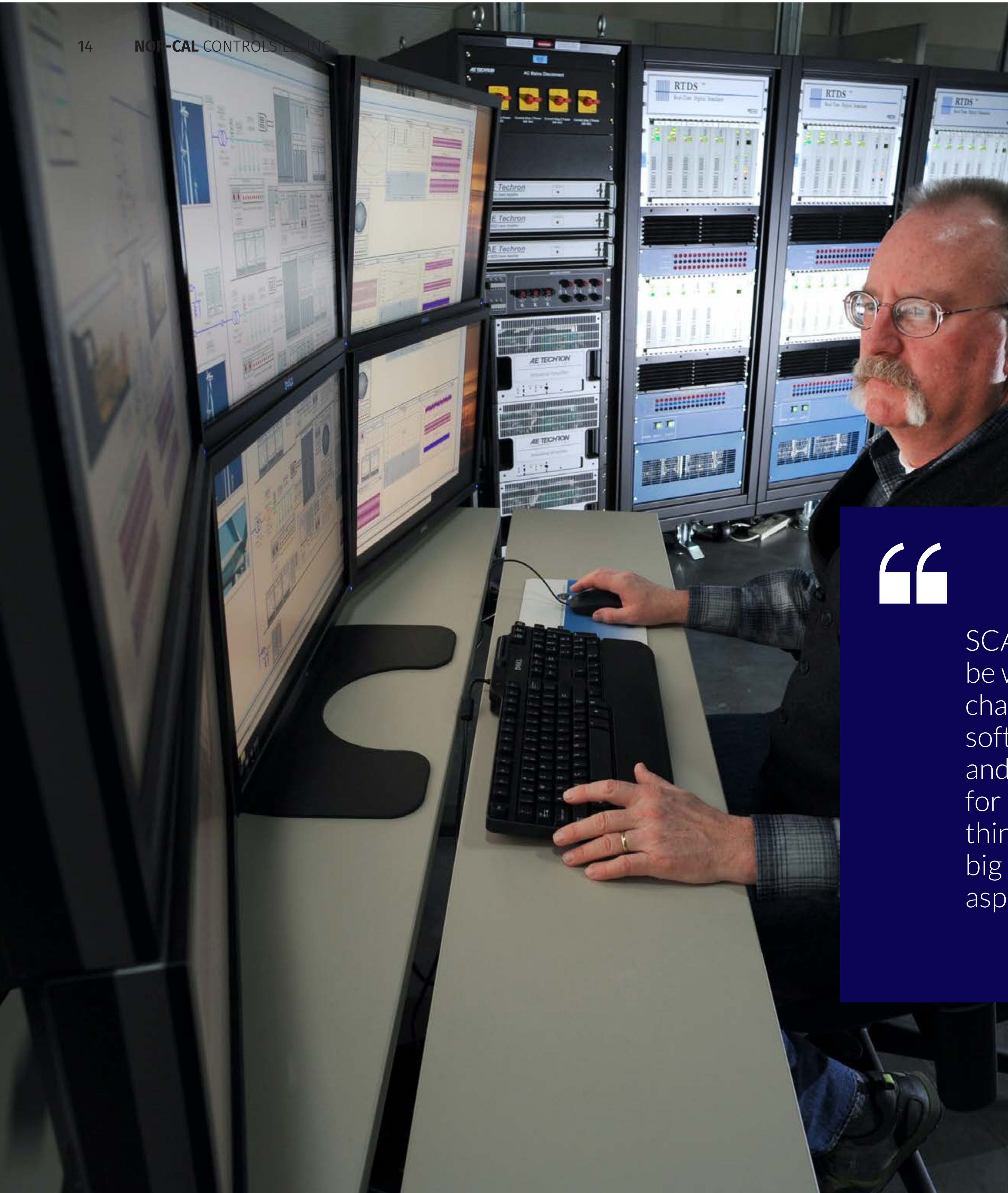
> "The focus moving forward will be on how to get that data out securely and **only have outbound traffic** with the only inbound traffic being for control point adjustment."
>
> \- BOB LOPEZ

DO YOU THINK WITH THE INCREASE IN STORAGE AND EMS SYSTEMS, WILL THERE BE A CHANGE TO CYBERSECURITY REQUIREMENTS?

EV: When we look at how storage systems are going to be utilized, it changes how we think about cybersecurity. A storage facility presents a massive amount of energy contained within a smaller footprint. When those assets are utilized for ancillary services like black star, it becomes critical infrastructure. A PV asset does not pose an existential threat to the bulk electric system in the same way an energy storage facility might. There should be varying degrees of system requirements depending on the use case of the asset. With EMS solutions being marketed as cloud-based controls and system optimization platforms, there is a real vulnerability there that should be addressed. The recent high-profile cyberattacks really challenged how we think about cybersecurity, the supply chain, and how to ensure the safe and reliable operations of generating assets. As a result, I think we will see industry vendors and regulators define and implement standards and regulations addressing these vulnerabilities.

BL: I do not know enough about the NERC requirements to speak to how they are evolving, but in my mind if you look at traditional power generation sites, we can compare apples to apples when talking about solar. A thousand-megawatt gas turbine compared to a thousand-megawatt solar storage system will still have a fence line and a controls system, and so the access to those systems is similar. What would change just because it is solar PV/storage, I am not sure. The audits might become more frequent, or the requirements might become more stringent, but I think as far as locking down the perimeter physically and ensuring cybersecurity, I don' think that will get more involved than it already is. Like anything, the laws will keep changing and devices will keep changing but the overall trend will continue to be to protect and isolate. This is just my opinion.

Something I think that is currently lacking is rigid change management requirements and documentation. I think that will become a bigger focus in the future. There will need to be a requirement for more transparent, well-tracked records of all the changes made to a site.



HOW DO YOU THINK THESE CHANGES WILL IMPACT O&M TEAMS?

EV: O&M vendors must closely consider facility access, both from a physical and technological perspective. We cannot just assume that because it is behind a physical fence or has a firewall that the site is secure. We also cannot assume that all vendors and escorted site personnel are going to understand and follow good security procedures. I think O&M teams are going to have to play a larger role in enforcing procedures that address local and remote network connectivity, Transient Cyber Asset (TSA) management, physical access in and around the facility and consistent communication. This will require more management and oversight in addition to ongoing cyber awareness training.

BL: For the O&M teams, changes to their change management process will become a more integrated function of their audits and documentation, for example it will impact how they provide their submittals and how they complete their MOD testing. SCADA software and hardware solutions are there to support day-to-day operations, so the software should also support and enable automated quarterly change management audit generation, instead of someone going in and having to do a manual excel spreadsheet of the data. SCADA providers should be working to provide change management software to incorporate and automate that process for O&M teams and I think that will help with a big piece of the security aspect for us. Firewall components already have multiple software options that can pull data and show who logged on when for an audit. In the SCADA systems themselves, one thing that is not automated or cleanly tracked right now is change management, so automating that process will positively impact O&M teams from a security and

"SCADA providers should be working to provide change management software to incorporate and automate that process for O&M teams and I think that will help with a big piece of the security aspect for us."

BOB LOPEZ

DO YOU THINK SCADA WILL BECOME A LARGER OR SMALLER COMPONENT OF UTILITY-SCALE SOLAR PV AND ALSO ENERGY STORAGE PROJECT PLANNING IN THE NEXT 5 YEARS?

EV: We are finding that the controls methodology and EMS/SCADA design is being inserted into the discussion much earlier than it was previously because of its impact on the overall design, construction, and operations of solar + storage facilities. The use case for the facility plays a critical role in defining the controls requirements and design, driving the need to have the SCADA integrators engaged earlier on in the discussion as the use case is developed. The impact of EMS/SCADA designs on project contracting, project financing, insurance underwriting and regulatory requirements are further driving the early involvement of integrators. I'm hopeful that we won't be last to the design party much longer!

BL: I think planning for SCADA earlier on will become more important to EPCs and Asset Owners through educational efforts to increase awareness of what SCADA is and what we do for these sites. SCADA is an important aspect because it is the brains of the site, but often it is one of the least expensive components to the overall plant. The truth of it is that even though it is probably the least expensive part of a solar site, it is still the most visible and the most critical. Without a good power plant controller (PPC) you cannot meet your LGA requirements, and you are going to be shut down. So, you can spend $100,000,000 on field equipment, but if you do not take the time to really think about your SCADA project (even if it only costs you $100,000), then you are missing the boat. You are missing a key point of what will provide stable site operations supporting a reliable stable grid.

HOW DO YOU SEE ASSET OWNERS OPTIMIZING/ IMPROVING THEIR SCADA SYSTEMS IN THE NEXT 5 YEARS?

EV: I think Asset Owners have an appetite for it and we are seeing it as a requirement in many new projects. Years of vendor consolidation and departure within the industry have raised awareness and concern about long term support for these types of systems. I think the open architecture approach utilizing commercial hardware and software with a broader engineering and end-user base to help support these systems is what Asset Owners are really looking for.

When you look at it from an Asset Owner perspective, the idea of operating a 20–30-year asset and banking on a proprietary solution backed by a company that is financially limited or positioned for acquisition is a risky proposition. I think some of the more sophisticated Asset Owners who have been in the industry long enough to see the consolidations and departures have been recognizing that and are taking a vested interest in identifying a long-term solution. Some of these Owners may have assets of their own that are now unsupported from a SCADA perspective. As the Owners' knowledge of these types of systems matures or they add personnel with better understanding of these systems to their teams, it has moved them to view it as a requirement for their projects and write it into their specifications.

Each organization is going to have their own approach to optimizing and improving their portfolio's SCADA infrastructure. Either they will choose to do it in-house, or they will look to their preferred SCADA integrator to provide a long-term, scalable, and supportable solution. I think where the conversation gets interesting is around existing assets and what to do with those assets that may have older systems that are either nearing end-of-life or need to be retrofitted, a costly replacement up front that they may not have accounted for in their OPEX budget. Over time it is much more efficient and scalable from a business standpoint to standardize an approach across their portfolio from the start.

BL: I hope that the main SCADA software vendors like Wonderware, Cimplicity and Ignition can all agree on an interface that uses the same standardized, secure protocol. Let us say for instance we standardize on OPC UA. Then all the major SCADA software providers would have OPC UA functionality for their client's servers and controllers (whether they are GE, Emerson, Rockwell, or Allen Bradley PLCs). All of these PLCs have an OPC UA component in their hardware, so the compatible software can be used natively. This way it would not matter what software is being used at an enterprise level because each of those platforms use the same communication protocol, so I can pick anything I want. Even if the HMIs look slightly different, I can get the same customized overall feel for all sites because they are all speaking the same language.

If we really want these IoT changes to really take hold, the first thing we have to do is to make sure all of our hardware and software components are speaking the same language. Once we do that, we can all share in a mass, global web of SCADA integration and applications. Until then, everyone has a little bit of a black box, and everyone will be somewhat isolated. I think black box systems are going to be driven out in the future. It's a lot like the competition between Betamax and VHS in the 1980's. For a long time, people were torn both ways not knowing which tape player to go with. Then all of a sudden Betamax dropped off and VHS took hold. For what reason? Who knows? Maybe it was accessibility or cost. I think that SCADA manufacturers probably thought when they were first starting that they could provide full-service contracts taking care of everything, and that those kinds of solutions would be appealing. They may be appealing to some Owners, but I think what is really appealing is knowing that no matter what you buy for your portfolio, open architecture systems allow you to plug in different things at any time. It will not require a costly rip and replace or keep any one on the hook for service contracts.

HOW WILL IMPORTANT WILL SCADA SYSTEM STANDARDIZATION BE AS ASSET OWNERS CONTINUE TO CONSOLIDATE THEIR ASSETS?

EV: I touched on it in the last question, but I think standardization will be a necessity for Asset Owners to operate their portfolios efficiently and cost effectively moving forward. This topic is really captured in two buckets, first of which is new builds and second being existing assets. For any new builds, standardization is addressed through RFP specifications, and to this end we are seeing more open-architecture requirements. Existing assets with aging and/or proprietary SCADA systems will often need to be replaced, a big project that requires careful planning with all stakeholders involved. Addressing system standardization from the outside is a big commitment for asset owners, both in terms of dollars and time. The investment strategy – whether the asset is a long-term or short-term hold – is often a primary driver in the planning process.

We are starting to see momentum in standardization, and I believe this is partly driven by Developers and Asset Owners who are challenged with consolidating their assets. When we step back and look at the SCADA integrators who serve this market, we are starting to see very similar system architecture and hardware stacks. SCADA integrators also have a vested interest in consolidation for the consistency it allows as Asset Owners seek to grow their portfolios. The reality is the market is too large for any one integrator to support on its own, so there is a lot of benefit in working together to influence and support standards.

BL: Standardization is important, but I do not think we are going to see Asset Owners standardize on the software specifically. I think standardization will become important for things like screen development, tagging, color animation, and alarming amongst other things. If an organization can get that type of standardization in place, it would not matter which platform they picked. There would always be the same look and feel so that anyone could get into the system, troubleshoot it, and work with it. The key to that is just standardization of the components built within the SCADA system or the PPC logic.

IS THERE ANYTHING ELSE YOU BELIEVE WILL BE IMPORTANT FOR SCADA IN THE NEXT 5 YEARS WE HAVE NOT TOUCHED ON YET?

EV: I don't think we can stress enough the importance of cyber awareness and good security posture for Industrial Control Systems (ICS) and the facilities and control centers in which they are used. It is important to recognize that threat actors are advancing at a startling rate and that the scale at which they are growing requires heightened industry awareness and involvement. We really need to think about how these systems are designed, deployed, and managed, and which stakeholders want access to that data. We see a strong desire for vendors to monetize the data to provide new services that create additional value streams for their clients. However, we need to recognize the risk doing so presents from a cybersecurity standpoint. As an industry, we should align on good standards and practices that enable us to uphold our commitment to safe and reliable operations of the bulk electric system.

When we look at the growth of the industry and the advancements in PV and PV + storage technology, as well as a growing trend of larger projects with more complicated commissioning schedules, we will be required to evaluate our workforce and assess if we have the level of personnel and expertise needed to handle the changing landscape. I think we will need to broaden the technical expertise present within our workforce and engage various applicable engineering disciplines to design, deploy and maintain SCADA systems. This is not just a challenge specific to SCADA integrators, but to the broader industry. We can put massive amounts of piles, modules, inverters and batteries in the ground, but without the SCADA engineers, network engineers, metering and relay technicians and RIG engineers to commission the plants, that equipment in the ground doesn't do us any good.

BL: I am looking forward to getting to a place where SCADA providers can all agree that they want interoperability to be able to talk to both each other and all the other components. We can recognize that we are competing businesses, but if we are wide open on the communication protocols, everyone's platform can talk to each other and our customers will truly benefit.

Once we get to that level, and we are getting pretty close to that, it is going to be pretty cool having everyone wide open. If you compare the platforms right now, younger generations are preferring Ignition because it has a glossy front end that looks more like a web browser. If you look underneath the hood, all major SCADA platforms do high-performance graphics, so they all do the same thing. They all basically have an SQL Historian and can create models or templates with tags or objects that can do the same thing. So why does anyone go with a specific vendor? It is usually because of familiarity. If you come from a Wonderware background and you get into a position where you get to dictate which platform to use, you are going to go with Wonderware because you know it. However, the truth of it is, if a platform becomes cumbersome because the service team is unresponsive, you are going to look for something better. I believe we are at a point right now where it really comes down to customer preference, and that preference should be based on getting the best bang for your buck and getting reliable support and service when they need it.

END NOTES

[1] US Solar Market Insight, 16 Mar 2021; https://www.seia.org/us-solar-market-insight

NOR-CAL CONTROLS
ENERGY SOLUTIONS

4790 Golden Foothill Parkway
El Dorado Hills, CA
95762

+1-916-836-0800
contact@norcalcontrols.net

www.norcalcontrols.net